The Parliament of the Commonwealth of Australia

Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime

The Report of the Inquiry into Cyber Crime

House of Representatives
Standing Committee on Communications

June 2010
Canberra

© Commonwealth of Australia 2010
ISBN 978-0-642-79313-3 (Printed version)

ISBN 978-0-642-79314-0 (HTML version)

Contents

LIST OF TABLES

LIST OF FIGURES

Foreword

In the past decade, cyber crime has grown from the nuisance of the cyber smart hacker into an organised transnational crime committed for vast profit and often with devastating consequences for its victims. A sophisticated underground economy provides the IT tools to commit these crimes and the market for stolen identities and financial information.

In the technological world of cyber crime it can be easy to forget the human cost of the theft and deception inflicted on innocent people. We are reminded of the human cost by our constituents who face the emotional devastation and lasting financial consequences of the crimes perpetrated against them.

There has been an exponential growth in the volume of malicious software and the sophistication and adaptability of cyber crime techniques. In the face of these trends, the Committee believes the expectation that end users should or can bear the sole responsibility for their own personal online security is no longer a tenable proposition. We need to apply the same energy and commitment given to national security and the protection of critical infrastructure to the cyber crime threats that impact on society more generally.

A key message throughout this inquiry was that a more integrated, coordinated and concerted effort is required to combat the cyber crime that victimises ordinary consumers and private businesses. This requires a commitment to cooperation, strategic thinking and a cyber space perspective to overcome the silos of traditional institutions.

The Committee does not accept that the Internet is a kind of unpoliced 'wild west' − the Internet is a global communication medium that is subject to the same laws as the offline environment. It is true that technology enables criminals to obscure their identity and victimise people in different countries. It is equally true that technology allows us to trace perpetrators, to preserve, aggregate and analyse digital evidence, and to coordinate global enforcement action.

Through a nationally led and coordinated policy, as well as regulatory and law enforcement effort, Australia can deliver a more effective and strategic response to this problem. By necessity this has to be a joint public-private effort because the architecture of the Internet and the IT technology is in private hands. While the capacity to negotiate and create international agreements between nations is in the hands of the State.

The private sector, especially IT manufacturers, Internet Service Providers and web hosting companies, and the Domain Name Registrars and Resellers, all bear some corporate social responsibility to promote the integrity of the Internet. There is also a vast quantity of intelligence data that can be better shared between the public and private sector.

To this end the Committee has recommended that the interests and needs of consumers and business generally be elevated in the national *Cyber Security Strategy*. Some of the concrete steps that can be taken immediately include:

- a national coordination point to oversee this broader strategy;
- a national cyber crime reporting centre;
- better coordination and training for law enforcement agencies;
- public-private information sharing on a wider range of cyber crime types.

These new institutional arrangements should be supported by a stronger commitment to detect botnets, remediate infected computers and deal with compromised and fraudulent websites. This will require additional funding to support the Australian Communications and Media Authority.

The current strategy puts an emphasis on education and community awareness but seems to lack the coherence or clear benchmarks for success that might be expected for such an important priority. A clearly articulated national community education e-security strategy, including broader public campaigns, will help to promote more e-security awareness among the general public.

The private sector must also play its part. The Internet industry has to accept that commercial gains also carry social responsibilities. IT manufacturers also need to give a higher priority to security through better product testing, design and the provision of information to support informed consumer choices.

The reality of modern life is that information and communications technologies are a part of our everyday existence − the complexity and global reach of the Internet age can seem overwhelming but we should not lessen our commitment to protecting personal privacy or ensuring that informed consent and choice remain the central principles when transacting online.

Online businesses and public agencies must observe Australia's prohibitions against the over collection of personal information. The public also has a right to know if their personal information has been compromised because of a security breach.

On behalf of the Committee, I wish to thank the agencies, IT companies, peak bodies and the consumer groups who gave us substantial and well considered evidence. We also thank the State Governments who recognise this is an important national and international issue and are seeking ways to cooperate across jurisdictions to deal with this problem.

Finally, I also wish to thank my Committee colleagues who participated in this inquiry with enthusiasm for a difficult subject and with a commitment to bipartisanship. Members regularly hear the stories of their constituents seeking advice on where to take their complaints or how to protect themselves in the future. This first-hand experience and the cases we heard about during the inquiry served to remind us of the importance of tackling this insidious problem.

Ms Belinda Neal MP

Chair

Membership of the Committee

Chair	Ms Belinda Neal MP
Deputy Chair	The Hon Mark Vaile MP (until 26/8/08)
	Mrs Kay Hull MP (from 26/8/08)
Members	The Hon Bruce Billson MP (until 3/2/10)
	Mr David Bradbury MP
	Ms Julie Collins MP
	Mr Steve Georganas MP
	Mr Steve Irons MP (until 4/6/09)
	Ms Nola Marino MP (from 4/6/09)
	The Hon Peter Lindsay MP
	Ms Kerry Rea MP
	Ms Amanda Rishworth MP
	The Hon Tony Smith MP (from 3/2/10)

Committee Secretariat

Secretary	Jerome Brown
Inquiry Secretary	Jane Hearn
Research Officers	Dr Narelle McGlusky (until 4/11/09)
	Geoff Wells (from 12/11/09)
Administrative Officers	Heidi Luschtinetz
	Dorota Cooley

Terms of reference

The House of Representatives Standing Committee on Communications shall inquire into and report on the incidence of cybercrime on consumers:

a) nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans;

b) the implications of these risks on the wider economy, including the growing economic and security impact of botnets;

c) level of understanding and awareness of e-security risks within the Australian community;

d) measures currently deployed to mitigate e-security risks faced by Australian consumers:

   i) education initiatives

   ii) legislative and regulatory initiatives

   iii) cross-portfolio and inter-jurisdictional coordination

   iv) international co-operation;

e) future initiatives that will further mitigate the e-security risks to Australian internet users; and

f) emerging technologies to combat these risks.

Glossary and abbreviations

.auDA	.au Domain Administration
419 scam	See 'Advance-fee fraud'
ABA	Australian Banking Association
ABS	Australian Bureau of Statistics
ACC	Australian Crime Commission
ACCAN	Australian Communications Consumers Action Network
ACCC	Australian Competition and Consumer Commission
ACFT	Australian Consumer Fraud Task Force
ACMA	Australian Communications and Media Authority
Advance-fee fraud	A scam where the victim hands over money in the hope of realising a significantly larger gain
Adware	A type of software which directs advertisements at users and in some cases gathers personal information
AFP	Australian Federal Police
AGD	Attorney General's Department
AHTCC	Australian High Tech Crime Centre
AIC	Australian Institute of Criminology
AIIA	Australian Information Industry Association
AISI	Australia Internet Security Initiative

ALRC	Australian Law Reform Commission
Anti-virus software	Software to prevent, detect and remove malware
APCA	Australian Payments Clearing Association
APWG	Anti-Phishing Working Group
ASCCA	Australian Seniors Computer Clubs Associations
ASIC	Australian Securities and Investment Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AusCERT	Australian Computer Emergency Response Team
Backdoor	A hidden access point which permits a computer to be remotely accessed by another computer
Blacklist	A list or register of persons or computers who are denied access to a network or computer system
Bot	A malware-infected computer that can be remotely controlled over a network
Botherder	See 'botmaster'
Botmaster	The controller of a botnet
Botnet	A network of bot computers that can be simultaneously controlled from a central point
ccTLD	Country Code Top Level Domain, a domain name denoting where a website is registered (such as '.au')
CERT Australia	Computer Emergency Response Team Australia
Cloud computing	Computing where users can access programs, processes and information on-demand over the Internet, without such resources being installed on their own computer
CLPC	Cyber Space Law and Policy Centre
CNP Fraud	Card Not Present Fraud, online credit card fraud committed with stolen information only without the need for the physical credit card
Computer offences	Criminal acts of a technical nature such as hacking, DDoS attacks and malware intrusions

CTN	Consumer Telecommunications Network
Cyber attack	An attempt to undermine or compromise a computer system or the user of such a system
Cyber crime	A range of crime types including computer offences, online banking and credit card fraud, and online scams
Data breach	The unauthorised disclosure, release or loss of secure information to an insecure environment
DBCDE	Department of Broadband, Communications and the Digital Economy
DDoS	Distributed Denial of Service, a method by which botnets flood a computer system with information thus damaging or shutting down the system
DNS	Domain Name System, the system that translates user-friendly web addresses into IP addresses
DNS hijacking	The act of subverting a computer to contact a fake DNS server instead of a legitimate DNS server
DNS spoofing	The act of replacing a genuine IP address in the DNS with a fake IP address
DNSSEC	Domain Name System Security Extensions
Domain	See 'Domain names'
Domain hijacking	The act of taking control of a domain name by stealing the identity of a domain name owner
Domain Owner	The registrant of a particular domain name
Domain Registrar	An accredited organisation that manages the registration of particular domain names
Domain Reseller	An organisation that on-sells the rights to use particular domain names
Domain names	A hierarchical series of codes that combine to form unique web addresses (See 'gTLD' and 'ccTLD')
DSD	Defence Signals Directorate
E-security	The protection of computer systems from technical threats

ESPaC	E-Security Policy and Coordination Committee
FBI	US Federal Bureau of Investigation
FCCG	Queensland Police Fraud and Corporate Crime Group
Firewall	A part of a computer system or network that blocks unauthorised access
gTLD	Generic Top Level Domain, a domain name generally denoting the nature of a website's owner (such as '.gov')
Hacker	A person who illegally accesses, controls or damages other computer systems
Honeypot	A dummy computer, program or email account set up to attract and deflect cyber attacks on a system
HTCOC	High Tech Crime Operations Centre
HTTP	Hypertext Transfer Protocol, a protocol that enables computers to exchange data with web page hosts
ICANN	Internet Corporation for Assigned Names and Number
ICPEN	International Consumer Protection and Enforcement Network
ICT	Information and communications technology
Identity crime	The theft or misuse of another person's identity
Identity fraud	The illegal assumption of another person's identity for purposes of fraud
Identity theft	The theft of personal information
IIA	Internet Industry Association
IP Address	Internet Protocol Address, a number that identifies a device on a network
ISP	Internet Service Provider, a company that provides access to the Internet
IT	Information technology
ITU	International Telecommunication Union
JBFSIT	Joint Banking and Finance Sector Investigations Team
Keystroke logger	A hidden program which illegally records each key that

	is pressed on a computer's keyboard
LEA	Law enforcement agency
Malware	A generic term for software designed to damage or subvert a system
Money mule	A person who launders money via internet banking and wire transfers to online criminals
NBN	National Broadband Network
Nigerian scams	See 'Advance-fee fraud'
NSW	New South Wales
NT	Northern Territory
OECD	Organisation for Economic Co-operation and Development
Banking fraud	Fraud committed to illegally remove money from another person's bank account
Credit card fraud	Fraud committed using stolen credit card information
OPC	Office of the Privacy Commissioner
OVPC	Office of the Victorian Privacy Commissioner
Peer-to-peer	A form of decentralised network where computers can exchange information directly with any other computer
Phishing	The act of assuming the online identity of a legitimate organisation to trick users into divulging information or to commit fraud
PM & C	Department of the Prime Minister and Cabinet
QPS	Queensland Police Service
Romance scam	A scam where victims hand over money to fraudulent participants on online dating websites
Rootkit	A set of programs designed to hide malware infections on a computer
SA	South Australia
SME	Small or medium sized enterprise
SOCA	UK Serious and Organised Crime Agency

Spam	Unsolicited bulk email messages
Spamtrap	A dummy email address used to attract spam (See 'Honeypot')
Spyware	A program that illegally records data such as computer screen images, stored data and details on internet browsing activity
TISN	Trusted Information Sharing Network for Critical Infrastructure Protection
Toolkit	Off-the-shelf style, user-friendly malware packages
Trojan	Malware which appears legitimate but in fact contains hidden malicious functions
UK	United Kingdom
US	United States of America
Virus	Malware contained within a 'host' program which spreads by inserting a copy of itself into other programs
WA	Western Australia
Walled garden	Restricted network access to isolate infected computers from other computers on a network
Whitelist	A list or register of persons or computers who are permitted access to a network or computer system, to the exclusion of those not on the list
Worm	Self-replicating malware which transmits across a network without a host program
WPISP	OECD Working Party for Information Security and Privacy
Zombie	See 'Bot'

List of recommendations

3 Research and Data Collection

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.

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.

5 Domestic and International Coordination

Recommendation 3

That the Australian Government establish an Office of Online Security headed by a Cyber Security Coordinator with expertise in cyber crime and e-security located in the Department of Prime Minster and Cabinet, with responsibility for whole of Government coordination. The Office is to take a national perspective and work with State and Territory

governments, as well as federal regulators, departments, industry and consumers.

That the Australian Government establish a National Cyber Crime Advisory Committee with representation from both the public and private sector to provide expert advice to Government.

Recommendation 4

That the Australian Government, in consultation with the State and Territory governments and key IT, banking and other industry and consumer stakeholders, develop a national online cyber crime reporting facility geared toward consumers and small and medium sized businesses.

This model should include the following features:

- a single portal for standardised online receipt of cyber crime reports across a wide range of cyber crime types (e.g. malware, spam, phishing, scams, identity theft and fraud);
- a 24/7 reporting and helpline;
- no financial minimum to be applied to cyber crime reports;
- systematic data collection that allows data to be aggregated;
- referral to appropriate authorities and cooperation on the disruption of cyber crime and targeted prosecutions;
- free access to scanning software to detect malware;
- public information about cyber crime types and preventative measures to increase online personal security;
- e-security alerts tailored to the needs of ordinary consumers and small and medium sized businesses; and
- analysis of cyber crime methodologies and trends or cooperation with another body to perform that analysis.

Recommendation 5

That the Federal, State and Territory police forces establish an E Crime Managers Group to facilitate the sharing of information and cross jurisdiction cooperation.

Recommendation 6

That the Australian Government, in consultation with the State and Territory governments, industry and consumer organisations, develop a

national law enforcement training facility for the investigation of cyber crime.

Recommendation 7

That the Australian Government consult with major IT security vendors, academia and key industry stakeholders to develop:

- options for establishing a coordinated public-private capacity to provide real time operational information on a wider range of cyber crime types that impact on Australian consumers;
- an 'intelligence hub' that facilitates information sharing within and across industry sectors and provides:
  - ⇒ longer term analysis on cyber crime methodologies across a range of cyber crime types;
  - ⇒ education on the preservation of digital evidence; and
  - ⇒ support to law enforcement agencies for targeted prosecutions in Australia and overseas.

6 Criminal and Law Enforcement Framework

Recommendation 8

That the Federal, State and Territory Attorneys-General review the existing computer and identity fraud provisions and, if necessary, introduce or amend provisions to ensure consistency across all Australian jurisdictions.

Recommendation 9

That the Federal Attorney-General, in consultation with State and Territory counterparts, give priority to the review of Australian law and practice and move expeditiously to accede to the Council of Europe Convention on Cybercrime.

Recommendation 10

That Australia's cyber crime policy strategically target the underground economy in malicious IT tools and personal financial information; the disruption of botnets and the identification and prosecution of botherders.

Recommendation 11

That the Commonwealth, State and Territory governments establish a national working group on cyber crime to maintain an ongoing,

dedicated mechanism for the review and development of legislative responses to cyber crime.

That the working group take a whole of cyberspace perspective and consider relevant IT industry, consumer protection and privacy issues as well as the criminal law.

7 Protecting the Integrity of the Internet

Recommendation 12

That the Australian Communications and Media Authority further increase its access to network data for the purpose of detecting malware compromised computers. This should include active consideration of how to increase access to network data held by global IT security companies and, in consultation with relevant departments, whether legal protections to address commercial, regulatory and privacy concerns are desirable.

Recommendation 13

That the Australian Communications and Media Authority consider how best the Australian Internet Security Initiative network data might be used to support the threat assessment and emergency response functions of government.

Recommendation 14

That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to immediately elaborate a detailed e-security code of practice to be registered under the *Telecommunications Act 1997* (Cth).

That the code of practice include:

- an obligation that the Internet Service Provider provides basic security advice when an account is set up to assist the end user to protect themselves from hacking and malware infections;
- a mandatory obligation to inform end users when their IP address has been identified as linked to an infected machine(s);
- a clear policy on graduated access restrictions and, if necessary, disconnection until the infected machine is remediated;
- the provision of basic advice and referral for technical assistance for remediation; and

- a requirement that acceptable use policies include contractual obligations that require a subscriber to:
  - ⇒ install anti-virus software and firewalls before the Internet connection is activated;
  - ⇒ endeavour to keep e-security software protections up to date; and
  - ⇒ take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.

Recommendation 15

That the Australian Government, in consultation with the Internet industry, review the scope and adequacy of s.313 of the *Telecommunications Act 1997* (Cth) to promote Internet Service Provider action to combat the problem of malware infected machines operating across the Internet.

Recommendation 16

That a more integrated model for the detection and removal of malware, built on the Australian Internet Security Initiative, be implemented. The new scheme should involve the Australian Communications and Media Authority, Internet Service Providers, IT security specialists, and end users in a more tightly coordinated scheme to detect and clean malware infected computers.

Recommendation 17

That the Australian Communications and Media Authority be funded to develop a system that can obtain data on compromised web pages from various sources (including developing an internal capability). This data be collated and provided as daily aggregated reports to Internet Service Providers identifying infected web pages residing on their networks.

That in addition to Internet Service Providers, domain owners and hosting companies also be included in the new scheme.

Recommendation 18

That the system for reporting and detecting compromised web pages proposed in recommendation 17 be supported by a registered industry code that outlines industry procedures for dealing with infected websites.

That the Australian Communications and Media Authority be empowered to enforce the provisions of the registered code, including,

for example, where there is a need to direct a service provider to remove malicious content.

That Internet Service Providers and hosting companies who act on reports of infected websites be indemnified against claims for losses.

Recommendation 19

That the Australian Communications and Media Authority and the Internet Industry Association review the *Spam Code of Practice* to assess the effectiveness of current industry standards for the reporting of spam.

That serious consideration be given to obliging Internet Service Providers to include the Australian Communications and Media Authority's *SpamMatters* program as part of their email service to subscribers.

Recommendation 20

That the Australian domain name registration industry be subject to a code of conduct that is consistent with the Anti-Phishing Working Group *Best Practices Recommendations for Registrars*.

The code of conduct should:

- enumerate the type of information that should be collected during the domain name registration process by the registrar, that would help to preserve evidence and assist law enforcement authorities;
- identify processes that should be put in place to identify fraudulent activity before the domain name registration takes effect; and
- provide clear procedures for responding to requests for rapid take down of fraudulent sites and sites that host malware.

Recommendation 21

That the Minister for Broadband, Communications and the Digital Economy make a reference to the House of Representatives Standing Committee on Communications to inquire into the regulation, standards and practices of the domain name registration industry in Australia.

8 Consumer Protection

Recommendation 22

That the Australian Government ensure that:

- remedies available under the new Australian Consumer Law can be effectively asserted against perpetrators outside Australia; and

- the *Foreign Judgments Act 1991* (Cth) be amended to allow for the reciprocal registration and enforcement of non-money judgments made under the Australian Consumer Law.

Recommendation 23

That the Treasurer amend the Australian Consumer Law to include specific protections against the unauthorised installation of software programs:

- the reform should target the unauthorised installation of programs that monitor, collect, and disclose information about end users' Internet purchasing and Internet browsing activity;
- the authority to install a software program must be based on informed consent; and
- to obtain informed consent the licence/agreement must require clear accessible and unambiguous language.

Recommendation 24

That the Australian Competition and Consumer Commission, in consultation with manufacturers and distributors of personal computers, mobile phones and related IT devices such as modems and routers, develop information standards to:

- address the e-security vulnerabilities of these products and the provision of e-security information to consumers at the point of sale; and
- require that the information is presented in a manner that is clear and accessible to a non-IT literate person.

Recommendation 25

That the Treasurer direct the Productivity Commission to conduct an in depth investigation and analysis of the economic and social costs of the lack of security in the IT hardware and software products market, and its impact on the efficient functioning of the Australian economy.

That, as part of its inquiry, the Productivity Commission address the merits of an industry specific regulation under the Australian Consumer Law, including a scheme for the compulsory independent testing and evaluation of IT products and a product labelling scheme.

Recommendation 26

That the Treasurer consult with State and Territory counterparts with a view to amending the Australian Consumer Law to provide a cause of

action for compensation against a manufacturer who releases an IT product onto the Australian market with known vulnerabilities that causes losses that could not have reasonably been avoided.

Recommendation 27

That the manufacturers of IT products adopt a best practice approach that ensures products are designed to prompt and guide end users to adopt more secure settings.

That the Australian Government monitor industry practice in this regard, and promote international standards that put a higher priority on security through product design.

9 Privacy Measures to Combat Cyber Crime

Recommendation 28

That the Office of the Privacy Commissioner use the full extent of its powers to ensure that overseas organisations that handle the personal information of Australian citizens and residents are aware of, and adhere to, their obligations under the *Privacy Act 1988* (Cth).

Recommendation 29

That the Office of the Privacy Commissioner expedite the adoption of an approved privacy code of practice for members of the Australian Internet industry, including smaller Internet Service Providers.

Recommendation 30

That the Office of the Privacy Commissioner encourage government agencies and commercial organisations to undertake regular audits to identify risks to personal information in both new and existing projects and policies.

10 Community Awareness and Education Initiatives

Recommendation 31

That the Department of Broadband, Communications and the Digital Economy, in consultation with relevant agencies, industry and 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.

Recommendation 32

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

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.

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.

1

Introduction

1.1 The Internet has developed rapidly over the past three decades, evolving from its military and academic origins to become a critical part of the communications infrastructure of most modern economies. It has brought with it a transformation in global communications, delivering new opportunities for business, service delivery, information sharing and communications. However, alongside these great benefits are new threats as cyber criminals exploit the weaknesses, complexity, speed and global scale of cyber space.

1.2 The nature of cyber crime has also undergone a transformation. The cyber criminal is no longer the nuisance hacker, motivated by the desire to show off their technical prowess, but more likely to be part of a loosely linked network of hackers, middlemen and organised crime who combine to commit large scale online crimes for significant profit. Cyber crime is now a sophisticated transnational threat that operates on an industrial scale and has become an increasingly important issue for the global community.

1.3 This inquiry is a timely adjunct to three major e-security policy reviews undertaken by the US, the UK and Australia in the past 18 months. In June 2009 the White House released the *Cyber Space Policy Review*,[1] the UK published *Digital Britain* and subsequently released the *Cyber Security Strategy of the United Kingdom* also in June 2009.[2] In Australia, an *E Security Review,* announced in early 2008, culminated in the release of the Australian Government's *Cyber Security Strategy* on 23 November 2009.[3]

---

1 *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, White House, 29 May 2009.

2 *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, Cabinet Office (UK), June 2009.

3 *Cyber Security Strategy*, Australian Government, 2009.

1.4 These reviews reflect the importance that governments of the developed economies attach to e-security as a national and international issue. The need for a more integrated and coherent policy response to the realities of cyber space has been recognised by the US, the UK and Australia. However, many of the responses to new cyber threats have been driven by national security concerns and the need to protect critical public infrastructure. While these are important national objectives, this inquiry was concerned with the incidence and impacts of a range of cyber crime types that affect Australian society more generally.

1.5 It is not the first Parliamentary investigation into the wider impacts of this problem. In 2004, the Parliamentary Joint Committee on the Australian Crime Commission (ACC) inquired into ACC's role in relation to cyber crime.[4] In the same year, the Victorian Parliament examined the problem of fraud in the context of e-commerce.[5] More recently, personal Internet security was the subject of an inquiry by the UK House of Lords Science and Technology Committee.[6]

Referral of the Inquiry

1.6 On 13 May 2009, Senator the Hon Stephen Conroy, Minister for Broadband, Communications and the Digital Economy (DBCDE) wrote to the House of Representatives Standing Committee on Communications (the Committee) asking it to inquire into the incidence and impact of cyber crime on consumers and the Australian economy, and examine the adequacy of Australia's measures to combat the problem.

1.7 The terms of reference are set out at the front of this report.

1.8 A media release announcing the inquiry was issued on 18 May 2009 and published on the Committee's website on the same day. The terms of reference were advertised and written submissions invited in *The Australian* on 27 May and 10 June 2009. The inquiry was also advertised in the July issue of *Net Guide* and *Australian PC*.

1.9 The Committee wrote to over two hundred stakeholders encompassing government departments, regulatory agencies, consumer groups, IT vendors, banks and credit unions, peak industry bodies, professional

4 Parliamentary Joint Committee on the Australian Crime Commission, *Cybercrime,* The Parliament of the Commonwealth of Australia, March 2004.

5 Drug and Crime Prevention Committee, *Final Report of the Inquiry into Fraud and Electronic Commerce*, Parliament of Victoria, January 2004.

6 Science and Technology Committee, *Personal Internet Security*, Volume 1 Report, House of Lords, August 2007.

associations, academics and researchers. These invitations included relevant overseas bodies.

1.10 Written submissions were received from sixty-eight organisations and individuals. The list of submissions appears as Appendix A. The Committee also accepted twenty-two exhibits. The list of exhibits appears as Appendix B.

1.11 Fifty-three witnesses appeared in person to give oral evidence during eleven separate hearings in Canberra and Sydney between August 2009 and March 2010, and several witnesses provided additional evidence in response to questions on notice. The list of witnesses appears as Appendix C. The Committee also conducted an inspection of the Australian Federal Police high tech crime facilities in Canberra on 23 November 2009.

Definition of Cyber Crime

1.12 The Committee had to consider the scope of the inquiry and, in particular, the meaning of 'cyber crime' in the context of the terms of reference. The *Cyber Security Strategy* defines 'cyber crime' as offences against computers and computer systems, such as hacking, malware intrusions, and denial of service attacks. However, it quickly became apparent that terms such as 'cyber crime', 'technology enabled crime', 'Internet crime', 'e-crime', and 'online crime' are used interchangeably across government agencies and the community. Given the complex and interlinked nature of criminal activity it was important not to be artificially limited by a narrow technical definition of cyber crime. The Committee has used 'cyber crime' in its wider sense to include both offences against computers and computer systems and technology enabled crime.

1.13 Some witnesses also made a distinction between 'e-security' and 'cyber safety', especially where the latter involved children and young people in conduct that is not generally characterised as e-crime. The Committee did not entirely accept the distinction. However, the evidence on the problems of cyber bullying, stalking, and the unauthorised publication of damaging, images, was limited. The Committee did not seek out evidence on online child sex exploitation or the online publication of pornography because, although this is an aspect of cyber crime, it has been dealt with extensively by the Parliament.

1.14 Finally, in March 2010 the Parliament established a Joint Select Committee on Cyber Safety to take a more in depth look at these related areas of online conduct, especially as they relate to children and young people. Consequently, while the Committee is concerned about the exposure of

children and young people to online exploitation and the misuse of new social media, this was not the focus of this inquiry.

Overview of the Report

1.15 There was a clear message to the Committee that home users are most vulnerable to cyber crime, often unwittingly exposing themselves and others to e-security risks through a lack of online protections. While prevention through education is important, on its own education is insufficient to combat sophisticated cyber crime techniques. The Committee believes that it is time to shift our thinking toward a model where consumers, industry and government accept greater shared responsibility for personal Internet security.

1.16 In overview, the following three chapters that explain the complex nature of cybercrime, the need for comprehensive research to support policy development and the gap between end user awareness and preventative action. The remaining seven chapters that discuss proposals to strengthen Australia's response by committing to a more integrated, coordinated and concerted effort to target both policy and law enforcement against cyber criminals.

1.17 Chapter 2 examines the nature, prevalence and economic impact of cyber crime. It explains the role of botnets, which provide the infrastructure from which most criminal activity is launched. Cyber crime is often a combination of activities such as malware, spam, phishing, and spyware and it can be difficult to separate the civil and criminal aspects. These techniques are used to steal vast quantities of personal and financial information for sale in the underground market and for use for financial and identity crimes. While anti-virus software and cautious online behaviour can reduce e-security risks many viruses and other criminal techniques are undetectable.

1.18 The need for data collection and research as a necessary pre-requisite to effective policy development is canvassed in Chapter 3. The evidence from Information Technology (IT) security companies shows an exponential growth in malware and related computer offences. Under reporting of computer offences and online identity and financial crimes makes it difficult to measure the scope of the problem. Other cyber crime types, such as fraudulent websites, romance scams and advance fee fraud, are also under reported often because the victims are too embarrassed to come forward.

1.19 Chapter 4 describes the current level of public awareness of e-security threats and the vulnerability of Australian end users. The evidence indicates that even high levels of awareness do not necessarily translate into preventative action. Surveys indicate that only about half of the end users connected to the Internet have installed anti-virus software and many do not update their software.[7] And, despite efforts by government agencies and the banking industry, the Australian Bureau of Statistics has estimated that in 2006 alone 30,400 Australians were a victim of an online phishing scam.[8]

1.20 It is against this background that the remaining chapters of the report discuss proposals for a more integrated, coordinated and concerted approach to the problem of cyber crime as it impacts on consumers and business.

1.21 The theme of Chapter 5 is coordination across government, law enforcement authorities and between the public and private sector. There is a plethora of government agencies and private stakeholders, including Internet Service Providers (ISPs), Domain Name Registrars as well as the IT industry, with some role in relation to cyber crime. The Committee believes that, to get a more strategic approach to policy and better overall coordination, the Commonwealth needs to take more of a leadership role. In particular, all Australians would benefit from a national point of coordination and oversight of a broader national cyberspace strategy.

1.22 The transnational nature of cyber crime also means that Australian law enforcement efforts need more strategic and nationally scaled coordination. The Committee has recommended a one stop shop national centre for reporting a range of cyber crime types. This would give the public a single point of entry to report cyber crime. It would allow for the handling at first instance of both civil and criminal matters, and the collection and aggregation of intelligence data so that investigators can see the bigger picture.

1.23 Chapter 5 also discusses real time information sharing and an 'intelligence hub' to promote intelligence sharing and better trend analysis. The aim is to move the existing public-private information sharing beyond national security threats to include a wider range of cyber crime types.

---

7 Australian Communications and Media Authority, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.39; AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

8 Australian Bureau of Statistics, *2007 Personal Fraud Survey, ABS Catalogue No 4528.0,* ABS, 2007, p. 21.

1.24 Chapter 6 outlines the existing criminal law relating to computer offences and identity fraud, and it briefly canvasses some aspects of law enforcement powers. The chapter concludes that the legal framework has undergone significant development, although there continues to be a problem of lack of uniformity. The Australian Government should also expedite its work to bring domestic laws into conformity with the Council of Europe Convention on Cybercrime and seek accession to the treaty as soon as possible. This is important to strengthen Australia's international cooperation and to show leadership in the Asia Pacific Region.

1.25 Chapter 7 looks at the role of public and commercial stakeholders in protecting the integrity of the Internet. As previously stated, the Committee believes that protecting the integrity of the Internet is a shared responsibility, between government, private sector stakeholders, and end users. To translate this philosophy into concrete action the government should work with industry to do four key things:

- develop the voluntary *E Security Code of Practice* for ISPs into a more comprehensive document and register it as a mandatory code under the *Telecommunications Act 1997* (Cth);
- require Domain Name Registrars and Resellers should be required to apply a 'know your customer' principle to reduce the fraudulent use of domain names;
- build on the Australian Internet Security Initiative to implement a more integrated scheme to detect botnets and remediate compromised computers operating across Australian networks;
- fund the Australian Communications and Media Authority (ACMA) to detect compromised websites and empower ACMA to order the temporary or permanent removal of fraudulent or compromised websites from the Australian Internet.

1.26 Chapter 8 looks at the consumer protection regime, and how it applies to cyber crime. The new *Australian Consumer Law* strengthens the enforcement powers of the Australian Competition and Consumer Commission to protect consumers. The Committee believes there should be a specific consumer law requirement for informed consent before software programs are downloaded.

1.27 The new framework also provides an opportunity to develop national information standards for IT vendors and retailers to provide consistent e-security information to consumers. This should be aimed at encouraging consumers to take preventative steps and ensure they are better informed about the e-security risks of the IT products they are buying. The issue of

IT vendor liability is discussed, and a more in depth investigation by the Productivity Commission is recommended. The Committee has also recommended that the IT industry adopt better design standards for prompting consumers to adopt stronger security settings.

1.28 Chapter 9 discusses privacy law protections and endorses many of the recommendations of the Australian Law Reform Commission that relate to privacy and new technologies. In particular, the Committee supports the mandatory reporting of data breaches to ensure that individuals are able to take steps to protect themselves.

1.29 Chapter 10 addresses the adequacy of community education and awareness raising initiatives. A great deal of effort is expended in communicating e-security messages to the population: to young people and their parents through the schools, to adult consumers via the banking industry and the Australian Consumer Fraud Task Force. The Committee heard that the DBCDE's *Cyber Security Awareness Week* will move onto a more continuous footing with initiatives throughout the year. The value of promoting IT literacy generally, as distinct from for purely vocational purposes, was also advocated.

1.30 Despite these efforts Australia still has a long way to go to achieve the kind of cultural change necessary to make the population more e-security aware and active. There is an important role here for a clearly articulated national cyber security community education strategy, that identifies the different target audiences and education and information strategies to reach those audiences. Such a strategy should include a broad based 'public health style' campaign to promote key e-security messages in simple and easy to understand language. The DBCDE is best placed to develop a national cyber security education strategy, which should be reported on annually to the Parliament.

1.31 The final chapter, Chapter 11, canvasses evidence of new and emerging technologies with e-security features. The Committee concludes that, while technology alone will not solve the problem of cyber crime, continued technological innovation is needed to meet new and evolving threats. The Committee concludes that the value of such technologies to mitigating cyber crime should be considered, and that a competitive and innovative IT security industry should be maintained. This does not,

however, prevent better security standards becoming a higher priority for IT vendors.

2

Nature, Prevalence and Economic Impact of Cyber Crime

Introduction

2.1 This chapter addresses the nature, prevalence and economic impact of cyber crime.

2.2 The problem of cyber crime crosses many traditional technical, conceptual and institutional boundaries, and, due to its prevalence, has real and increasing social and economic impacts on all Australians. The chapter concludes that because of the inter-related nature of the different aspects of cyber crime, a more holistic and strategic approach must be taken to its prevention.

Nature of cyber crime

2.3 This section demonstrates that cyber crime is highly complex, self-reinforcing, technologically advanced, geographically widespread and indiscriminate by examining the history, tools, industrial nature, perpetrators and victims of cyber crime.

Cyber crime and the Internet

2.4 Mr Peter Watson, Microsoft Pty Ltd, told the Committee that the Internet, by its very design, is an inherently vulnerable network which has enabled cyber crime to flourish in a new virtual 'Wild West' environment.[1]

2.5 The Internet originated from a relatively basic network set up to share information between trusted people and organisations for military and academic purposes, with no view to the security of the computers attached to these networks, nor the information stored on these computers.[2]

2.6 Today, this open and insecure system has evolved into a world wide network, directly connecting in excess of one billion users, and is employed for much more than the simple sharing of information.

2.7 Cyber crime flourishes in the online environment for a variety of reasons:

- the fundamentally insecure nature of the Internet leaves computers vulnerable to exploitation by less-than-trustworthy Internet users;
- the huge number of computers connected to the Internet gives cyber criminals a wide array of targets;
- the Internet is an effective medium for running automated systems, thus leading to the automation of online criminal activity; and
- the unregulated nature of the Internet makes it inherently difficult to control the content and data traversing the network, thus impeding efforts to combat malicious exploitation of the Internet.[3]

Why do people commit cyber crime?

2.8 Cyber criminals may be motivated by curiosity, fame-seeking, personal reasons (such as stalking or emotional harassment), political reasons (such as protests), espionage or cyber warfare. However, during the inquiry financial gain was repeatedly identified as the prime motivator of cyber crime.[4]

---

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

2 CSIRO, *Submission 26*, p.4; Dr Paul Twomey, Internet Corporation for Assigned Names and Numbers (ICANN), *Transcript of Evidence,* 8 October 2009, p.2.

3 See for example: Australian Computer Society, *Submission 38*, p.2. Dr Paul Twomey, ICANN, *Transcript of Evidence,* 8 October 2009, p.2; Australian Communications Consumer Action Network (ACCAN), *Submission 57*, p.53; Mr Stephen Wilson, Lockstep Technologies Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.44; Symantec Asia Pacific Pty Ltd, *Submission 32*, p.19; Microsoft Australia, *Submission 35*, p.1; Internet Safety Institute, *Submission 37*, p.5.

4 See for example: Dr Russell Smith, Australian Institute of Criminology (AIC), *Transcript of Evidence*, 19 August 2009, p.3; AIC, *Submission 41*, p.10; Mr Michael Sinkowitsch, Fujitsu

2.9 The Committee heard that cyber crime has become a highly lucrative business through cyber attacks which involve the theft of personal information, fraud, illegally accessing financial systems and online extortion. Additionally, an underground economy has developed through which cyber criminals may earn money by trading cyber crime related goods and services.[5]

How do people currently commit cyber crime?

2.10 Modern cyber crime is facilitated by a range of technologies and techniques including:

- hacking;
- malicious software (malware);
- botnets;
- spam;
- DNS based attacks;
- phishing;
- identity theft and identity fraud;
- scams;
- extortion;
- underground cyber crime forums; and
- money laundering techniques.

2.11 As with all aspects of cyber crime, cyber crime technologies and techniques are often interrelated and complementary. These technologies and techniques, and their purposes, are defined below.

Australia Ltd, *Transcript of Evidence*, p.49; Dr Paul Twomey, ICAAN, *Transcript of Evidence*, 8 October 2009, p.6; Organisation for Economic Cooperation and Development (OECD), *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.17.

5 See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.3; Mr Peter Coroneos, Internet Industry Association (IIA), *Transcript of Evidence*, 11 September 2009, p.13; Dr Paul Twomey, ICANN, *Transcript of Evidence*, 8 October 2009, p.6; Australian Federal Police (AFP), *Submission 25*, p.3; PayPal Incorporated, *Submission 60*, Symantec Asia Pacific Pty Ltd, *Submission 32*, p.3; Department of Broadband, Communications and the Digital Economy (DBCDE), *Submission 34*, p.6.

Hacking

2.12 'Hacking' is a term with multiple meanings. It can refer to testing and exploring computer systems, highly skilled computer programming or the practice of accessing and altering other people's computers. Hacking may be carried out with honest aims or with criminal intent.[6]

2.13 In relation to cyber crime, and for the purpose of this report, hacking refers to the practice of illegally accessing, controlling or damaging other people's computer systems. A hacker may use their own technical knowledge or may employ any of the cyber crime tools and techniques that are listed below.

Malicious software (Malware)

2.14 Malware is a general term for software designed to damage or subvert a computer or information system.[7] A range of different types of malware exists:

- viruses, worms and trojans are pieces of computer code or computer programs that automatically infiltrate computer systems, to degrade computer performance or to deliver other types of malware;[8]
- a backdoor permits a computer to be remotely controlled over a network;[9]
- rootkits are sets of programs that hide malware infections on a computer by concealing infected files and turning off anti-virus protection programs;[10] and
- keystroke loggers and spyware are programs that illegally capture data from a computer (spyware is related to a legitimate type of software called adware, described below).[11]

---

6 See for example: G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, p.83; AIC, *High tech crime brief: Hacking offences*, AIC, 2005, p.1.

7 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.10.

8 See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.91; G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, p.87; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.91.

9 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.90.

10 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.90;

2.15 Malware may propagate through virtually any medium that contains data or transmits data between information systems including infected websites, email, instant messaging, removable data hardware (such as USB drives), file sharing networks and wireless networks.[12]

2.16 Previously, websites transmitting malware tended to be less reputable, and poorly maintained, many of which were designed purely to infect computers. However, cyber criminals are increasingly using highly-reputable and popular legitimate websites and social networking pages to infect computers. A cyber criminal will exploit a vulnerability of the system that is hosting the website or social networking page in order to hide malware in the system, unbeknown to the legitimate website operator. When a benign user visits this legitimate website or social networking page the malware will automatically and covertly install on the victim's computer.[13]

2.17 Malware may install itself on a computer via a self-propagating mechanism, or when a user clicks on a malicious link in an email, opens a malicious file or visits a website where malware is hosted.[14]

The relationship between adware and spyware

2.18 Adware is a legitimate type of software, similar to spyware, which is often automatically, and openly, installed on a computer as part of a larger software package.[15] Adware enables software providers to earn revenue by directing advertisements at the users of their software via 'pop-ups' or banner advertisements. Adware programs may also gather personal information which is then used by the adware company to tailor their advertisements to be more effective.[16]

2.19 The distinction between adware and spyware can turn on whether the adware company has adequately informed the end user of the function of

11 See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.90-91; G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, pp.79-87.

12 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.12;

13 See for example: Australian Communications and Media Authority (ACMA), *Submission 56*, p.14; Symantec Corporation, *Submission 32*, p.2.

14 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.12;

15 Symantec Asia Pacific Pty Ltd, *Submission 32*, p.20.

16 AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1.

the software and the use of any personal information which is gathered.[17] Where the adware company gathers information outside of its permissions, or uses the information for purposes outside of its advertised terms, the software may cease to be adware, and become spyware.

Botnets

2.20 As previously mentioned, backdoors are a category of malware that enable a cyber criminal to remotely control an infected computer over a network. Such an infected computer is often called a robot or 'bot' computer. When several computers are infected with a backdoor and become bots, they can be simultaneously controlled from a single remote 'command and control' (C&C) mechanism. These remotely controlled networks of bot computers are known as 'botnets'.

2.21 Botnets can be comprised of a huge number of computers, with there being many documented cases of botnets comprised of more than 100,000 computers. Table 2.1 below shows the biggest botnets for 2009 as reported by MessageLabs, a subsidiary of the Symantec Corporation.

Table 2.1 Biggest botnets in 2009

botnet	estimated botnet size	Country of Infection
Rustock	540k to 810k	Brazil (21%), USA (9%), Poland (7%)
Cutwail	100k to 1600k	Vietnam (17%), RepKorea(12%), Brazil (10%)
Bagle	520k to 780k	Brazil (12%), Spain (9%), USA (9%)
Bobax	100k to 160k	Spain (12%), Italy (7%), India (7%)
Grum	580k to 860k	Vietnam (18%), Russia (17%), Ukraine (8%)
Maazben	240k to 360k	Romania (17%), Brazil (11%), Saudi Arabia (7%)
Festi	140k to 220k	Vietnam (31%), India (11%), China (5%)
Mega-D	50k to 70k	Vietnam (14%), Brazil (11%), India (6%)
Xarvester	20k to 36k	Brazil (15%), Poland (11%), USA (10%)
Gheg	50k to 70k	Brazil (15%), Poland (8%), Vietnam (8%)
Unclassified Botnets	120k to 180k	
Other, smaller botnets	130k to 190k	

Source MessageLabs, *Message Labs Intelligence: 2009 Annual Security Report*, MessageLabs, December 2009, p.8.

2.22 Botnets are considered to be one of the biggest enablers of cyber crime with the Cyberspace Law and Policy Centre, from the University of New

17 K Howard, Mallesons Stephen Jacques, *Computers and Law*, March 2006, p.17.

South Wales, submitting that 'almost every major online crime may be traced to botnets'.[18]

2.23 Below is a description of the different functions of botnets followed by a description of methods by which botnets are becoming increasingly resilient.

Functions of botnets

2.24 A botnet can be instructed by its controller, known as a 'botmaster', to carry out a range of functions (as outlined in Figure 2.1 below) including:

- launching 'distributed denial of service' (DDoS) attacks (a method by which botnets flood a computer system with information thus damaging or shutting down the system);[19]
- hosting malicious websites (such as money laundering, malware or phishing websites) or obscene content (such as child pornography) to shield the originator from being identified;[20]
- scanning for, and exploiting, software vulnerabilities in other computers and websites;[21] and
- sending large numbers of unsolicited emails known as spam.[22]

18 Cyberspace Law and Policy Centre (CLPC), *Submission 62*, p.3.

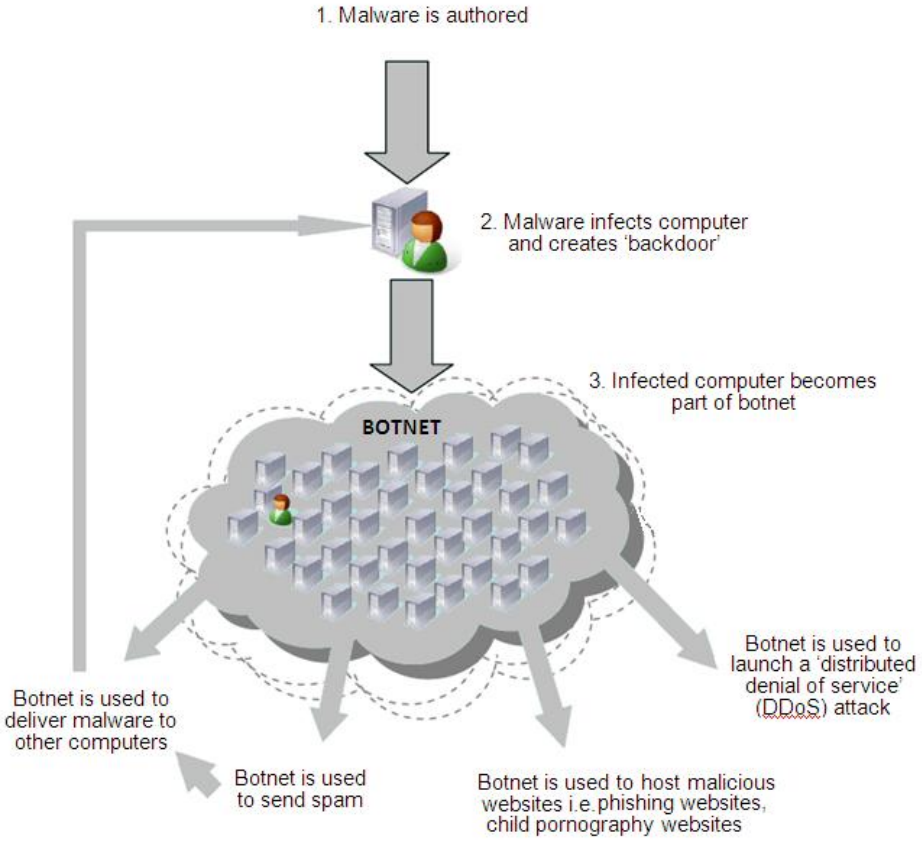
19 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.15. See also: G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, pp.81; KR Choo, *Trends and issues in crime and criminal justice: Zombies and Botnets*, AIC, Canberra, 2007, p.4.

20 See for example: RSA Security Inc, *Exhibit 2*, p.2; MT Banday, JA Quadri and NA Shah, 'Study of Botnets and their threats to Internet Security', *Sprouts: Working papers on information systems*, 2009, p.8, viewed 22 December 2009, <http://sprouts.aisnet.org>; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.23.

21 Symantec Asia Pacific Pty Ltd, *Submission 32*, p.6.

22 Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.6.

Figure 2.1 Initiation, growth and function of a botnet



Source OECD Committee for Information, Computer and Communications Policy, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p. 23.

2.25 The relationship between spam and botnets is significant: spam can be used to spread malware, such as backdoors, to other computers which in turn may recruit more bot computers to a botnet (see Figure 2.1). This demonstrates the interconnectedness and self-reinforcing nature of cyber crime.[23]

Resilience of botnets

2.26 Botnets are becoming ever more resilient through: improved C&C techniques; an ability to remotely upgrade very quickly; and a practice called 'fast fluxing', which shields important parts of the botnet from being identified and shutdown.

2.27 As previously mentioned, botmasters control botnets via C&C mechanisms. The botmaster posts a command on the C&C mechanism

23 IIA, *Submission 54*, p.3. See also: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.37.

(often a hijacked bot computer itself), which is then automatically disseminated to the individual bot computers that comprise the botnet. Botnets can operate on a centralised model (where each bot computer individually contacts a single central C&C mechanism to receive commands) or a decentralised model (where commands can be posted on any part of the botnet and then automatically passed from computer to computer via a peer to peer network).[24]

2.28 The decentralised botnet model is extremely hard to stop or dismantle as there is no centralised C&C point which can be targeted. If a number of bot computers are identified and taken offline, the gaps in the network will close up and the botnet will continue to function.[25]

2.29 Botnets are also high resilient due to the ease with which botmasters can rapidly update the underlying malware which runs the botnet. This enables botnets to rapidly adjust to exploit newly discovered vulnerabilities, and to respond to new anti-botnet measures.[26]

2.30 Botnets are further strengthened by the process of fast fluxing, whereby important parts of a botnet can be shielded from being traced, identified and shutdown. During this process, data travelling to and from important parts of the botnet (such as bot computers that host malicious websites or C&C mechanisms) first passes through any one of a number of decoy or proxy computers. Fast fluxing refers to the practice of employing the large number of computers in a botnet to rapidly alternate which computers are used as proxies. Thus when an attempt is made to trace the host computer, the trace only leads back to one of these relatively insignificant and temporary proxy computers.[27]

---

24 See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.24; AFP, *Submission 25*, p.9; JB Grizzard, VS Sharma, C Nunnery, BBH Kang and D Dagon, *Peer-to-Peer Botnets: Overview and Case Study*, in proceedings of USENIX Association First Workshop on Hot Topics in Understanding Botnets, 10 April 2007, Cambridge, USA, pp.5-6, viewed 24 December 2009, <http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard.pdf>.

25 JB Grizzard, VS Sharma, C Nunnery, BBH Kang and D Dagon, *Peer-to-Peer Botnets: Overview and Case Study*, in proceedings of USENIX Association First Workshop on Hot Topics in Understanding Botnets, 10 April 2007, Cambridge, USA, p.1, viewed 24 December 2009, <http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard.pdf>.

26 Symantec Asia Pacific Pty Ltd, *Submission 32*, p.6; CLPC, *Submission* 62, p.6.

27 See for example: RSA Security Inc., *Exhibit 3*, p.2; Dr Paul Twomey, ICANN, *Transcript of Evidence*, 8 October 2009, p.8; Fortinet, *Submission 29*, p.9; Symantec Asia Pacific Pty Ltd, *Submission 32*, p.15.

Spam

2.31 Spam refers to unsolicited emails, or the electronic equivalent of 'junk mail'. Spam is often disseminated in large amounts by sending out generic emails to large lists of email addresses.[28]

2.32 Spam may be sent through normal email accounts provided by an ISP, free online email services such as Hotmail, hijacked email servers, offshore companies that specialise in sending bulk mail, or the large number of computers connected to a botnet.[29] Additionally, in order to avoid anti-spam programs that identify generic emails or offending spammer email addresses, spammers employ programs which subtly change each email or hide the actual spammer's email address.[30]

2.33 Spammers can acquire lists of email addresses by: using different pieces of address-harvesting software to locate, steal, decipher and compile email addresses; hacking into the information systems of organisations; creating fake websites which fool users into entering their email address on the website; or through buying lists of email addresses on the black market.[31]

2.34 Spam has a variety of uses including: the mass delivery of legitimate advertising;[32] the mass delivery of scams and phishing schemes;[33] and the delivery of malware and in turn the expansion of botnets.[34]

DNS based attacks

2.35 The Domain Name System (DNS) is one of the underpinning aspects of the Internet. The DNS converts user-friendly text commands (in the form of web addresses) into IP addresses (complex numbers which identify each individual computer connected to the Internet). Thus the DNS

28 AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1.

29 See for example: P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.6; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.27; MessageLabs, *The Dark Art of Spam*, MessageLabs, 2009, pp.3-4.

30 P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.6.

31 See for example: P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.6; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.27; AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1; Mr Anthony Burke, Australian Bankers Association NSW Inc., *Transcript of Evidence*, 8 October 2009, p.59.

32 P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.1,5. See also: AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1.

33 ACCC, *Exhibit 16*, p.43.

34 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.27.

enables users to easily access computers that host web pages, without the need for complicated codes.[35]

2.36 Cyber criminals subvert the DNS in a number of ways:

- 'DNS spoofing' is a practice where cyber criminals hack into the DNS and replace a genuine IP address that leads to a legitimate website with a fake IP address that diverts users to a malicious website, such as a phishing website, or a website that infects computers with malware;[36]
- 'DNS hijacking' employs a trojan that changes the settings on a user's computer to access the DNS through a rogue DNS server instead of a legitimate ISP server, thus enabling users to be diverted to false websites;[37] and
- 'domain hijacking' is where a cyber criminal takes control of a domain name by stealing the identity of a domain name owner, then uses this domain name to host a malicious website.[38]

Phishing

2.37 Phishing describes an online attempt to assume the identity of, or mimic, a legitimate organisation for the purpose of convincing users to divulge personal information such as financial details, passwords, usernames and email addresses.[39]

2.38 The AIC provided the following example of a phishing website. Figure 2.2 shows the top section of a web page which appears to be from the legitimate 'Bank of the West' website.

35 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>.

36 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>.

37 F Hacquebord and C Lu, *Rogue Domain Name System Servers,* blog post, TrendLabs Malware Blog, Trend Micro, 27 March 2007, viewed 26 February 2010, <http://blog.trendmicro.com/rogue-domain-name-system-servers-5breposted5d>.

38 ICANN Security and Stability Advisory Committee, *Domain name hijacking: incidents, threats, risks, and remedial actions,* ICANN, 12 July 2005, p.8.

39 See for example: G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, p.85; Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November, 2009, p.19.

Figure 2.2 Example of phishing website

Source Australian Institute of Criminology, *Exhibit No. 5*, p. 8.

2.39 However, as demonstrated below in Figure 2.3, upon closer inspection of the address in the top bar of the browser, it can be seen that the W in 'Bank of the West' has been replaced with two V's to give the appearance of a W.

Figure 2.3 Close up of web address in phishing website

Source Australian Institute of Criminology, *Exhibit No. 5*, p. 8.

2.40 An unwitting user may be directed to this phishing website by clicking on the link in a fake spam email or through subversion of the DNS. The users may then fall for the confidence trick of the phishing website and may divulge personal details. In turn, the user may become a victim of identity theft or identity fraud.[40]

Identity theft and identity fraud

2.41 Through the use of keystroke loggers, spyware, and phishing websites cyber criminals may obtain a wide range of personal details. This is known as identity theft. These stolen details may then be used to commit 'identity fraud' (such as illegally accessing a victim's bank or credit card account, or taking out loans under a victim's name), sold online to other cyber criminals or used to fabricate fake official documents such as passports.[41]

40 Dr Russel Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.6.

41 See for example: Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November, 2009, pp.19, 24; Australian Bureau of Statistics, 2007 *Personal Fraud Survey*, ABS, Cat. No. 4528.0, 2007, p.8; Australian Government, *Dealing with identity theft: Protecting your identity*, Attorney General's Department (AGD), 2009, p. 4; AusCERT, *Computer Crime and Security Survey*, AusCERT, 2006, p.28.

2.42 Stolen information may also be used to commit further cyber crime activities. For example, a cyber criminal may use a stolen identity to open a new Internet account with an ISP from which to commit criminal acts.[42]

Scams

2.43 Online scams are another lucrative activity for cyber criminals. A plethora of scams exist on the Internet and new scams are continually emerging. Some of the scams brought to the Committee's attention were: romance scams, where victims hand over money to fraudulent participants on online dating websites (see the case study below for a victim's account of such a scam); advance-fee scams where the victim is promised large returns on an upfront payment; and fake lottery, ticketing or online shopping scams, where victims are fooled into paying for a nonexistent product.[43]

Case study: A victim's account of a romance scam

Witness A, who is based in Australia, established an online relationship via a dating website with a man claiming to be a citizen of the USA. The man claimed to be travelling to Nigeria to work, after which he proposed to visit Witness A in Australia. Over the following months the man claimed to have run into a range of difficulties while in Nigeria and repeatedly asked for assistance in the form of money transfers and the provision of valuable goods. Witness A was suspicious of these requests, but felt emotionally compelled to assist their 'partner' to travel to Australia. Witness A lost AUD$20,000 before becoming aware that they were being victimised, and suffered significant emotional distress as a result of the scam.

Source Witness A, *Transcript of Evidence*, 17 March 2010, pp.2-4.

2.44 Perpetrators may use other cyber crime tools to fashion and disseminate online scams. For example, a cyber criminal may use seemingly inconsequential information gained from a spyware program, such as an address or friends' names, to make a personalised and highly convincing scam email. Additionally, a cyber criminal may seek to reach a wide number of victims by sending out a scam in a spam email.

---

42 Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, p.19.

43 See for example: AIC, *Submission 41*, p.4; Mr Scott Gregson, Australian Competition and Consumer Commission (ACCC), *Transcript of Evidence*, 18 November 2009, p.1; ACCC, *Exhibit 16*, p.10.

Extortion

2.45 Cyber criminals carry out online extortion via DDoS attacks and specially designed malware.

2.46 Cyber criminals may threaten to carry out a DDoS attack on a business' website if they don't pay a fee. This is particularly the case with businesses that are wholly reliant on their website, such as online gambling companies. For example, in 2006 three Russian nationals were found guilty of, among other offences, carrying out a DDoS attack on an Australian gambling website when the company refused to pay $10,000 in extortion money. The DDoS attack shut down access to the gambling website and was said to have cost the gambling company $200,000 in lost revenue.[44]

2.47 Additionally, a virus, worm or trojan may be designed to automatically encrypt the data on an infected computer. The cyber criminal will then demand money from the victim in return for the 'key' with which to unencrypt the data.[45]

Underground cyber crime forums and websites

2.48 Cyber criminals utilise online forums and websites in order to communicate and trade. These websites or forums are often run purely for the purpose of facilitating cyber crime, and may be hosted on hijacked bot computers. This issue is discussed further in the section on the cyber crime industry below.[46]

Money laundering techniques

2.49 Financially motivated criminals use the online environment to launder illicit money received through other cyber crime activities. A variety of techniques exist for online money laundering including the use of money mules and 'virtual' currencies from online games.

2.50 Money mules are often benign Internet users, recruited via websites set up to lure users into applying for work-from-home jobs as a 'financial officer'. They receive funds into their bank account from cyber criminals, withdraw the money in cash and send the money back to the cyber

44 KR Choo, *Trends and issues in crime and criminal justice: Zombies and Botnets*, AIC, Canberra, 2007, p.4.

45 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.16.

46 Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, p.9.

criminals via a wire transfer service. By withdrawing the money in cash, the sum of money becomes very hard to trace. In return for this service the mule is given a commission by the cyber criminal.[47]

2.51 The Northern Territory Government suggested that immediate wire transfer services such as Western Union were one of the main methods for mules to transfer illicit cash.[48]

2.52 Many online games have a virtual economy by which online players can exchange items within the game for virtual currencies. A gamer may pay real world dollars to receive a certain amount of the virtual currency for use in the game. A money launderer may purchase virtual currency using illicit cash, then exchange the virtual currency back into real world cash, thus reducing the traceability of the illicit funds.[49]

Interrelatedness of cyber crime techniques and tools

2.53 The different tools and techniques of cyber crime cannot be viewed in isolation. Below is a brief summary of some key relationships:

- malware can create botnets which in turn may scan other systems for vulnerabilities and infect other computers with malware;
- botnets may be used to send spam, which in turn delivers malware and extends the botnet;
- malware may steal personal information which may then be used to create and disseminate spam, phishing schemes and scam emails; and
- botnets (through fast fluxing) may perpetuate the hosting of malicious websites which facilitate further cyber crime such as phishing websites, mule recruitment websites or underground cyber crime forums.

The cyber crime industry

2.54 Australian governments, businesses and home-users are being targeted by a highly organised cyber crime industry. Below is a brief description of the emergence and operation of the cyber crime industry and an examination of its ramifications for cyber crime more generally.

47 Australian Broadcasting Corporation (ABC), *Fear in the Fast Lane*, Four Corners program transcript, ABC, 17 August 2009, viewed 11 January 2010, <http://www.abc.net.au/4corners/content/2009/s2658405.htm>; Australian Bankers' Association, *Submission 7.1*, p.2. See also: Mr John Geurts, *Transcript of Evidence*, 8 October 2009, p.57; Mr Craig Scroggie, *Transcript of Evidence,* 9 October 2009, p.54-55.

48 Northern Territory Government, *Submission 53*, p.1.

49 AIC, *Submission 41,* p.8-9.

The emergence and operation of the cyber crime industry

2.55 The current cyber crime industry is driven by an underground cyber crime market place. Due to an increased number of people looking to commit cyber crime, and a resulting increased demand for cyber crime tools and services, an underground market has emerged where cyber criminals may purchase and supply cyber crime goods (such as pre-packaged malware and stolen information) and services (such as spamming or DDoS attack services). This market is often referred to as the underground cyber crime economy.[50]

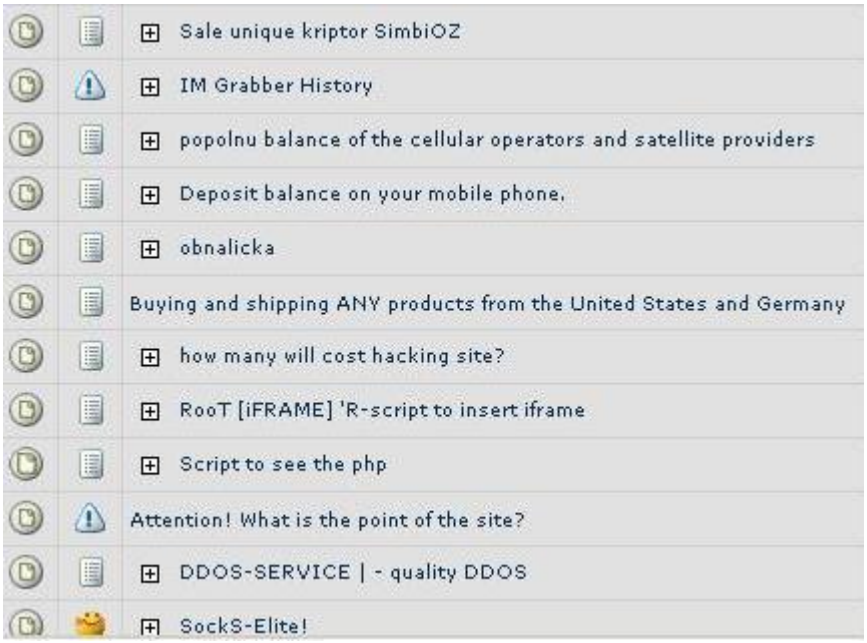
2.56 The trade that occurs in this underground market is often carried out on online cyber crime forums. In order to evade law enforcement, these forums are often hidden and require membership. Detective Superintendent Brian Hay from the Queensland Police Service described these forums as 'an Aladdin's cave of criminality'.[51]

2.57 Figure 2.4 below shows a screenshot from an online cyber crime forum. The row second from the bottom shows a cyber criminal advertising a DDoS attack service, while the sixth row from the bottom shows a potential cyber criminal inquiring as to the cost of having a website hacked.

50 See for example: Internet Safety Institute, *Submission 37*, p. 7; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.16; AFP, *Submission 25*, pp.4,6; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.8.

51 See for example: Detective Superintendent Brian Hay, quoted in ABC, *Fear in the Fast Lane*, Four Corners program transcript, ABC, 17 August 2009, viewed 11 January 2010, <http://www.abc.net.au/4corners/content/2009/s2658405.htm>; Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, pp.4-5; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.8; Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.55.

Figure 2.4 Screenshot of an online cyber crime trade forum



Source Panda Security, *Cybercrime… for sale*, blog post, Panda Security Forum, 24 April 2007, viewed 13 January 2010, <http://support.pandasecurity.com/forum/viewtopic.php?f=16&t=608>.

2.58 The *Symantec Global Internet Security Threat Report: Trends for 2008* listed the most commonly traded cyber crime goods and services, and the prices of these goods and services, as observed by Symantec during 2008. Included were credit card information (trading at between US$0.06 to US$30 per card), full identities (trading at between US$0.70 to US$60) and scam design and delivery services (US$5 to US$20 for design, US$2.50 to US$100 per week for scam website hosting).[52]

2.59 Forums such as these constitute an integral part of the underground economy through enabling goods and services to be easily traded anywhere around the world.[53]

2.60 Ultimately, the emergence of this market place has resulted in the formation of a cyber crime industry where each cyber criminal may provide a discrete input in the process of targeting end users. For example, a spammer may charge a fee for disseminating an email that provides a

52 Symantec Corporation, *Symantec Global Internet Security Report Trends for 2008,* Symantec Corporation, April 2009, p.10.

53 See for example: Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, pp.4-5; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.16; AIC, *Submission 41*, p.7.

link to a phishing site, but may not be involved in running or profiting from the phishing website itself.[54]

The cyber crime industry and the evolution of cyber crime

2.61 The cyber crime industry has caused cyber crime more generally to evolve in a range of ways.

2.62 The large financial incentives provided by the underground cyber crime economy drive a development and testing process which leads to high quality malware that evades new anti-malware defences and avoids detection by Internet security companies thus increasing its profitability.[55]

2.63 Similarly, the market for malware has driven malware to become more user-friendly. Cyber criminals produce pre-packaged off-the-shelf style software packages (known as toolkits) which allow users to commit cyber crime acts (such as infiltrating a system with spyware or creating a botnet) with minimal technical knowledge.[56]

2.64 Figure 2.5 shows a screenshot from a popular toolkit called the 'Zeus Crimeware Toolkit' which enables entry-level cyber criminals to create their own botnets.[57]

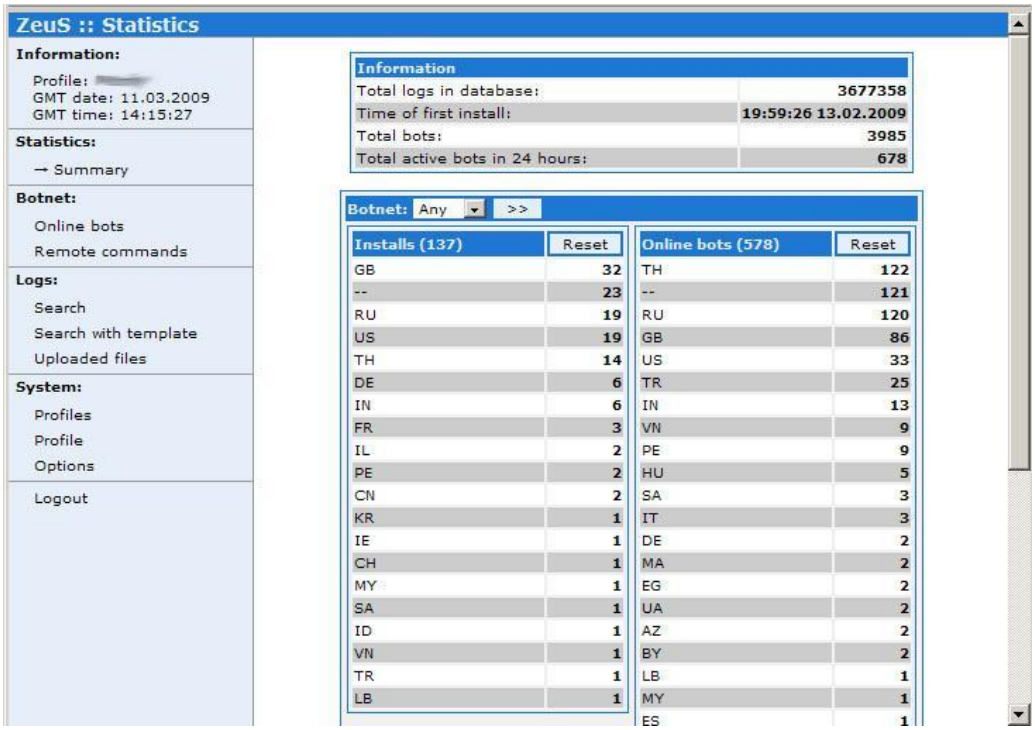
54 See for example: Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.54; Dr Russell Smith, AIC, *Transcript of Evidence*, pp.6-9; AIC, *Submission 41*, p.9.

55 See for example: Internet Safety Institute, *Submission 37*, p. 7; Mr David Zielezna, ACMA, *Transcript of Evidence*, 21 October 2009, p.5; Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.14.

56 Symantec Corporation, *Web Based Attacks February 2009*, Symantec Corporation, February 2009, p.10.

57 P Coogan, Zeus, *King of the underground crimeware toolkits*, blog post, Symantec Security Blogs, Symantec Corporation, 25 August 2009, viewed 14 January 2009, <http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>.

Figure 2.5 Screenshot of 'Zeus Crimeware Toolkit'



Source P Coogan, *Zeus, King of the underground crimeware toolkits*, blog post, Symantec Security Blogs, Symantec Corporation, 25 August 2009, viewed 14 January 2009 ,<http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>.

2.65 This toolkit enables unskilled cyber criminals to create their own tailored botnets through the use of an automated trojan to exploit computer vulnerabilities. As can be seen, the toolkit provides an up-to-date country-specific summary of the number of computers that are infected, the number of bot computers that are online and a 'remote commands' option through which the botnet can be directed. [58]

2.66 The lucrative cyber crime economy has also driven criminals to move from committing large indiscriminate cyber attacks to committing several smaller targeted and low level attacks in order to avoid detection by Internet security and law enforcement organisations.[59]

2.67 Finally, the underground cyber crime economy has led cyber criminals to increase the efficiency of the links between different areas of cyber crime

58 P Coogan, Zeus, *King of the underground crimeware toolkits*, blog post, Symantec Security Blogs, Symantec Corporation, 25 August 2009, viewed 14 January 2009, <http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>.

59 See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.20; Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3.

(such as the links between scam operators and money launderers) to the point where organised criminal networks have emerged.[60]

2.68 Below is a case study that provides an example of a cyber attack on German banks which incorporates all of the above mentioned aspects of the cyber crime industry.

Case study: German example of the operation of the cyber crime industry

In August 2009, a group of coordinated cyber criminals first purchased a toolkit from an online cyber crime forum. This toolkit was then used to infect legitimate and fake websites with a trojan. When a user visited one of the infected websites the trojan would automatically install on the visiting computer. When this infected computer was used for online banking, the trojan would store the details. The trojan was then instructed to automatically log into the bank account and transfer money to a money mule's bank account for laundering. The trojan was automated to only transfer small amounts of money to avoid detection by banks' anti-fraud systems. This operation ran for two weeks and generated almost €1200 per day.

Source Finjan Malicious Code Research Centre, *Cybercrime intelligence report*, Issue 3, Finajn Malicious Code Research Centre, 2009.

Who commits cyber crime?

2.69 A variety of different people commit cyber crime including individual hackers, organised crime groups, corrupt company employees and foreign intelligence operatives.[61]

2.70 Witnesses suggested that, currently, perpetrators of cyber crime tend to be financially-motivated organised criminal networks with decentralised and flexible structures, and consisting of members from a variety of different countries. The majority of these attacks are said to originate from outside of Australia.[62]

2.71 Organised cyber criminal networks differ from traditional 'real world' organised crime groups in that there is not necessarily a hierarchical structure where all cyber attacks committed through the network are

60 AFP, *Submission 25*, p.4.

61 See for example: Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.47; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.11.

62 See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, p.9; AFP, *Submission 25*, p.3.

coordinated from the top. These criminal networks have a decentralised structure where members are anonymous and relatively independent. When a cyber criminal, or group of cyber criminals, wishes to commit a cyber attack, they may use the network to source the resources and skills for that particular operation.[63]

2.72 These cyber crime networks may consist of members from many different countries. The Committee heard that most cyber attacks appear to originate from America, China, Europe and Russia. It was also stated that organised criminal networks are appearing in South-East Asia. It was suggested that cyber criminals may find it easier to operate in countries were governmental institutions or the rule of law is not as strong, or where cyber crime makes a significant contribution to the growth of a developing economy.[64]

2.73 Cyber crime networks also target users from other countries in order to take advantage of traditional law enforcement boundaries that make it much harder for their crime to be investigated.[65]

Who are the victims of cyber crime?

2.74 All aspects of Australian society including Australian government, private businesses and home users, are victimised by cyber criminals.[66]

2.75 Australian governments, whether federal, state or territory, are potential targets of cyber attacks. Cyber attacks may target governments for a variety of reasons including to conduct protests or for cyber espionage. However Governments are also increasingly being targeted by financially motivated cyber criminals.[67] Government agencies are increasingly using the Internet to provide information to, and exchange information with, the public. This makes government organisations a target for financially-

63 AFP, *Submission 25*, p.3.

64 See for example: Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.61; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.7; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009; Mr Richard Johnson, Westpac Banking Corporation, *Transcript of Evidence*, 8 October 2009, p.56.

65 See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.20; Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.20.

66 See for example: AusCERT, *Submission 30*, p.4; AGD, *Submission 44*, p.3.

67 See for example: Australian Taxation Office (ATO), *Submission 59,* p.4; Australian Seniors Computers Clubs Association (ASSCA), *Submission 63*, p.5; Mr Michael Cranston, ATO, *Transcript of Evidence*, 16 September 2009, p.2; Lockstep, *Submission 36*, p.10; AusCERT, *Submission 30*, p.9.

motivated cyber attacks aimed at illegally obtaining funds or information, illustrated in the case study below.[68]

Case study: Fake Australian Taxation Office phishing website hosted in Ukraine

The ATO reported that recently a number of Australian tax payers had been lured to a fake website hosted in Ukraine. The website, a mirror image of the ATO's legitimate website, asked visitors to enter a range of personal details in order to receive a tax refund of $9500. ATO submitted that this website was aimed at harvesting passwords and credit card numbers.

Source Australian Taxation Office, *Submission 58*, p.5.

2.76 Similarly, Australian businesses, whether small, medium or large organisations, are potential targets of cyber crime. Australian businesses may be the target of a variety of attacks including online fraud, theft of information and extortion.[69]

2.77 Home users are also vulnerable to cyber attacks due to low levels of online security. Cyber criminals seek information and money from home users through the use of scams, phishing schemes and malware. Due to their low level of security, home computers are highly vulnerable to being recruited to botnets.[70] Additionally, home users that fall victim to an online scam are more likely to be targeted by further scams. Cyber criminals note users who have responded to scams and place them on a 'sucker list' which may then be used to distribute further scams to these vulnerable home users.[71]

2.78 As the Internet is a resource shared among several different sectors of society, attacks on one section of Australian society may have flow on

68 See for example: ATO, *Submission 59,* p.4; ASSCA, *Submission 63*, p.5; Mr Michael Cranston, ATO, *Transcript of Evidence*, 16 September 2009, p.2; Lockstep, *Submission 36*, p.10; AusCERT, *Submission 30*, p.9.

69 See for example: Mr Christopher Hamilton, *Transcript of Evidence*, p.71; Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p. 52; Symantec Corporation, *Submission 32*, p.9; KR Choo, *Trends and issues in crime and criminal justice: Zombies and Botnets*, AIC, Canberra, 2007, p.4; ABC, *Fear in the Fast Lane*, Four Corners program transcript, ABC, 17 August 2009, viewed 11 January 2010, <http://www.abc.net.au/4corners/content/2009/s2658405.htm>.

70 AFP, *Submission 25*, p.5; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.13; ACCC, *Submission 46*, p.4; Mrs Nancy Bosler, ASSCA, *Transcript of Evidence*, p.1; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.14.

71 Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.14.

effects for other areas of society.[72] For example, due to the vulnerability of home users, botnets are often comprised predominantly of home computers. These botnets can then be used to launch attacks against businesses and governments.[73]

Prevalence of Cyber Crime

2.79 Witnesses emphasised that while the majority of Internet activity is legitimate, cyber crime has touched a significant number of Australians and is growing.[74]

2.80 This section examines the current level of cyber crime both globally and in Australia, and the current trends of cyber crime.

2.81 There is a wide variety of often incomparable information on cyber crime, all of which inevitably suffers from some degree of inaccuracy. However, despite these variations and inaccuracies, all information supports the same conclusion: cyber crime is highly prevalent and is growing at an increasing rate.[75]

Current level of cyber crime threat

2.82 Tables 2.2 and 2.3 below summarise the statistics made available to the Committee, including global statistics and statistics that focus solely on Australia.

72 Mr Anthony Burke, Australian Bankers Association NSW Inc, *Transcript of Evidence*, 8 October 2009, p.62.

73 AFP, *Submission 25*, p.5.

74 See for example: Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.16.

75 Mr Alistair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.63; ACMA, *Submission 56*, p.4.

Table 2.2 Global statistics illustrating the high incidence of cyber crime

Global statistics
Hacking
- In 2008, Verizon observed the compromise of over 180 million business records due to hacking.
Malware
- Symantec has detected a total of approximately 2.6 million different malware programs, 60 per cent of which were detected in 2008.
Malware infections via legitimate websites
- A 2007 study of 4.5 million web pages by Google found that one out of every ten websites contains malware.
Botnets
- McAfee estimates that nearly 40 million computers were recruited to botnets in the first three quarters of 2009.
- The Internet Society of Australia submitted that estimates of the number of bot computers range from five percent of all computers connected to the Internet (over 20 million) to twenty five per cent of all computers connected to the Internet (over 250 million).
DDoS attacks
- Telstra submitted that the size of the largest DDoS attacks increased a hundredfold between 2001 and 2007, from 0.4 gigabits per second to 40 gigabits per second.
Cyber crime industry
- Verizon reports that 91 per cent of the data breaches it observed in 2008 were linked to organised criminal networks.
Phishing and spam
- In the year 2008, Symantec observed 349.6 billion spam messages across the Internet.
- Symantec claim that in 2008 approximately 90 per cent of spam was sent via botnets.
- The Anti-Phishing Working Group, an international consortium of organisations against phishing, identified over 210 thousand unique phishing websites in the first half of 2009.

Source Verizon Business, *2009 Data Breach Investigations Report, Verizon Business*, 2009, p.2; Australian Communication and Media Authority, *Submission 56*, pp.4,7; Symantec Corporation, *Symantec Global Internet Security Threat Report: Trends for 2008*, Symantec Corporation, April 2009, pp.10,16,90 ; McAfee Inc, *McAfee Threats Report Third Quarter 2009*, McAfee Inc, 2009, p.3; Internet Society of Australia, *Submission 45*, pp.3-4; Telstra, *Submission 43.1*, p.2; Anti-Phishing Working Group, *Phishing Activity Trends Report: 1st Half 2009*, APWG, 2009, p.3; BBC News, *Google searches web's darkside,* online news article, 11 may 2007, viewed 19 January 2009, <http://news.bbc.co.uk/2/hi/technology/6645895.stm>.

Table 2.3 Australian statistics illustrating the incidence of cyber crime

Australian statistics
Malware
- A 2008 AusCERT survey of 1,001 Australian adults reported that 23 per cent of respondents had confirmed malware infections on their home computers.
- A September 2009 ACCAN survey of 141 Australian home users indicated that one in five respondents had been a victim of cyber crime.
Botnets
- On average over the 2008-09 financial year, ACMA received 4,291 reports per day of Australian computers infected with botnet malware.
- ACMA submitted that the number of Australian computers recruited to botnets in June 2009 may have been considerably greater than 10,000 computers per day.
Scams
- The ACCC received 12,000 online scam complaints in the 2007-08 financial year.
- Eighty-six per cent of respondents to a 2009 online survey by the Australian Consumer Fraud Taskforce claimed to have been invited to participate in a scam, 73 per cent of whom were targeted via email.
Businesses targeted
- The Australian Institute of Criminology report that fourteen per cent of Australian businesses experienced one or more computer security incidents in the 2006-07 financial year.
Online credit card and bank card fraud
- The 2007 Personal Fraud Survey by the Australian Bureau of Statistics (ABS) inferred that, in the twelve months prior to the survey, 76,000 Australians were the victim of online credit card or bank card fraud.
- The Australian Payments Clearing Association report that in the 2007-08 financial year the Australian payments industry, including banks and credit unions, lost $63.5 million due to online credit card and bank card fraud.
Phishing and spam
- The 2007 Personal Fraud Survey by the ABS estimated that, in the twelve months prior to the survey, 30,400 Australians were the victim of online phishing scams.
- The Commonwealth Bank of Australia receives 3,000 spam and phishing related reports per day, with the highest reporting period being May last year when 30,000 reports were being received per day.

Source Australian Communication and Media Authority, *Submission 56*, pp.4,7; Australian Competition and Consumer Commission, *Submission 46*, p.3; Internet Society of Australia, Submission 45, pp.3-4; K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, Australian Institute of Criminology, 2009, p.xi; Australian Bureau of Statistics, *2007 Personal Fraud Survey*, ABS, Cat. No. 4528.0, 2007, pp.14, 21; Australian Payments Clearing Association, *Submission 50*, p.5; Mr John Geurts, Commonwealth Bank of Australia, *Transcript of Evidence*, 8 October 2009, p.59; J Dearden, *Comparing the 2008 and 2009 ACFT online survey results*, powerpoint presentation at Australian Consumer Fraud Taskforce Forum 2009, 8 October 2009, p.8; AusCERT, *AusCERT Home Users Computer Security Survey 2008,* AusCERT, 2008, p.3.

2.83 These statistics, whilst varying and sometimes imprecise, provide a number of insights into the current level of cyber crime:

- globally, malware and botnets are widespread and facilitate significant DDoS attacks, data breaches and phishing schemes;
- globally, it is very common for trusted and legitimate websites to be inadvertently hosting and propagating malware;
- a significant number of Australian computers are infected with malware and are part of botnets; and
- a significant number of Australian businesses and home users are the target of online scams, phishing schemes and identity fraud.

2.84 It can be seen that cyber crime is highly prevalent and directly affects a significant number of Australians.[76]

2.85 In 2006 and 2008 the Department of Broadband, Communications and the Digital Economy (DBCDE) commissioned KPMG to carry out cyber security threat and vulnerability assessments for home users and small businesses.[77] These reports are not publicly available. However ACMA informed the Committee that there are potentially tens of thousands of compromised Australian computers.[78]

2.86 These concerns were reiterated to the Committee by Mr Mike Rothery, the First Assistant Secretary, National Security Resilience Policy Division, Attorney General's Department (AGD):

> We are concerned that there are many thousands of compromised machines out there … in many cases … being used as part of botnets to do other things—launch spam attacks, denial of service, phishing attacks and a whole range of things, … many tens of thousands.[79]

The outlook for cyber crime in Australia

2.87 Throughout the inquiry witnesses continually reinforced to the Committee that cyber crime is a rapidly evolving phenomenon. The Committee heard that the cyber crime industry, driven by the lucrative underground cyber

76 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.15.

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

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

79 Mr Mike Rothery, AGD, *Transcript of Evidence*, 25 November 2009, p.10.

crime economy, will continue to adapt in order to exploit new technologies and in order to respond to new anti-cyber crime measures.[80]

2.88 Mr Graham Ingram, General Manager of the Australian Computer Emergency Response Team (AusCERT), summarised the outlook for cyber crime in Australia:

> [Cyber crime in Australia] is getting out of control and we are losing. And I think that, with the pressures coming on us over the next few years, if nothing is done to change the current direction we will lose faster.[81]

2.89 The future of cyber crime in Australia can be predicted by observing a range of trends in Internet and technology use, malware and cyber attacks.

2.90 During the inquiry a range of trends in Internet and technology usage were viewed as increasing the prevalence of cyber crime. For example, witnesses argued that the increased uptake of high speed 'always on' broadband services will increase the threat of cyber crime in Australia (a 2009 ABS survey estimated that Australian household broadband connections grew 18 per cent to 5 million during 2008-09).[82] Similarly, the Committee heard that the uptake of new computer systems, software and hardware (such as cloud computing, social networking and wireless systems) will lead to new vulnerabilities.[83] An additional concern was that as technologies become more user-friendly, computer users will require less computer knowledge and will therefore be more vulnerable to cyber crime.[84]

---

80 See for example: Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009 p.3; Mr Graham Ingham, AusCERT, *Transcript of Evidence*, 11 September 2009, p.11; Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.14; Mr Richard Johnson, Westpac Banking Corporation, *Transcript of Evidence*, 8 October 2009, p.56; Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.47.

81 Mr Graham Ingham, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3.

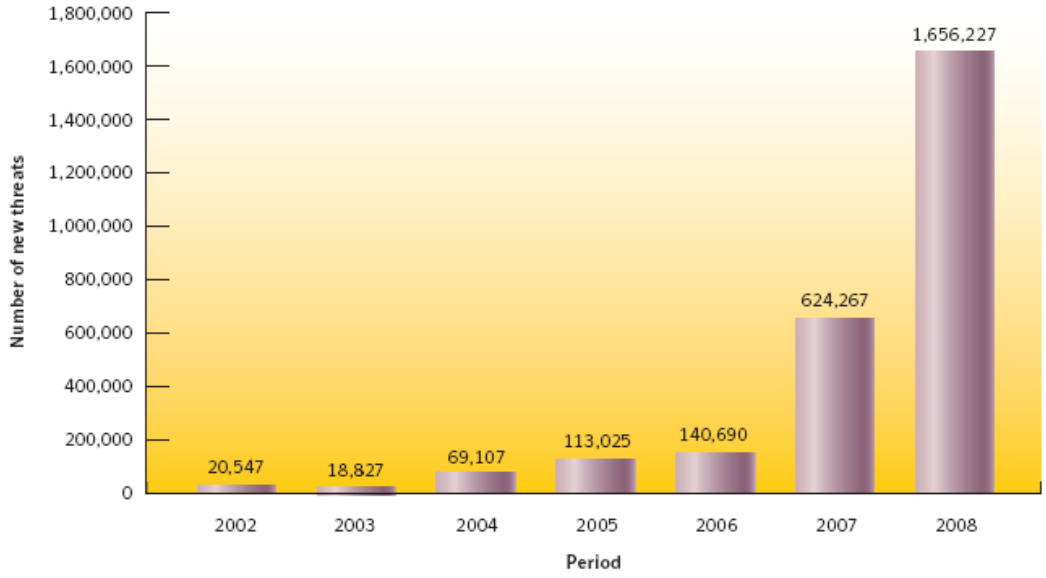
82 See for example: Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3; Mr Peter Coroneos, IIA, *Transcript of Evidence,* 11 September 2009, p.22; Internet Safety Institute, *Submission 37*, p.4; Mr Anthony Burke, Australian Bankers Association NWS Inc., *Transcript of Evidence*, 8 October 2009, p.55; Mr Terry Hilsberg, ROAR Film Pty Ltd, *Transcript of Evidence*, 8 October 2009, p.66; Mr John Galligan, Microsoft Pty Ltd, *Transcript of Evidence*, 9 October 2009, Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.15; ABS, *Household Use of Information Technology 2008-09*, ABS, Cat. No. 8146.0, 16 December 2009, p.37.

83 Mr Graham Ingham, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3; ATO, *Submission 59*, p.6; ROAR Film Pty Ltd, *Submission 64*, p.5; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.5; McAfee Australia, *Submission 10*, p.2.

84 Microsoft Australia, *Submission 35*, p.4.

2.91 Trends in malware were also identified as an area of concern. For example, Symantec reported that malware is being produced at an ever increasing rate (refer to Figure 2.6), with detected malware levels jumping 60 per cent in 2008.[85] Additionally it was argued that cyber criminals are increasingly propagating malware via popular and trusted websites[86], and that this malware is increasingly surreptitious, specialised and targeted.[87] The Committee also heard that botnets continue to grow (refer to Figure 2.7) and are likely to become more versatile in exploiting new vulnerabilities and in responding to anti-botnet measures.[88]

Figure 2.6 Number of new malware programs detected globally per year, 2002 to 2008



Source Symantec Corporation, *Symantec Global Internet Security Threat Report: Trends for 2008*, Symantec Corporation, April 2009, p.10.

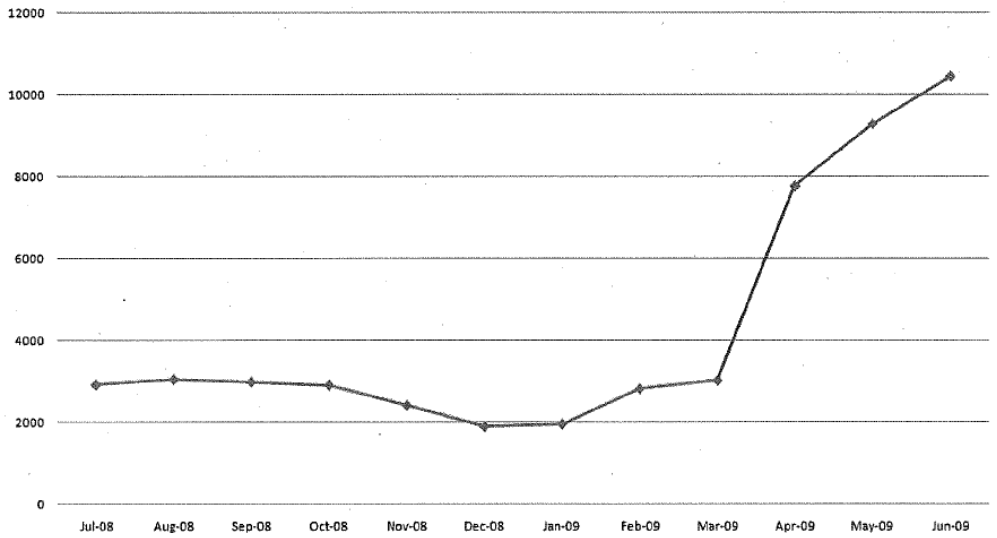
85 Symantec Corporation, *Symantec Global Internet Security Threat Report: Trends for 2008*, Symantec Corporation, April 2009, p.10.

86 See for example: Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.7; Mr Bruce Matthews, ACMA, *Transcript of Evidence*, p.5.

87 Telstra, *Submission 43*, p.2.

88 The ICANN, *Submission 40*, p.1.

Figure 2.7 Average number of IP addresses that are part of botnets reported to ISPs via ACMA's Australian Internet Security Initiative per day July 2008 to 2009



Note: AISI figures do not accurately identify how many Australian computers are compromised due to multiple computers that operate under the same IP address and due to computers that may be missed or not identified during the reporting process. ACMA submits however that the number of Australian computers compromised is likely to be considerably greater than shown in AISI reports.

Source Australian Communication and Media Authority, *Submission 56*, p.5.

2.92 Other acts of cyber crime were also said to be increasing. Submitters stated that organised cyber criminals are committing increasingly low profile attacks against identified vulnerable users including small businesses, home users and prior scam victims.[89] Also, it was argued that as the cyber crime industry supplies increasingly user-friendly malware and skilled hackers-for-hire, the skills needed to carry out complex cyber attacks will gradually decrease.[90] The Committee also heard that cyber criminals are increasingly targeting victims in other countries in order to reduce their risk by taking advantage of jurisdictional barriers to law enforcement investigations.[91]

2.93 Mr Alistair MacGibbon, Director, Internet Safety Institute, told the Committee that cyber criminals have, and continue to compile, large stockpiles of stolen information but are not efficient at converting this stolen information into money. Mr MacGibbon stated that his main fear is

89 See for example: AIC, *Submission 41*, pp.2-3; AFP, *Submission 25*, p.3; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.13; Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.52; DBCDE, *Submission 34*, p.3.

90 See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.30; ACS, *Submission 38*, p.6.

91 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.30.

that cyber criminals will improve their techniques for monetising this information thus leading to a new wave of cyber attacks.[92]

Economic impact of cyber crime

2.94 Cyber crime has many current and potential negative economic impacts on Australians. Contributors to the inquiry outlined a range of ways in which cyber crime threatens the Australian economy:

- widespread cyber crime may undermine confidence in aspects of the digital economy thus inhibiting the growth of the Australian economy;
- continued cyber attacks against particular businesses may damage their reputation and result in a loss of customers and revenue;
- the development of measures to combat and respond to cyber attacks imposes a significant cost on businesses;
- cyber attacks cause direct financial losses to consumers and businesses resulting from the theft of information and money, or extortion; and
- cyber attacks targeting Australia's critical infrastructure may lead to immediate and long term economic losses.

2.95 These impacts are described below.

Economic loss from diminished confidence in Australia's digital economy

2.96 Australia's economy is currently benefiting from the increased development and use of new information and communication technologies. This area of our economy is referred to as the 'digital economy'. DBCDE define the digital economy as:

> The global network of economic and social activities that are enabled by information and communications technologies, such as the Internet, mobile and sensor networks.[93]

2.97 The digital economy consists of devices such as computers and phones as well as the infrastructure that enables the sharing of information such as telephone lines and mobile phone towers. The digital economy enables all aspects of Australian society to carry out a range of activities with increased ease and efficiency such as accessing government information,

92 Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.69.

93 DBCDE, *Australia's Digital Economy: Future Directions*, DBCDE, 2009, p.2.

conducting financial transactions or communicating in real time with geographically distant friends or family.[94]

2.98 Ultimately, the digital economy opens up new opportunities for the Australian economy as a whole to increase its efficiency and to grow.[95]

2.99 Many contributors to the inquiry warned of the significant negative economic impact which would be caused by cyber crime undermining confidence in Australia's digital economy.[96] Ms Loretta Johnson, General Manager, Policy and Government Relations, Australian Information Industry Association (AIIA), provided a summary of this concern:

> The productivity, efficiency and economic growth advantages that can be delivered by our rapidly developing digital infrastructure are recognised by governments and users alike. The secure and safe use of that infrastructure should be a focus for governments which are concerned with enhancing their nation's GDP for the benefit of their own citizens. If that focus is lost, users will lose confidence in the internet as a business and commercial tool, leading to a consequent decrease in the efficiencies and productivities that digital engagement can deliver.[97]

2.100 It is difficult to quantify the negative economic impact caused by a loss of confidence in online services.[98] However, Mr Paul Kurtz, Executive Director of the US-based Cyber Security Industry Alliance, has suggested that a loss of consumer confidence in the digital environment is a billion dollar problem.[99]

2.101 ACMA's 2009 publication *Australia in the Digital Economy: Trust and Confidence* concluded that, while Australians are aware and concerned about the risks of using the Internet, these concerns do not currently stop

---

94 DBCDE, *Australia's Digital Economy: Future Directions*, DBCDE, 2009, pp.2-3.

95 DBCDE, *Australia's Digital Economy: Future Directions*, DBCDE, 2009, p.1.

96 See for example: AusCERT, *Submission 30*, p.11; IIA, *Submission 54*, p.4; Microsoft Australia, *Submission 35*, p.5; Symantec Corporation, *Submission 32*, p.8; Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.10; Lockstep Technologies Pty Ltd, *Submission 36*, p.10; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.41-42.

97 Ms Loretta Johnson, Australian Information Industry Association, *Transcript of Evidence*, 11 September 2009, p.24.

98 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.7.

99 Cyber Security Industry Alliance, 'Survey: Lack of confidence in cyber security has economic, political effects', *Insurance Journal*, Wells Publishing, June 2006, viewed 29 January 2009, <http://www.insurancejournal.com/news/national/2006/06/07/69215.htm>.

people from using the Internet.[100] However, the 2008-09 ABS *Household Use of Technology Survey* estimated that over one million Australians refrain from purchasing goods or services on line due to concerns over online security or privacy.[101] Similarly, the Australian Communications Consumers Action Network (ACCAN) informed the Committee that they have encountered a large number of consumers who are refusing to use the Internet because of fears they will lose money to cyber crime.[102]

Financial loss to business from damaged reputation

2.102 Where a business is the target of persistent or high-profile cyber attacks, their reputation among clients and share holders may suffer, thus resulting in lower share prices, fewer clients and lower revenues.[103] For example, in January 2009, US-based payment processor Heartland Payment Systems experienced significant divestment which halved its stock price following a malware-enabled data breach which potentially compromised tens of millions of credit and debit card transactions.[104]

Cost of anti-cyber crime measures and cyber crime complaints

2.103 Many private businesses that supply ICT goods and services, or conduct business over the Internet, must direct significant resources towards dealing with cyber crime.[105] A 2009 AIC survey estimated that the annual cost of computer security measures for Australian businesses is between $1.37 billion and AU$1.95 billion.[106]

Direct financial losses to Australian businesses and home users

2.104 Australian businesses and home users continually suffer direct financial losses from cyber crime. Cyber criminals use scams, fraud and extortion to illegally obtain money from these victims. The loss to home users and business is difficult to quantify; however, the AIC estimate Australian

---

100 ACMA, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.1.

101 ABS, *Household Use of Information Technology 2008-09*, ABS, Cat. No. 8146.0, 16 December 2009, p.30.

102 Mr Allan Asher, ACCAN, *Transcript of Evidence*, 8 October 2009, p.16.

103 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.40-41.

104 AM Freed, *Another Payment Card Processor Hacked*, Information Security Resources, Infosec Island Network, February 14 2009, viewed 29 January 2009, <http://information-security-resources.com/2009/02/14/another-payment-card-processor-hacked/>.

105 OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.40-41.

106 K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, AIC, 2009, p.iii.

businesses lost between $595 million and $649 million in the 2006-07 financial year.[107]

Economic loss from disruption to Australia's critical infrastructure

2.105 Australia's national information infrastructure supports a range of computerised control mechanisms that govern other aspects Australia's critical infrastructure. Contributors argued that there is real potential for cyber criminals to highjack, damage or inhibit these systems which in turn could cause longer-term disruptions to economic development.[108]

Committee View

2.106 Cyber crime crosses many technological, conceptual and institutional boundaries, and, through its high prevalence, has real and increasing impacts on many Australians. Australia's public policy response must take account of several key factors:

- organised criminal networks consist of members from, and commit attacks across, several different traditional law enforcement and regulatory jurisdictions thus challenging traditional law enforcement and regulatory methods and procedures;
- cyber crime is rapidly evolving and responsive to anti-cyber crime measures, thus any legislative, regulatory, technological, intelligence and educational initiatives must be kept under constant review;
- the interrelated nature of different aspects of cyber crime makes it important to take a strategic and holistic approach to intervention; and
- the complex nature of cyber crime makes the reporting, gathering and analysis of data and intelligence an important element of the national and international effort to combat cyber crime.

2.107 While it is probably impossible to eradicate all cyber crime (just as it is in the offline environment) it is possible to ensure that Australia maintains an understanding of the threats and builds capacity to prevent cyber attacks. It is clear to the Committee that the many different aspects of

---

107 See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.38; K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, AIC, 2009, p.xi

108 See for example: AIC, *Submission 41*, p.16; Australian Information Industry Association, *Submission 22*, p.9; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.42-43.

cyber crime are interrelated and Australia's response cannot deal with these various aspects of cyber crime in complete isolation.

2.108 The following chapters canvass some of the options for expanding the current national strategy and building a broader, and more integrated response that takes account of the needs of consumers.

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.

4

Community Awareness and Vulnerability

Introduction

4.1 This chapter discusses the current level of e-security awareness among Australian home users and small businesses. The evidence demonstrates a considerable inconsistency between levels of awareness of e-security threats and actual online behaviour, indicating that home users and small businesses remain highly vulnerable to a range of cyber crime types.

Levels of Awareness and Uptake of E-security Measures

4.2 As mentioned previously in this report, there is a wide variety of inconsistent and often incomparable information on the level of cyber crime activity due to varying definitions of cyber crime, fragmented intelligence gathering and the under reporting of cyber crime by victims.[1]

4.3 These data collection issues have also given rise to a number of conflicting statistics on the level of cyber crime awareness in the Australian community. While some sources indicate that the level of awareness is high, other sources show that this does not necessarily translate into better online practices.

4.4 Evidence to the Committee supports the notion that home users have some awareness of cyber security risks:

---

1 Mr Alistair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.63.

- a July 2009 Australian Communications and Media Authority (ACMA) survey of Australian home users between the ages of eight and seventeen found that 75 per cent of respondents knew not to divulge personal details on the internet;[2]
- a March 2009 ACMA survey of 1,631 adult home users found that 81 per cent of respondents assessed their online skills as average or above;[3]
- a 2008 survey by internet security provider AVG found that 77 per cent of Australian respondents were aware of the need to regularly update their internet security software; [4]
- a 2006 survey by the Consumers' Telecommunications Network (CTN) found that almost 90 per cent of respondents were aware of and understood spam, and more than 66 per cent of respondents were aware of and understood malware;[5] and
- the same 2006 CTN survey found the 75 per cent of respondents recognised and did not respond to scam emails.[6]

4.5 The evidence also suggested that Australian small businesses possess some understanding of cyber security issues:

- a 2009 global survey by Symantec of 1,425 small and medium sized enterprises (SMEs) found that these businesses are acutely aware of today's security risks;[7]
- a 2009 ABS survey of Australian small businesses found that 85 per cent of respondents used one or more computer security tools such as anti-virus or encryption software;[8] and
- a 2006 AusCERT survey of Australian organisations found that 99 per cent used virus protection and 98 per cent used firewalls.[9]

---

2 ACMA, *Click and connect: Young Australians' use of online social media – 02: Quantitative research report*, ACMA, July 2009, p.10.

3 ACMA, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.29.

4 AVG, *Australia Tops Global Cyber Crime Impact Survey*, media release, AVG, 10 June 2008, viewed 21 January 2010, <http://www.avg.com.au/news/avg_cyber_crime_impact_survey/>.

5 Consumers' Telecommunications Network (CTN), *Surfing on thin ice: consumers and malware, adware, spam and phishing*, CTN, November 2009, p.9.

6 Consumers' Telecommunications Network, *Surfing on thin ice: consumers and malware, adware, spam and phishing*, CTN, November 2009, p.33.

7 Symantec Corporation, *Submission 32*, p.9

8 K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, Australian Institute of Criminology, 2009, p.xii.

9 AusCERT, *Computer Crime and Secuirty Survey*, AusCERT, 2006, p.8.

4.6 However, a range of other evidence indicated that Australian home users and small businesses still take insufficient precautions against cyber crime.[10] This evidence includes, for example:

- a March 2009 ACMA survey of 1,631 adult home users found that only 49 per cent of those who assessed their online skills as high had installed anti-virus software;[11]
- a 2008 AusCERT survey of 1,001 Australian adult home users found that 11 per cent of respondents never update their operating system and eight per cent never update their anti-virus software; [12]
- the 2008 AusCERT survey also found that 75 per cent of respondents connect to the internet using an administrator account and 30 per cent had clicked on links in spam emails (both of which significantly reduce the effectiveness of computer security mechanisms);[13]
- the 2009 Symantec survey of SMEs found that out-of-date or improper security measures each accounted for over a third of the security breaches against Australian SMEs;[14] and
- only ten per cent of respondents to a 2006 AusCERT survey of Australian organisations thought they were managing all aspects of computer security well.[15]

4.7 The level of cyber crime in Australia demonstrates that end users are not heeding advice on e-security threats. For example, while the Australian banking industry said that customers are highly aware of the threat posed by phishing emails,[16] a 2007 ABS survey estimated that, in the twelve months prior to the survey, 30,400 Australians were the victim of online phishing scams.[17]

---

10 See for example: Australian Computer Society (ACS), *Submission* 38, p.8; Dr Russell Smith, Australian Institute of Criminology (AIC), *Transcript of Evidence*, 19 August 2009, p.9; Mr Peter Coroneos, Internet Industry Association (IIA), *Transcript of Evidence*, 11 September 2009, p.18; Australian Federal Police (AFP), *Submission 25*, p.10; AusCERT, *Submission 30*, p.12.

11 ACMA, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.39.

12 AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

13 AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

14 Symantec Corporation, *Symantec Survey Reveals More than Half of Small and Midsized Businesses in Australia and New Zealand Experience Security Breaches*, media release, Symantec Corporation, 12 May 2009, p.1.

15 AusCERT, *Computer Crime and Security Survey*, AusCERT, 2006, p.4.

16 Mr Anthony Burke, Australian Bankers Association NSW Inc, and Mr John Guerts, Commonwealth Bank of Australia, *Tanscript of Evidence*, 8 October 2009, p.59.

17 Australian Bureau of Statistics (ABS), *2007 Personal Fraud Survey*, ABS, Cat. No. 4528.0, 2007, pp.14, 21.

4.8 Similarly, despite an apparent awareness of the threats posed by identity theft and fraud, the ABS survey estimated that 76,000 Australians were victims of online credit card or bank card fraud in the year preceding the survey.[18]

4.9 Even where end users do take sufficient technical precautions, they may still fall victim to online scams due to emotional vulnerabilities. For example, the ACCC informed the Committee of an increasing number of dating or romance scams.[19] Additionally, the 2006 ABS survey indicated that at least 31,700 Australians were the victims of online scams in the twelve months prior to the survey.[20]

4.10 The continued impact of romance scams provides a particularly good example of how knowledge of cyber crime risks is not necessarily translating into protective actions. The Queensland Police Service (QPS) informed the Committee that, in the case of romance scams, 76 per cent of victims who lost large amounts of money continued to willingly participate in such scams despite being notified by the QPS that they were being victimised.[21] Similarly, Mr Peter Shenwun, Consular Minister, Nigerian High Commission in Australia, told the Committee that many victims of advance-fee fraud originating out of Nigeria seek to continue contact with scammers, despite being advised not to by Nigerian authorities.[22]

4.11 AusCERT argued that the range of seemingly inconsistent evidence indicates that home users may hold misconceptions about the level of protection provided by their security measures. AusCERT's *Home Users Computer Security Survey 2008* found that:

- 68 percent of people were confident or very confident in managing their own computer security;
- 92 per cent thought their ISP should inform customers of malware infections (which does not necessarily occur); and
- 46 per cent incorrectly believed that data exchanged with secure websites cannot be accessed by hackers.[23]

---

18 ABS, *2007 Personal Fraud Survey*, ABS, 2007, pp.14, 21, 24.

19 Mr Scott Gregson, Australian Competition and Consumer Commission (ACCC), *Transcript of Evidence*, 18 November 2009, p.1.

20 ABS, *2007 Personal Fraud Survey*, ABS, 2007, pp.14, 21, 24.

21 Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, pp.3-4.

22 Mr Peter Shenwun, Nigerian High Commission, *Transcript of Evidence*, 17 March 2010, p.1.

23 See for example: AusCERT, *Submission 30*, p.12; AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

4.12 The Tasmanian Government stated that although there appears to be a general awareness in the community of the need for some level of protection, most home users and SMEs do not have adequate security.[24]

4.13 The Australian Computer Society argued that Australians seem to be aware of, and are taking precautions against, old cyber crime threats but are not aware of, or taking steps against, new and emerging cyber crime threats.[25] For example, while users may be installing anti-virus software to combat some e-security risks, QPS informed the Committee that they observed a 1,000 per cent increase in the incidence of romance scams between 2006 and 2009.[26]

Issues that contribute to low levels of awareness

4.14 The Committee received evidence on a number of factors that contribute to the low level of awareness of cyber crime threats among Australia home users and small businesses:

- limitations of current educational initiatives;[27]
- a complex public policy response to cyber crime;[28] and
- inadequate online safety mechanisms that may not alert end users to new cyber security threats and attacks.[29]

4.15 These issues, and proposals to deal with them, are examined more thoroughly in the following chapters.

---

24 Tasmanian Government, *Submission 51*, p.3.

25 ACS, *Submission 38*, p.8.

26 Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, p.4.

27 See for example: Consumers' Telecommunications Network, *Surfing on thin ice: consumers and malware, adware, spam and phishing*, CTN, November 2009, p.21; Internet Safety Institute, *Submission 37*, p.10; Mr Terry Hilsberg, ROAR Film Pty Ltd, *Transcript of Evidence*, 8 October 2009, p.69; Telstra, *Submission 43*, p.4.

28 See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.15; Mr Mike Rothery, Attorney General's Department (AGD), *Transcript of Evidence*, 25 November 2009, p.14; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2; Internet Safety Institute, *Submission 37*, p.8; Fujitsu, *Submission 13*, p.7; IIA, *Submission 54*, p.5.

29 See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.9; Mr Scott Ridgway, ACCC, *Transcript of Evidence*, 18 November 2009, p.7; Dr Paul Brooks, *Transcript of Evidence*, 9 October 2009, p.11; Mr Mike Rothery, AGD, *Transcript of Evidence*, 25 November 2009, p.12.

Committee View

4.16 The Committee considers that the level of awareness of cyber crime threats among Australian home users and small businesses is insufficient to ensure their safety online.

4.17 The Committee is of the view that the vulnerability of Australian home users and small businesses presents a risk to all sections of the Australian community. The insufficient uptake of simple e-security measures means that home users and small businesses will continue to be victimised by cyber criminals. This has direct financial and emotional impacts on the victims themselves, and exposes other sections of Australia's ICT systems to attack, including areas of government.

4.18 Community education and awareness raising is part of the Australian Government's *Cyber Security Strategy*. The adequacy of Australia's current initiatives is examined in Chapter 10.

5

Domestic and International Coordination

Introduction

5.1 This chapter gives a broad outline of the national framework for coordinating cyber crime policy and existing mechanisms for international engagement.

5.2 The chapter concludes that existing coordination mechanisms are heavily weighted toward national security and critical infrastructure. A more centralised and genuinely national approach is required to ensure that strategic responses to cyber crime that impact on the broader Australian society are as effective as possible.

Cyber Security Strategy

5.1 Since 2001 the Australian Government's approach to e-security has been governed by the *E Security National Agenda.* The policy was reviewed in 2004 and 2006. In 2008 a further review was initiated in response to the 'increased level of cyber threat' and rapid growth in the use of information and communication technology, including the roll out of the National Broadband Network.[1] On 23 November 2009 the *Cyber Security Strategy* was launched bringing together a number of existing e-security activities under the umbrella of one policy and introducing some new initiatives.[2]

---

1 AGD, *Submission 44*, p.6.

2 Attorney General Hon Robert McClelland MP; Minister for Broadband, Communications and the Digital Economy, Senator The Hon Stephen Conroy; Minister for Defence, Senator the Hon John Faulkner, Joint Media Release, *Australian Cyber Security Strategy Launched*, 23 November 2009; *Cyber Security Strategy,* Australian Government, p.vi.

5.2 The *Cyber Security Strategy* emphasises the protection of national security, government computer systems and critical infrastructure. There will be a benefit to the public through the increased capacity to protect government computer systems and institutions, such as banks, and public utilities on which the whole community rely. However, the new computer response team, CERT Australia, does not receive complaints about cyber crime or providing technical assistance to the general public or small and medium sized businesses.

5.3 In practice, the *Cyber Security Strategy* retains the previous emphasis on community education so that end users can better protect themselves against online crime. The Committee was told that community education alone is no longer a sufficient response to sophisticated cyber crime activities that impact the whole community. It was argued that there needs to be more importance attached to the needs of consumers and business generally and more strategic approaches to the inter-connected nature of cyber space.[3]

Domestic Policy Coordination

5.4 Under the current arrangements, the Attorney-General's Department (AGD) has primary responsibility for e-security policy across the Australian Government and is the lead agency for identity security and critical infrastructure.[4] The Committee was told that the E-Security Policy and Coordination Committee (ESPaC), a bi monthly interdepartmental committee chaired by AGD, provides a whole of government perspective on e-security policy and coordination.[5]

5.5 Following the *E Security Review* the Committee has been renamed the Cyber Security Policy and Coordination Committee and its membership has been expanded. Membership is now comprised of the:

- Australian Federal Police (High Tech Crime Operations);
- Australian Government Information Management Office;
- Australian Security Intelligence Organisation;
- Defence Signals Directorate;

3 Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.4; Cyber Space Law and Policy Centre, *Submission 62*, p.6.

4 AGD, *Submission 44*, p.2.

5 AGD, *Submission 44*, p.7

- Department of Broadband, Communications and the Digital Economy (DBCDE);
- Department of Defence; and
- Department of the Prime Minister and Cabinet (PM&C).

5.6 The Cyber Security Policy and Coordination Committee:

- provides whole of government strategic leadership on cyber security;
- determines priorities for the Australian Government;
- coordinates the response to cyber security events; and
- coordinates Australian government cyber security policy internationally.[6]

5.7 The Committee formally reports on the progress of its annual work plan to the Deputy National Security Advisor on an annual basis. The Committee also coordinates the 'provision of threat and security environment assessments to the National Security Committee of Cabinet, through the Secretaries Committee on National Security as required'.[7]

National Coordination of Cyber Space Policy

5.8 The evidence demonstrated that Internet activity involves a range of policy areas, including criminal law, privacy, consumer protection, telecommunications, broadcasting, and corporation law. Consequently, there is a plethora of Commonwealth, State and Territory departments and agencies with responsibility for some aspect of the wider problem of cyber crime.

5.9 In relation to policy, AGD has responsibility for criminal law and law enforcement policy but it does not have policy responsibility for cyber safety, privacy or consumer protection.[8] These areas fall variously to DBCDE, PM&C, and Treasury. State and Territory Governments are also responsible for a range of legal policy in criminal law, privacy, education, and consumer protection that impact on cyber crime.

5.10 Federal, State and Territory police forces enforce the laws against cyber crime. In addition, a range of civil regulatory bodies have an enforcement role in relation to different aspects of cyber crime activity:

---

6 *Cyber Security Strategy*, Australian Government, 2009, p.30.

7 AGD, *Submission 44,* pp. 22-23.

8 AGD, *Submission 44*, p.14.

- Australian Communications and Media Authority (ACMA) administers the Australian Internet Security Initiative (botnet detection) and administers the *Spam Act 2003* (Cth);
- the Australian Competition and Consumer Commission (ACCC) hosts the *ScamWatch* website, and takes thousands of complaints of online fraud and scams, which it deals with in the context of misleading and deceptive trade under the *Trade Practices Act 1974* (Cth);
- State and Territory Fair Trade offices deal with these matters under State and Territory law;
- the Federal Privacy Commissioner administers the *Privacy Act 1988* (Cth), which regulates the collection and disclosure of personal information;
- complementary privacy laws are administered by State and Territory Commissioners; and
- corporations are regulated by the Australian Securities and Investment Commission (ASIC) under the *Australian Securities and Investments Commissions Act 2001* (Cth) and the *Corporations Act 200* (Cth).

5.11 Although difficult to avoid, this highly decentralised approach was regarded by some as an impediment to a nationally coordinated and strategic response to tackling the problem of cyber crime. For example, Mr Alastair MacGibbon, Director Internet Safety Institute said:

> … there no single institution in Australia (or for that matter anywhere else in the world) which has a whole-of-internet national view of eSecurity victimisation.[9]

5.12 The Cyber Space Law and Policy Centre (CLPC) said that as a consequence of this fragmentation legal policy and regulatory measures are 'convoluted' and unable to target the interlinked nature of cyber crime and its related activities.[10] The witness doubted whether Australian law could effectively deal with the commission of cyber crimes facilitated through a mix of these activities because 'each one is categorised and dealt with by separate agencies (police, ACMA, and the ACCC) making investigation difficult or impossible'.[11]

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

10 CLPC, *Supplementary Submission 62.1*, p.5.

11 CLPC, *Supplementary Submission 62.1*, p.5.

5.13 Microsoft advocated that Australia consider a more expansive strategy and create a 'cyber Tzar' position located in PM & C and a strategy that engages 'all elements of national power':

> When one recognises the breadth of the challenge and the need for a massively decentralised but coordinated response among the federal, state and territory agencies, we believe that the Committee should consider whether or not Australia's national cyber security strategy and its implementation should be led by a single coordinating authority at the highest Executive level, like the Department of Prime Minister and Cabinet or through an appointed "cyber security czar". As the Committee would be aware, the US is moving to a similar model, where their national cyber security strategy will be led and coordinated by the White House.[12]

5.14 Mr James Shaw, Director, Government Relations, Telstra Corporation Ltd., also advocated a centralised point within government to manage a more coordinated approach:

> At the moment it is dealt with in a variety of areas of government. In their best endeavours they collaborate as best they can. A lot of that, though, is ad doc rather than done in a strategic sense from one point in government with an overall policy strategy agenda.[13]

5.15 To expand the reach of Australia's e-security strategy, Telstra suggested the creation of a National Cyber Crime Advisory Committee 'focussing on strategic leadership and information sharing between public and private sectors, federal, state and local entities'.[14] Such a Committee would comprise independent experts from a range of cyber space related areas, including consumers, to provide best advice on a range of cyber crime issues.[15]

5.16 The Australian Communications Consumer Action Network (ACCAN), also highlighted the need for a 'more coordinated and rigorous approach' to protecting online consumers.[16] It was suggested that Australia should adopt a similar approach to that of the UK and create an Office of Online Security, which can address the 'multitude of economic and social

12 Microsoft Australia, *Submission 35*, p.6.

13 Mr James Shaw, Telstra Corporation Ltd., *Transcript of Evidence*, 11 September 2009, pp.44-45.

14 Telstra Corporation Ltd, *Submission 43*, p.3.

15 Mr James Shaw, Telstra Corporation Ltd., *Transcript of Evidence*, 11 September 2009, p.44.

16 ACCAN, *Submission 57*, p.1.

implications of online security issues'.[17] The UK Office of Cyber Security operates within the Cabinet Office to provide strategic oversight.

5.17 ACCAN suggested that an Australian Office of Online Security should have responsibility for high level policy on cyber security and its impact on consumers, and report at 'Cabinet level on improvements, research and further challenges in cyber security.'[18] The Office could, for example, set benchmarks for preinstalled security features for the sale of computers and work with DBCDE to develop a National Strategy for E-Security Awareness.

5.18 Mr Graham Ingram, Director, AusCERT, advocated a 'cyber space' perspective that integrates the relevant government agencies and clearly identifies the role and responsibilities of ISPs, Domain Name Registrars, and IT companies. He proposed that that these private stakeholders should all be part of a nationally coordinated effort to reduce e-security risks.[19] Similarly, Mr Alastair MacGibbon, Director, Internet Safety Institute, also suggested that private companies, such as ISPs and Domain Name Registrars, have some responsibilities in this area.[20]

5.19 The whole Internet community needs to be brought together:

> We need to have a national response, the same way as if we have a response to a pandemic. We need everyone to know what they are doing and having it coordinated. We do not have that strategic approach to this problem currently.[21]

5.20 Sophos also advocated a more holistic national approach that involves IT vendors, and ISPs in a concerted effort to deal with the problem of botnets:

> With suitable Federal legislation, with mandated remediation or suspension, with national education initiatives, and with appropriate resources within government and ISPs, it would be possible to place additional pressure on these hijacked computers to be cleaned up. If successful, this would reduce the number of Australian-based bots, benefiting internet users not just in Australia, but all over the world.[22]

---

17 ACCAN, *Submission 57*, p.5.

18 ACCAN, *Submission 57*, p.5.

19 AusCERT, *Submission 30*, pp. 14 and 17; see also, *Transcript of Evidence,* 11 September 2009, p.5.

20 Mr Alastair MacGibbon, *Transcript of Evidence*, 11 September 2009, pp.60-61.

21 Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.5.

22 Sophos, *Submission 66,* p.6.

5.21 The role and responsibilities of ISPs and Domain Name Registrars and Resellers is discussed in Chapter 7.

Committee View

5.22 The Australian community's increasing reliance on ICT and the Internet combined with the complexity of online crime poses a significant challenge to policy makers, law enforcement and regulatory authorities. As discussed in Chapter 2, the interconnectedness of cyber space means that both the legitimate and illegitimate use of these technologies crosses inter-state and international boundaries and blurs the distinctions between civil and criminal matters.

5.23 This has implications for the development of a nationally coordinated and integrated policy on cyber security, strategic approaches to legal regulation, and the development of systems that maximise expertise and resources. The Committee commends the efforts of regulators and agencies tackling the problems of malicious Internet use but notes that the system remains inherently complex and fragmented.

5.24 The current *Cyber Security Strategy* places significant emphasis on national security and the protection of critical infrastructure. These are important national objectives. However, the Committee is concerned that education and awareness raising is no longer sufficient on its own as a national strategic response to the problem of cyber crime that impacts on the wider Australian community.

5.25 The breadth and complexity of the problem justifies a more national and centrally coordinated strategy that takes a more comprehensive and integrated cyber space perspective.

Recommendation 3

That the Australian Government establish an Office of Online Security headed by a Cyber Security Coordinator with expertise in cyber crime and e-security located in the Department of Prime Minster and Cabinet, with responsibility for whole of Government coordination. The Office is to take a national perspective and work with State and Territory governments, as well as federal regulators, departments, industry and consumers.

That the Australian Government establish a National Cyber Crime Advisory Committee with representation from both the public and private sector to provide expert advice to Government.

International Engagement

5.26 The DBCDE submitted that:

> Given the borderless nature of the internet, the isolated efforts of individual countries are not enough to effectively address global e-security challenges. Australia is actively working bilaterally and in key international forums to improve the international e-security environment. The main objective of this work is to assist countries that may be sources of e-security threats to improve their domestic response and to set in place international cooperative arrangements to address e-security threats.[23]

5.27 Similarly, the AGD outlined the importance of international engagement to promote coordinated international policy development, information sharing on cyber crime trends and response preparedness.[24]

5.28 The Departments identified a significant number of international fora in which Australia participates in and, in some cases, takes a leading role:

- **International Watch and Warning Network (IWWN)** is an international forum for international cooperation and coordination on cyber information sharing and incident response. It is comprised of government cyber security policy makers, managers of computer

23 DBCDE, *Submission 34*, p.15.

24 AGD, *Submission 44*, p.13.

security incident response teams with national responsibility and law enforcement representatives with responsibility for cyber crime matters.

- **Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL)** aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing and implementing appropriate telecommunications and information policies.
- The DBCDE submitted that Australia is a key driver of e-security work in the APEC group and has led a number of projects including:
  - ⇒ development of awareness raising materials for small business and consumers on wireless security and Voice Over Internet Protocol (VoIP) security;
  - ⇒ a joint project with the United States within APEC TEL on e-security awareness raising which aims to develop a coordinated approach in the region;
  - ⇒ participating actively in projects focused on ICT products and standards and hand-held mobile device security; and
  - ⇒ joint projects between APEC TEL and the OECD on e-security issues. The two groups have developed an analytical report on malware. These projects ensure common policy approaches are developed over a wider number of countries which leads to better outcomes for consumers.
- **Meridian** process brings together senior government officials from around the world who are policy makers on issues of critical information infrastructure protection (CIIP).
- **International Telecommunication Union (ITU)** is the leading United Nations agency for information and communication technologies and is currently examining a range of e-security issues under its Global Cybersecurity Agenda. The ITU's powers can bind member countries to take specific courses of action.
  - ⇒ The DBCDE participated in the regional workshop on *Frameworks for cybersecurity and critical information infrastructure protection* in August 2007 in Vietnam. This representation has allowed Australia to play a part in the development of policy documents on these issues for developing countries.
  - ⇒ The DBCDE held an ITU workshop on e-security and critical infrastructure protection in Brisbane in July 2008. This provided Australia with an opportunity to bring together Pacific Island countries to share e-security experiences and resources with these countries.

- ⇒ The ITU, with assistance from the Department, commissioned a scoping study on the feasibility of establishing a Computer Emergency Response Team for the Pacific Region (PacCERT). The first part of the study identified a definite need to develop a PacCERT, and found that a growing capability to deliver this already exists within the region. The second part of the study, relating to the implementation of a PacCERT, was to be finalised by the ITU in the second half of 2009. This work will include a detailed project plan covering staffing, location, funding, governance and the required linkages with other relevant parties, including domestic law enforcement authorities.

- **OECD Working Party for Information Security and Privacy (WPISP)** provides a platform for pursuing international aspects of Australian communications policy relating to cyber security, critical infrastructure protection, authentication, privacy, malware and spam.
  - ⇒ Australia currently chairs this Working Party and has been an active contributor in the development of common policy approaches to identity management, malware, critical infrastructure protection, cross border cooperation and privacy.
  - ⇒ Australia was the primary author of the OECD's Spam Toolkit which provided a multi-pronged strategy to deal with spam. This has improved international cooperation and information sharing on the issue of spam.
  - ⇒ The Working Party was also the vehicle for launching the joint APEC-TEL/OECD work on malware. Current work includes consideration of:
    - ⇒ identity management;
    - ⇒ malware;
    - ⇒ sensor-based environments;
    - ⇒ privacy in light of technology, and globalisation; and
    - ⇒ APEC–OECD work on protection of children online.
  - ⇒ Future work items may include work on generic best practice guidelines for ISPs to provide assistance to their customers on e-security matters. This work could build and potentially expand on work being done on the proposed Australian ISP E-Security Code of Practice.

- **International Multilateral Partnership against Cyber Threats (IMPACT)** is a public-private initiative against cyber-terrorism led by

Malaysia. It is the first global public-private initiative against cyber-terrorism and brings together governments, industry leaders and e-security experts.

- **Forum of Incident Response and Security Teams (FIRST)** conference brings together a variety of computer security incident response teams from government, commercial, and educational organisations. It aims to foster cooperation and coordination in incident prevention to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. There is also an associated meeting of national computer emergency response teams (CERTs) known as SECOND that provides a mechanism for cooperation and collaboration to solve many of the issues that national CERTs share in common.[25]

Committee View

5.29 The problem of cyber crime is by its nature an international one and the Committee believes that Australia should maintain a high level of engagement in relevant international fora. However, it is important that resources should not be excessively diverted to these efforts at the expense of developing and implementing concrete measures to assist ordinary Australian consumers and businesses at home.

25 AGD, *Submission 44*, p.13; DBCDE, *Submission 34*, pp.16-17.

Law Enforcement Coordination

5.30 The following sections focus on the reporting of cyber crime to law enforcement authorities and consumer protection regulators. In particular, it discusses how to improve the reporting and investigation of cyber crime that impacts on end users and small and medium sized businesses. The coordination between Australian law enforcement authorities for investigation of cyber crime and training in the investigation of high tech crime are discussed. Finally, the issue of public-private intelligence sharing across a wider range of cyber crime types is canvassed.

Cyber Crime Reporting and Assistance

5.31 A key issue raised in evidence was the difficulty law enforcement agencies face in addressing complaints about cyber crime from end users. It was said that, in practice, 'online consumers and to a lesser degree businesses, have been left to fend for themselves online'.[26] From a policing point of view, the problem of cyber crime was described as presenting 'unique challenge for governments, particularly law enforcement and crime prevention agencies'.[27] There are several factors that need to be taken into account.

5.32 First, cyber crime is invariably cross jurisdictional, with victims and perpetrators, and sometimes the evidence, all in different jurisdictions. The NT Government said that crimes are 'generally operated by overseas crime groups harvesting bank account details' and transfer funds via 'mules given instructions to send it overseas via Western Union'.[28] This makes close coordination between police forces within Australia and internationally essential.

5.33 Second, as noted above, the nature of cyber crime is highly complex and generally involves a series of interconnected conduct. The combination of activities (spam, malware, adware, spyware, phishing, fake and infected websites, email scams etc) are used together to steal financial credentials and personal identifying information, recruit money mules and ultimately to defraud, trick or steal money on an industrialised scale.[29]

---

26 Internet Safety Institute, *Submission 37*, p.9.

27 Queensland Government, *Submission 67*, p.7.

28 Northern Territory Government, *Submission 53*, p.1.

29 AusCERT, *Submission 30*, p.11.

5.34 The combination of these activities frequently engages both civil and criminal legal regimes and involves multiple agencies domestically and internationally.[30] The ACCC, for example, may receive a complaint about fraudulent conduct that also involves the proliferation of malware via spam emails in a phishing attack.[31] In practice, reporting of cyber crime or improper Internet use, if it occurs at all, is distributed across a variety of Commonwealth, State and Territory agencies and private institutions.

5.35 Third, cyber crime activities are generally organised on a large scale but individual incidents are frequently of a small value or have no immediately obvious destructive impact. Consequently, many crimes go undetected providing 'high rewards' for the criminal while attracting 'little attention from police and regulators'.[32] The under-reporting of computer offences where data is compromised through the use of ICT and later used for theft, fraud or other offences is also problematic.[33]

5.36 Additionally, small value crimes often fall below the thresholds applied to trigger an investigation. The CLPC said:

> Investigations and prosecution of many cyber crimes, in particular fraud, is often done on a balance of expenditure and impact. Most Australian states specify a minimum loss threshold, below which an investigation cannot be launched (e.g. $35,000).[34]

5.37 It is possible to commit:

> … credit card fraud of $5 million dollars without attracting investigative attention providing that the amounts stolen per jurisdiction operate below whatever the budget threshold existing in the jurisdiction. Steal $10 from 100 people in NSW another $10 from 100 people in Victoria, another $10 from 1000 people in France, and so forth.[35]

5.38 Measuring the scale of identity crime is also 'hampered by inadequate reporting practices' because a larger proportion of crimes are reported to

---

30 For example, Internet Safety Institute, *Submission 37*, p.11; OECD, *Malicious Software (Malware): A Security Threat to* the *Internet Economy*, 2008, pp.22-29; AusCert, *Submission 30*, p.11; Ms Penelope Musgrave, Director, Criminal Law Review, NSW Government, *Transcript of Evidence*, 8 October 2009, p.76.

31 ACCC, *Submission 46*, p.3.

32 Internet Safety Institute, *Submission 37*, p.7; see also, Ms Penelope Musgrave, Director Criminal Law Review, NSW Government, *Transcript of Evidence*, 8 October 2009, p.76.

33 AFP, *Supplementary Submission 25.1*, p.9.

34 CLPC, *Submission 62.1*, p.9.

35 CLPC, *Submission 62.1*, p.9.

financial institutions.[36] This, in turn, presents difficulties for police and for policy makers. Dr Russell Smith agreed that there are 'probably too many agencies involved in handling these … issues' and the problem is exacerbated where people report these matters to multiple agencies and institutions:

> They will go to their banks, card issuers, consumer affairs agencies, state and territory police and the Federal Police, and also places like ASIC and the ACCC. So there is a great need for coordination of information.[37]

5.39 Finally, the Committee was also told there is a tendency for Internet economic crimes to be given a 'lower priority and resourcing by police than offline crimes of a similar magnitude'.[38] The ability of police forces, especially at the local level, to accept and respond to the plethora of online criminal activity is limited. The issue is further complicated by the mix of civil and criminal activity involved.

5.40 The result is a lack of capacity in the law enforcement system to aggregate those types of Internet crime that involve 'small impact victimisation distributed across numerous jurisdictions'.[39] This stops law enforcement authorities from 'seeing a true picture' of the volume and scope of the cyber crime problem.[40] In turn, it allows criminal networks to benefit from aggregating the financial reward of dispersed activities, which may have no immediately obvious destructive effect.

5.41 The Committee was told the reason for setting up the first Australian High Tech Crime Centre (AHTCC) in 2003 was to overcome the fragmentation and develop a more coordinated approach. The AHTCC was an attempt by 'Australian law enforcement agencies … to implement a collaborative approach to preventing and investigating technology enabled crime …'[41]

5.42 The purpose of the AHTCC was to coordinate:

> … the information that is coming in so that all of those hundreds of small cases involving small amounts of money would go to one

36 AGD, *Supplementary Submission 44.1*, p.3.

37 Dr Russell Smith, AIC, *Transcript of Evidence,* 19 August 2009, p.15.

38 Internet Safety Institute, *Submission 37*, p.7.

39 CLPC, *Supplementary Submission 62.1*, p.5.

40 Mr Alastair MacGibbon, *Cyber security: Threats and responses in the information age*, APSI, December 2009, p.11.

41 South Australia Police, *Submission 2*, p.3.

> place, and then you would be able to see patterns emerging and put police resources into it.[42]

5.43 It was governed by a national board with high level representation from each of the State and Territory police forces.[43] The website provided information about a range of Internet crime types, and a system of pre-formatted crime reports for malware intrusions and DDOS attacks.[44]

5.44 One of the achievements of the AHTCC was the creation of the Joint Banking and Finance Sector Investigations Team (JBFSIT), to work collaboratively with the finance sector. The JBFSIT, which still exists, takes action against phishing sites targeting Australia financial institutions, mule recruitment sites and malware download sites.

5.45 In November 2007, the Ministerial Council for Police and Emergency Management endorsed the AHTCC becoming a business unit of the AFP.[45] The South Australian Police explained that:

> Most State based law enforcement agencies provided staff and some funding to the AHTCC until it was disbanded in 2007. … Conflicting investigational priorities and an emphasis of addressing Commonwealth priorities to the detriment of State based investigations contributed to the eventual disbandment of the AHTCC in 2007.[46]

High Tech Crime Operations Centre

5.46 The new High Tech Crime Operations Centre (HTCOC) was established in March 2008 as a portfolio within the AFP. The Committee was told that a single portfolio now exists that consolidates all of the AFP 'high-tech investigations arm and high-tech operations support resources'.[47] The role of the HTCOC is to:

- provide a national coordinated approach to combating serious, complex and multi-jurisdictional technology enabled crimes, especially those beyond the capability of single jurisdictions;

---

42 Dr Russell Smith, AIC, *Transcript of Evidence,* 19 August 2009, p.15.

43 Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2.

44 The AHTCC no longer exists. However, the website remains live and accessible via: <http://www.ahtcc.gov.au/tech_crimes_types/computer_intrusion.htm#report>, viewed 11 January 2009.

45 Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.1.

46 South Australia Police, *Submission 2*, p.3.

47 Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2.

- assist in improving the capacity of all jurisdictions to deal with technology enabled crime; and
- support efforts to protect the National Information Infrastructure (NII).

5.47 The AFP stressed the importance of collaboration with the private sector, and with international partners via its network of AFP liaison officers. The JBFSIT continues to operate in Sydney and, in 2008, expanded to Melbourne. An example of this collaboration is with RSA, the Security Division of EMC. RSA submitted that the RSA Anti-Fraud Command Centre has shut down more than 150,000 phishing attacks and reduced the average shutdown time of attacks from 115 hours to five hours. The submitter told the Committee that:

> At the request of Australia's banks for the better good of consumers, RSA is working closely with the High Tech Crime Centre to shut down criminal activity such as phishing attacks.[48]

5.48 The AFP told the Committee that:

> Collaboration with the financial sector is focused on prevention strategies to mitigate the impact of on-line consumers from phishing and malicious software. The analysis of data contained within the portal enables law enforcement to identify those responsible for online fraud activities.[49]

5.49 However, the offenders are 'usually based offshore and collaboration with international partner agencies via the AFP International Network is fundamental to successful investigations and subsequent prosecution outcomes'.[50]

5.50 The effectiveness of these strategies is difficult to measures in terms of prosecutions alone, either in Australia or internationally. In one example, the AFP were successful when 'online covert investigators identified a person attempting to sell a database online belonging to an Australian Domain Registrar':

> The database contained the compromised details of 70,000 Australian online consumers and 12,000 credit cards with an estimated financial exposure of $4.26 million.[51]

---

48 RSA, *Submission 28*, p.3.

49 AFP, *Submission 25*, p.16.

50 AFP, *Submission 25*, p.16.

51 AFP, *Clarification regarding High Tech Crime Operations article,* National Media Release, 23 September 2009.

5.51 However, the AFP does not keep statistics on cyber crime reports or prosecutions that involve technology enabled crime. The Committee invited the Commonwealth Director of Public Prosecutions to make a submission to the inquiry, but none was forthcoming. The AGD provided basic statistics that show there has been an average of eight prosecutions annually over the past five years for computer offences under Part 10.7 of the Commonwealth Criminal Code. The majority of the forty-one recorded convictions over the past five years have resulted in fines and bonds, suggesting that these matters fall toward the less serious end of the scale. Five cases have involved imprisonment, and four cases attracted a suspended sentence.[52]

5.52 The Committee also noted CLPC's criticism that Australia's law enforcement strategy puts little emphasis on prosecuting botherders or addressing botnets:

> To date there have been no public prosecutions in Australia of botnet herders. In fact, there is a paucity of prosecutions on the international front as well. Those botnet herders who have been prosecuted tend to come from the lower end of the cybercrime chain, and do not represent botnets run by organised crime groups.[53]

5.53 The CLPC advocated a more proactive approach that targets the dismantling of botnets, which provide the technical infrastructure to launch most of the cyber crime activities. As it was pointed out in Chapter 2, most botnets are self-replicating and self-sustaining and so there is also need for a cleanup process to prevent other criminals from taking over the botnet. The issue of remediation generally is discussed in Chapter 7.

Cyber Crime Reporting

5.54 The HTCOC is not a national focal point for the reporting of cyber crime and, in general, does not take a lead role in coordinating cyber crime investigations. A cyber crime could be reported to the AFP through the local Operations Monitoring Centre or AFP Headquarters. However, the activity must be sufficiently serious or reflect a Commonwealth priority to warrant AFP involvement.[54]

---

52 AGD, *Supplementary Submission 44.2*, p.14; note this data does not indicate whether these offences have been prosecuted by Commonwealth or State or Territory authorities.

53 CLPC, *Submission 62*, p.3.

54 For example, a large scale DDOS attack on a Commonwealth Government website or hacking and theft from a bank system may warrant an investigation.

5.55 The AFP said that:

> Public reporting is not standardised and public perceptions would be enhanced were a simple uniform system to be introduced. Thus far, public reporting of e-security threats has been facilitated through State and Territory Police, the AFP, and AusCERT. Many of these reports are lodged online via each agency's respective website. However, cases reported are often low level incidents, and not usually critical enough to warrant AFP intervention.[55]

5.56 An incident that is small value and/or impacts only on one individual (or one company) will rank as a low impact crime and is likely to be referred to State or Territory police.[56] Consequently, the AFP does not have a dedicated facility for online reporting of cyber crime or a special hotline reporting number (except in relation to online child sex exploitation) for the general public.[57] The AFP website directs the public (including businesses) to local State or Territory police to report computer offences.[58] However, this is no guarantee that a complaint will be accepted or investigated, as the victim will be usually be asked to report it to the police force of the State where the perpetrator resides or may be referred to another agency, such as the ACCC.[59]

5.57 The Committee was told there is no easy or well known way for someone to report a cyber crime 'whether it is to do with domain names or whatever':[60]

> People know how to report a normal sort of crime. … People who are victims of some sort of cybercrime do not know how or where to report it. If they do front up to their local police station or ring – presumably, it will not be 000 – some authority who they think should be able to take an investigation to the next step, in many cases they have no idea how to handle it either.[61]

---

55 AFP, *Submission 25*, p.20.

56 The assessment of whether an investigation will be undertaken is considered under the framework of the *Case Categorisation and Prioritisation Model* (November 2009).

57 As noted above, the former AHTCC website did provide for online reporting of a DDOS attack and malware intrusion. The Committee notes that this website is still accessible via a general Internet search but the model is, in fact, defunct.

58 Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.6.

59 Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

60 Mr Paul Brooks, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

61 Mr Paul Brooks, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

5.58 Mr Paul Brooks, Director, Internet Society of Australia, also observed that cyber crime reporting between the hours of nine to five is inadequate and reporting methods need to be improved.[62] Mr David Ready, a private citizen, expressed his frustration that he was unable to report a phishing site hosted in Australia to the AFP and the Domain Name Registrar one Friday evening in 2006.[63] As Mr Ready pointed out, criminals do not work normal office hours, and, continuation of a fake currency website over the weekend exposed people worldwide to potential victimisation.[64]

5.59 Mr Paul Brooks also stressed that a reporting system must take account of those cases where, for example, an ISP account has been stolen and the user no longer has email. In these cases, complete reliance on an online reporting system would be no improvement.[65]

Recent Innovations in Cyber Crime Reporting

5.60 There have been some innovations with reporting online crime at the State level in recent years. The Queensland Police Fraud and Corporate Crime Group (FCCG) have worked on the problem of 'Nigerian Fraud' through operations Echo Track and Hotel Fortress. An important aspect of this work is the online reporting portal 'for direct reference to the Nigerian Economic Financial Crime Commission and the Ghana Police'.[66] The Committee heard that these operations have so far led to in excess of ten arrests, and one prosecution, in Nigeria.[67]

5.61 The second example, also from Queensland, is the work of the FCCG in conjunction with eBay to establish the 'eBay project'. The eBay project is a 'national web based reporting system' that enables members of the public to report online auction fraud via an 'online reporting function, which includes pre-formatted statements'.[68] Initially the reporting system was only available to eBay users, but has now been extended to all online auction sites. The system collects the essential facts and enables the project to identify potential crimes, making distinctions between civil and criminal matters, and referring offences to the relevant police agency. The

62 Mr Paul Brooks, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

63 Mr David Ready, *Submission 6*, p.1.

64 Mr David Ready, *Submission 6*, p.1.

65 Mr Paul Brooks, Director, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.7.

66 Queensland Government, *Submission 67*, p.7.

67 Detective Superintendent Brian Hay, Queensland Police Service, *Transcript of Evidence*, 17 March 2010, p.3.

68 Queensland Government, *Submission 67*, p.6.

project also provides police agencies with a single point of aggregated data. [69]

5.62 The Queensland Government implemented the project to relieve the burden on front line local police and to provide a more intelligence based approach to the problem:

> Since the commencement of the eBay project in mid May 2007 there has been a steady acceleration in the number of on-line reports made. As a result the project has served as an invaluable intelligence gathering tool assisting police to identify serial offenders across jurisdictions. In Queensland alone, 788 complaints have been logged to date via this system. It is believed the e-Bay project will allow for more timely investigation and prosecutions by law enforcement agencies thereby limiting the time available for serious offenders to continue committing offences.[70]

Reporting to Consumer Protection Agencies

5.63 There have also been some developments in the field of consumer protection to facilitate cyber crime reporting. The website *ScamWatch* is hosted by the ACCC and functions as a point of access to the work of the *Australasian Consumer Fraud Taskforce*.[71]

5.64 *ScamWatch* is the national platform for disseminating information to the public on how to 'recognise, avoid and report scams'.[72] The public can report a scam to the ACCC via the website and follow links to other State and Territory consumer protection agencies. However, the quality of fraud and scam reporting facilities across these agencies varies. There also appears to be limited capacity to aggregate data received via these reporting mechanisms as there is no comprehensive data collection from these sources.

5.65 To improve information sharing the Auzshare system was created in 2005. Auzshare is a secure online website and database used by the Australian and New Zealand consumer protection authorities to share

---

69 Detective Superintendent Brian Hay, Queensland Police Service, *Transcript of Evidence*, 17 March 2010, p.2.

70 Queensland Government, *Submission 67*, p.6.

71 The Australasian Consumer Fraud Taskforce is comprised of nineteen government regulatory agencies and departments with responsibility for consumer protection regarding frauds and scams; ACCC, *Submission 46*, p.5.

72 ACCC, *Submission 46*, p.4.

depersonalised information about complaints, including scams.[73] It enables agencies to issue alerts to each other where there is a cross border issue.

5.66 However, it has also been noted that differing systems and approaches to, for example, categorisation of complaints, reduces the effectiveness of Auzshare.[74] The Productivity Commission's review of the Australian consumer protection framework has also 'highlighted the benefits of a linked complaints information system, and the need for comprehensive and consistent data provisions'.[75]

eConsumer.gov

5.67 In addition, the eConsumer.gov site provides a complaint portal where consumers from anywhere in the world can report a scam involving a foreign company that appears to be located in a member country.[76] The reporting facility is an initiative of the International Consumer Protection and Enforcement Network (ICPEN). The information contained in the 'complaint is entered into Consumer Sentinel, a consumer complaint database maintained by the US Federal Trade Commission'.[77]

5.68 The data is accessible to certified government law enforcement and regulatory agencies in ICPEN-member countries and is used to 'investigate suspect companies and individuals, uncover new scams, and spot trends in fraud'.[78] Information submitted through the online complaint form may be used to aggregate the data to analyse trends and statistics that may be released to the public.

5.69 These initiatives in both in the traditional criminal law and consumer protection areas demonstrate the potential for systems to improve public reporting on a range of cyber crime activity, and the opportunity to use that data to analyse large scale activity, support investigations, analyse trends and help measure the scale of the problem.

---

73 ACCC, *Supplementary Submission 46.1*, p.2.

74 Mr Peter Kell, Deputy Chair, ACCC, ACFT Consumer Fraud Research Forum, *Consumer Complaints about Scams: Managing and Sharing Information,* October 2009.

75 Mr Peter Kell, Deputy Chair, ACCC, ACFT Consumer Fraud Research Forum, *Consumer Complaints about Scams: Managing and Sharing Information*, October 2009.

76 ACCC, *Submission 46*, p.7.

77 ICPEN, viewed 18 January 2009, <http://www.econsumer.gov/english/report/overview.shtm>.

78 ICPEN, viewed 18 January 2009, <http://www.econsumer.gov/english/report/overview.shtm>.

A New National Approach to Cyber Crime Reporting

5.70 Several submitters proposed the creation of a national body to establish a more coherent response to victims and improve strategic capacity to detect and pursue online crime. Dr Russell Smith told the Committee there are now central reporting agencies in the UK, the US and Canada and:

> If they are adequately funded, I think they can make some inroads into solving some of the problems.[79]

5.71 In the US, the Internet Crime Complaints Centre provides an online reporting mechanism for the public to make complaints of cyber crime, especially online fraud, and functions as a clearing house on cyber crime.[80] The Centre is managed by the FBI and works closely with other bodies, such as the US Cyber Forensics and Training Alliance (NCFTA). The Federal Trade Commission and other agencies also take reports of various cyber crime types.

5.72 In the UK the Police Centre e-Crime Unit is located within the Serious and Organised Crime Agency (SOCA), with a remit to investigate serious e-crime.[81] However, it does not take reports from individual members of the public and the decentralised policing structure has made analysis at the national level difficult.[82] Under a recently adopted *ACPO e-Crime Strategy* the National Fraud Reporting Centre was designated as the national reporting centre for cyber crime.[83] As part of the *National Fraud Strategy*, investigators can now take cases that individually may not have been investigated but together represent significant loss.[84]

5.73 The NSW Government argued that consumers would benefit greatly from centralised cyber crime reporting:

> At present, agencies such as ACMA and others provide an avenue for reporting some cyber crimes (eg spam), but the broad range of

79 Dr Russell Smith, AIC, *Transcript of Evidence,* 19 August 2009, p.15.

80 Queensland Government, *Submission 67*, p.7.

81 The SOCA e-Crime Unit is separate from the Child Exploitation and Online Protection Centre. Cases that fall within the PCeU Case Acceptance Criteria include: significant intrusions into government, commercial or academic networks; denial of service attacks, and other criminal use of Botnets; significant data breaches; significant false identity websites; mass victimisation e-crimes, such as large scale phishing, and electronic attacks on the Critical National Infrastructure, *ACPO e-Crime Strategy*, 2009, p.8.

82 *ACPO e-Crime Strategy*, 2009, p.2.

83 The City of London Police, which has been designated the National Lead Police Force for Fraud, hosts the facility.

84 Jeremy Kirk, IDG New Service, UK Police to Track E-Crime, *Fraud Down to the Last Pence*, 25 March, 2009.

> cyber-scams that now exist suggest that the community may be better served by providing a central point to refer suspected cyber-scams, rather than the segmented and ad-hoc arrangements currently in place.[85]

5.74 Detective Inspector William van der Graff commented that a lot of resources are devoted to the problem of online scams but there are few prosecutions:

> I would like to see a national body that looks at this data and launches prosecutions of people internationally. I should say it is not necessarily easy. We are doing one at the moment and the people we are trying to track are very good. We may not meet with success in this case, but until we attempt it we do not know.[86]

5.75 The Queensland Government suggested a Centre, like the FBI Internet Crime Centre, complemented by an E Crime Mangers Group. The E Crime Mangers Group would have representation from each Australian policing agency.[87] It would promote national coordination, facilitate inter-jurisdictional operations, establish national standards and facilitate information sharing.[88]

5.76 AusCert and the Internet Safety Institute argued for a more integrated and consumer focused centre that can provide an Internet wide perspective to the problem.[89] To achieve a more effective response to the range of cyber crime activity will require a higher level of cooperation between civil and law enforcement agencies.[90]

5.77 In a recent paper for Australian Strategic Policy Institute, Mr Alastair MacGibbon, Director, Internet Safety Institute said that:

> Australia needs an internet crime reporting and analysis centre for homes and businesses. The relevant federal law enforcement and consumer protection agencies are not constituted, staffed, or able

85 NSW Government, *Submission 49*, p.6.

86 Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

87 Queensland Government, *Submission 67*, p.7.

88 Queensland Government, *Submission 67*, p.7; By contrast, the UK Police Service has already established standards for professional practice within e-crime, such as the *ACPO Good Practice Guide for Computer Based Evidence* and the *ACPO Managers Guide to e-Crime*; *ACPO e-Crime Strategy*, 2009, p.18.

89 Mr Graham Ingram, Director, AusCERT, *Transcript of Evidence,* 11 September 2009, p.5; Mr Alastair MacGibbon, Director, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

90 AusCERT, *Submission 30,* p.15; Internet Safety Institute, *Submission 37*, pp.3 and 10.

> to deal with the often small and seemingly inconsequential incidents of fraud, spam, scams, data loss, inappropriate content, or sometimes IT security incidents. We need an Internet 'shopfront' approach. A place for people to report matters, and to seek advice: a single consumer orientated destination, scaled for the Internet, which takes a national whole of government approach.[91]

5.78 In evidence to the Committee, Mr Alastair MacGibbon explained the purpose of centralised reporting would be to provide a one stop shop for the public and small businesses who believe they are a victim of cyber crime. It would operate on a 24 hour 7 day a week basis and be a combined public and private project. The aim would be to: provide a simple reporting mechanism for ordinary consumers: improve data collection, and intelligence analysis and sharing across police forces and other agencies; support targeted prosecutions; better identification of cyber crime trends; and provide education on e-security risks.[92]

5.79 The reporting system would provide for standardised first instance reporting and data collection on a range of cyber crime types. Police services would need to learn about large scale reporting, because these crime types involve large numbers of incidents that occur in a fragmented way.[93]

> An internet crime reporting and analysis centre would be most successful as a public-private partnership which could allow real-time information flow between the government's CERT Australia and the Cyber Security Operations Centre, giving Australia a more holistic view of Australia's internet health, and improving our ability to respond to threats and rebound.[94]

5.80 The IT company, McAfee, expressed strong support for working with other partners to establish a centralised online reporting mechanism for the general public in Australia. In the US, McAfee has already launched the *Cybercrime Response Unit* (CRU), an online portal for consumers and small and medium sized businesses. The CRU provides education about

---

91 Mr Alastair MacGibbon, *Cyber security: Threats and responses in the information age*, Australian Strategic Policy Institute, December 2009, p.11.

92 Mr Alastair MacGibbon, Director, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

93 Mr Alastair MacGibbon, Director, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

94 Mr Alastair MacGibbon, *Cyber security: Threats and responses in the information age*, Australian Strategic Policy Institute, December 2009, p.11.

online behaviours that lead to higher risks of cyber crime, and provides links to resources to report online crimes.[95]

5.81 The CRU includes free access to a 'non-intrusive' scanner that checks the PC to identify possible weaknesses in the owner's computer and risky online behaviour. The scan produces a report with recommendations on what the user can to do protect themselves from online threats. The issue of remediation of infected machines is discussed in Chapter 7.

5.82 McAfee funds all aspects of the portal, including CRU staff to answer victims' questions and clarify where to report the crime.[96] McAfee also told the Committee that it has developed close working relationships with US, European and British enforcement authorities. It shares intelligence on latest threat advice, and provides specific case support.[97]

5.83 On request by the Committee, McAfee expanded on the detail for a similar but more advanced model for Australia.[98] The company said it is willing to fund an Australian e-security portal that would also provide a 'central gateway' notifying appropriate agencies of incidents of cyber crime and:[99]

> … is willing to provide additional resources to ensure that law enforcement, financial service providers, and telecom service providers have the intelligence from this portal that they need to use the information effectively.[100]

5.84 Central reporting would enable more effective use of resources and quicker response times through the:

> … cross analysis of victim reports across Australian jurisdictions, combined with our Global Threat Intelligence or reputation-based scoring of cyber crimes and their websites globally… [101]

5.85 One of the benefits of central reporting is that it:

> … could greatly enhance law enforcement's ability to respond to only the immediate crimes and not spend as much time fielding general questions and following information that is not necessarily

95 McAfee, *Submission 10*, pp.11-12.
96 McAfee, *Supplementary Submission 10.1*, pp.2-4.
97 McAfee, *Supplementary Submission 10.1*, p.3.
98 McAfee, *Supplementary Submission 10.1*, pp.1-3.
99 McAfee, *Supplementary Submission 10.1*, p.3.
100 McAfee, *Supplementary Submission 10.1*, p.2.
101 McAfee, *Supplementary Submission 10.1*, p.3.

> in and of itself, an online crime or one in which no usable information is available.[102]

5.86 The aim would be to provide a technical solution to e-crime reporting but, the company stressed, collaboration between Federal, State and Territory police forces would remain critical to ensure suitable action is taken in response to incident reports.[103]

5.87 Detective Superintendent Brian Hay, Queensland Police Service, suggested that such a reporting centre should sit with an agency outside of the law enforcement sphere:

> A federal agency would be an appropriate body. If you look at the UK model, it has a non-law enforcement agency as the lead agency. The United Kingdom's National Fraud Authority is the lead agency for the reporting portal, but it is not a law enforcement agency. So I would be looking at a federal agency that is not the police, because a lot of the issues that will come forward are very much consumer based issues.[104]

5.88 McAfee also suggested that monetary thresholds should be removed.[105] By way of example, McAfee referred to the US *Identity Theft Enforcement and Restitution Act*, passed in September 2008 to eliminate the previous threshold of $5,000.[106] Instead of filtering out complaints via a financial threshold that inhibit investigations, the model recognises the dispersed nature and impact of computer based identity crimes. The penalty provisions are also triggered by an estimate of the aggregated losses resulting from a crime that victimises more than one person.[107]

5.89 The Committee has no evidence that any Australian jurisdiction has legislated money thresholds. However, it was suggested that an explicit mechanism to ensure that cyber crime incidents, including small value crimes, can be multiplied across police forces may be necessary. The CLPC suggested that a Memorandum of Understanding or, if necessary, a legal

---

102 McAfee, *Supplementary Submission 10.1*, p.2.

103 McAfee, *Supplementary Submission 10.1*, p.3

104 Detective Superintendent Brian Hay, Queensland Police Service, *Transcript of Evidence*, 17 March 2010, p.9.

105 McAfee, *Submission 10*, p.7.

106 McAfee, *Submission 10*, p.7.

107 Section 1030 Title 18 of the *United States Code*; Roy Jordan, *Client Memorandum*, Department of Parliamentary Services, 12 January 2010; the penalty for computer offences resulting in an aggregated loss to one or more person of at least $5,000 (over a twelve month period) attracts a fine of up to 5 years imprisonment (or both).

provision, should be adopted between Australian police forces (and internationally) to facilitate the aggregation of shared intelligence.[108]

Committee View

5.90 The evidence highlighted two interrelated issues that arise from Australia's current approach to the incidence of cyber crime and cyber crime reporting.

5.91 First, it is difficult for end users to know where to report an e-security incident (whether malware intrusions or identity fraud) and probably a degree of uncertainty over what redress is available. Under-reporting means that it is difficult to measure the size of the problem and, if reporting does occur, an incident could be reported to multiple agencies and private institutions.

5.92 The second and related issue is the lack of a nationally scaled institutionalised capacity to systematically collect and aggregate the intelligence data. There is no standardised method for receiving reports of e-crime from the general public or from companies that want to report. Nor is there any clear mechanism for sharing information on cyber crime reports between police forces, or between criminal and civil agencies such as the ACCC. This means lost opportunities for strategic intelligence analysis and detection of organised crime and support for prosecution in Australia or overseas.

5.93 A central reporting portal would enable reporting across the range of cyber crime types (malware, spam, phishing, scams, identity theft and fraud etc). Data collection and analysis would strengthen the detection of organised crime and support law enforcement efforts across jurisdictions. It would also provide existing agencies such as CERT Australia and the Cyber Security Operations Centre a more complete view of criminal activity on the Internet.

5.94 Where a consumer has suffered a malware intrusion, free access to scanning software and, where necessary, specialised IT assistance to remediate infected machines would help prevent re-victimisation. Remediation is discussed in Chapter 7. Information about cyber crime threats and e-security alerts, such as the Stay Smart Online alert service, and information about preventative e-security measures could also be integrated into the one body.

108 CLPC, *Supplementary Submission 62.1*, p.9.

5.95 To maximise its effectiveness the body should be staffed by suitably qualified analysts and investigators, who could be dedicated or seconded from the various agencies, including the research staff from the Australian Institute of Criminology. Specialist banking and fraud investigators funded by the private sector will be integral and, in the Committee's view, should be funded by the private sector.

Recommendation 4

That the Australian Government, in consultation with the State and Territory governments and key IT, banking and other industry and consumer stakeholders, develop a national online cyber crime reporting facility geared toward consumers and small and medium sized businesses.

This model should include the following features:

- **a single portal for standardised online receipt of cyber crime reports across a wide range of cyber crime types (e.g. malware, spam, phishing, scams, identity theft and fraud);**
- **a 24/7 reporting and helpline;**
- **no financial minimum to be applied to cyber crime reports;**
- **systematic data collection that allows data to be aggregated;**
- **referral to appropriate authorities and cooperation the on disruption and cyber crime and targeted prosecutions;**
- **free access to scanning software to detect malware;**
- **public information about cyber crime types and preventative measures to increase online personal security;**
- **e-security alerts tailored to the needs of ordinary consumers and small and medium sized businesses; and**
- **analysis of cyber crime methodologies and trends or cooperation with another body to perform that analysis.**

Criminal Law Enforcement Coordination

5.96 The NSW Government contended that the HTCOC has a role to 'provide a national approach to combating cyber-crime especially where the abilities of a particular jurisdiction are limited.'[109] However, the Tasmanian Government submitted that 'since the closure of the AHTCC there has not been significant cross-jurisdictional coordination in relation to e-security risks'.[110]

5.97 The NT Government also said that:

> It was hoped when the AHTCC was established in 2003 that it would provide a liaison with international police and help coordinate offences from the Australian end and refer them overseas. From an NT Police perspective the AHTCC appears to be focused primarily on internet banking fraud and is not in a position to offer substantial assistance in the other areas… [111]

5.98 The AFP considered that the former AHTCC was an 'effective model for undertaking investigation and sharing information and expertise' because it was a national body and provided a consistent approach.[112] While it aims to build on those relationships, Commander Gaughan agreed that coordination with State and Territory police is 'where the difficulty currently lies'.[113]

5.99 The Australian Banking Association (ABA) argued that at the national level, the difficulties encountered in fighting cyber crime are not legal jurisdictional issues but 'differing priorities between agencies on prevention, detection and prosecution'.[114] There is a 'need for more coordination and cooperation between agencies in sharing vital information and intelligence risks (prevention)'.[115] At the present time

109 NSW Government, *Submission 49*, p.4.
110 Tasmanian Government, *Submission 51*, p.4.
111 NT Government, *Submission 53*, p.2.
112 AFP, *Submission 25*, p.15.
113 Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, pp.2-3.
114 ABA, *Submission 7*, p.6.
115 ABA, *Submission 7*, p.7.

there is no national centralised mechanism for coordinating these activities.[116]

5.100 Similarly, the South Australia Police said that there is no 'coordinated medium for information to be exchanged about crime trends and methods'.[117] The re-establishment of the E-Crime Investigation Managers Committee under the auspices of Australian New Zealand Police Advisory Agency (ANZPAA) may improve information exchange. However, there was no suggestion that this alone would be sufficient.[118]

5.101 It was noted that the capacity of consumer protection and law enforcement agencies to respond varies across the jurisdictions. The highly technical nature of these crime types requires specialist skills and equipment.[119] Most State and Territory police forces have specialist investigators and some capacity for forensic analysis. The NSW Police has the NSW Police Fraud Squad Computer Crime Team and South Australia Police has a small Electronic Crime Section comprised of a manager, five investigators and four electronic evidence specialists.[120] But smaller jurisdictions, such as Tasmania, have less capacity to address the problem.[121]

5.102 The Tasmanian Government argued that cyber crime can only be properly addressed at the national level:

> Many e-security issues affect consumers across Australia and internationally, and consequently it is not practical for State agencies to address them individually. Further, responses by individual states risks significant duplication of resources, which can be ill-afforded by small jurisdictions. This is especially the case with regard to highly technical problems such as those posed by the increasing criminal use of malware.[122]

5.103 The lack of national coordination means that cooperation between police forces operates on a case by case basis with police services across Australia 'providing assistance or referrals to one another'.[123]

---

116 ABA, *Submission 7*, p.6.
117 South Australian Police, *Submission 10,* p.4.
118 South Australian Police, *Submission 10,* p.4.
119 NSW Government, *Submission 49*, p.4.
120 South Australia Police, *Submission 2*, p.1.
121 Tasmanian Government, *Submission 51*, pp.1-5.
122 Tasmanian Government, *Submission 51,* p.5.
123 Tasmanian Government, *Submission 51*, p.4.

5.104 'Pending the development of a more formal coordination mechanism', Tasmanian investigators have joined the AUSPOL email list hosted by AusCERT.[124] AUSPOL enables e-crime investigators to share information by posting 'queries and information to their colleagues across the country.'[125]

Training and development

5.105 There was also a call from some police forces for a more coordinated approach to training and development, which the Committee was told is expensive and only happens on an ad hoc basis. South Australia Police argued that there is a lack of 'consistency in the frequency and level of training provided to law enforcement detectives involved in investigating technology enabled crime'.[126] This area of crime requires regular upgrading of skills as new technologies means that 'new investigative techniques are required'.[127] It was suggested that minimum standards should be set and processes established to ensure the capacity of the police to respond to technology enabled crime is maintained.[128]

5.106 The NSW Government proposed the creation of a National Cyber Crime Training Institute that could be the centre of training and skills development for police working in this field.[129] Detective Inspector William van der Graff, Coordinator, Computer Crime Team, Fraud Squad, NSW Police Force, argued that such a body would be an effective way of ensuring over the longer term that sufficient numbers of police officers are adequately skilled in this area.[130] Although a National Cyber Crime Training Institute would primarily serve the needs of law enforcement agencies, he suggested that it could potentially also provide training for other arms of government.[131]

---

124 Tasmanian Government, *Submission 51*, p.4.

125 Tasmanian Government, *Submission 51*, p.4.

126 South Australia Police, *Submission 2*, p.3.

127 South Australia Police, *Submission 2*, p.3.

128 South Australia Police, *Submission 2*, p.3.

129 Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

130 Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

131 Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

5.107 AGD informed the Committee that the AFP offers electronic crime based training courses to other Commonwealth, State and Territory law enforcement agencies. The includes the AFP's:

- Internet Policing Program which provides training in the tactical use of the Internet including online conversations with suspects and advanced internet search techniques;
- Child Protection Operations workshop which provides training for investigating online child sex offences and child sex tourism internationally with a focus on the nexus between international law enforcement, the AFP and State and Territory police; and
- Management of Serious Crime course, a multi-agency, multi-jurisdictional program provided to a range of senior law enforcement practitioners across the Commonwealth and the States and Territories that includes a focus on cyber crime investigations.[132]

5.108 The AGD also told the Committee that the AFP is establishing a Technology Enabled Crime Centre of Excellence within its High Tech Crime Operations portfolio:

> This Centre brings together technical, legal and other subject matter experts to provide the AFP and its partner agencies with a single point of contact on issues of technology enabled crime. The Centre is being formed in recognition of the increasing complexity of technology enabled crime and the need to deliver contemporary, specialist advice to investigators working on these matters.[133]

5.109 In June 2009, the AFP hosted the Australian High Tech Crime Conference with the University of Technology, Sydney and the Australian Institute of Criminology. Such conferences were said to be useful to develop and maintain links between law enforcement, the judiciary, the legal profession, academia, industry experts and government officials. AGD said:

> The conference was successful in sharing information, ensuring a dialogue on key challenges, addressing investigative techniques and discussing legal and legislative issues relating to technology based crimes. The AFP will continue to host this conference annually.[134]

132 AGD, *Supplementary Submission 44.2*, p.11.

133 AGD, *Supplementary Submission 44.2*, p.11.

134 AGD, *Supplementary Submission 44.2*, p.11.

Committee View

5.110 The measures outlined by AGD will all contribute to building better law enforcement capacity and provide opportunities to share information and skills. However, the Committee believes that the proposal for an E Crime Managers Group and a National Cyber Crime Training Institute have considerable merit, and would go a long way toward ensuring a more effective harnessing of police resources.

5.111 The responsibility for developing and maintaining these structures should be shared across all Australian governments, to ensure that such measures are responsive to the needs of all jurisdictions.

Recommendation 5

That the Federal, State and Territory police forces establish an E Crime Managers Group to facilitate the sharing of information and cross jurisdiction cooperation.

Recommendation 6

That the Australian Government, in consultation with the State and Territory governments, industry and consumer organisations, develop a national law enforcement training facility for the investigation of cyber crime.

Public-Private Cyber Crime Intelligence Sharing

5.112 Many witnesses emphasised the importance of the government and private sector 'working together to improve computer security', both in relation to critical infrastructure and the wider area of cyber crime that impacts on Australian society more broadly.[135] The evidence indicated a need for intelligence sharing on a wider range of cyber crime types and this information to be both:

- in real time operational intelligence; and

135 See for example: Microsoft, *Submission 35*, p.11; Australian Information Industry Association, *Submission 22*, p.12; AGD, *Submission 44*, p.11.

- longer term analysis and information sharing within and between industries; and
- be based on pre-sanctioned trusted information sharing networks.

5.113 As noted above, the Australia Government has recently established the DSD Cyber Security Operations Centre and, in collaboration with AusCERT, moved to bring computer emergency response team functions together under CERT Australia. The primary mechanism for public-private sharing of sensitive security related information remains the pre-existing Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).[136]

5.114 Under the umbrella of the TISN, CERT Australia will now operate the three sectoral exchanges to share technical information in the:

- banking sector;
- communications sectors; and
- owners and operators of control systems in power and water utilities.[137]

5.115 Witnesses made several points about the nature of the public-private collaboration. The first issue was the scope of the existing TISN, which is focused on national security and critical infrastructure. For example, Telstra said:

> Within the current national critical infrastructure framework of the existing Trusted Information Sharing Network (TISN) … focus is specifically on the national security context of cyber crime (i.e. e-security). The existence of this framework may provide an opportunity to extend the TISN focus into cyber crime and its impact on Australian society more broadly.[138]

5.116 The ABA also expressed concern that the existing TISN does not cover all the types of cyber crime intelligence that interest the banking sector:

> Strict boundaries between national security, critical infrastructure protection, financial crimes and other non-financial crimes may no longer be appropriate as the mechanisms used by cyber criminals are common to all.[139]

5.117 The ABA explained that they want to see a more integrated approach:

---

136 AGD, *Submission 44*, p.10.

137 AGD, *Submission 44*, p.11.

138 Telstra, *Submission 43*, p.3.

139 Mr Tony Burke, ABA, *Transcript of Evidence,* 8 October 2009, p.51.

> In terms of the traditional intelligence cycle this probably means the centralisation of the planning and direction, analysis and production functions with sharing of the collection, processing and dissemination functions.[140]

5.118 The ABA, advocated a 'more formal arrangement for sharing intelligence with its Members' and said that:

> No governing body currently exists to allow strategic threats to be continually assessed between the public and private sectors (other than in the area of Critical Infrastructure) in this area.[141]

5.119 Given the interdependency of the public and private sectors, the ABA said this situation 'places Australian institutions in both the public and private sector at a disadvantage when it comes to protecting Australian internet users'.[142]

5.120 Mr Richard Johnson, Chief Information Security Officer, Westpac Banking Corporation, told the Committee that while relationships have been developed with 'segments of the banking industry, the AFP and some other government bodies, these relationships are effectively point-to-point, personal based relationships….':

> The large number of working groups, advisory groups, government agencies, departments and law enforcement bodies may be better served by a single point of coordination on cyber crime issues and information exchange.[143]

5.121 RSA also submitted that private industry associations and their security solution providing members cannot 'gain the upper hand on their own' and called for a more centralised and coordinated leadership from the Australian Government.[144]

5.122 In addition to the scope of the TISN, some witnesses commented on the nature of the trust relationship and indicated some concern about the timeliness of information. Mr Johnson, Westpac, said the key to trusted relationships is the 'free and open bidirectional sharing of information and intelligence'.[145] The witness told the Committee there is a lack of

---

140 Mr Tony Burke, ABA, *Transcript of Evidence,* 8 October 2009, p.51.

141 ABA, *Submission 7,* p.13.

142 ABA, *Submission 7,* p.14.

143 Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.52.

144 RSA, *Submission 28*, p.3.

145 Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.52.

formalised and pre-sanctioned trust relationships between government and industry and this has:

> … left both groups effectively unsure of exactly what can be shared. Information that is shared is therefore redacted to such a point that it borders on being meaningless. In other words, we do not know what we do not know.[146]

5.123 Importantly, the apparent lack of pre-sanctioned relationships was said to affect the timeliness of sharing real time operational intelligence. Mr Johnson, Westpac, explained that:

> Timeliness of this information is critical to be effective. Cybercrime threats, by their very nature, are given to evolve rapidly. Current information-sharing arrangements are dependent on multiple levels of clearance and release approval, severely limiting the usefulness of information that can be shared. A true national, trusted intelligence-sharing network is required, with preclearance of participants and of the information types which can be shared. This needs to operate in real time to match the nature of the threat. By sharing information and pooling data, analysis of the entire dataset can be performed and each participant will gain a holistic view of the common threat which today we can each only see from our own point of view.[147]

5.124 Symantec, a global IT security vendor, also provided comment on the TISN. In particular, Symantec said that trust, time and resources are the key to public-private cooperation and it was important for the relationship to be one of exchange. For example, offering participants exclusive cyber threat intelligence information that cannot be obtained elsewhere. Symantec also observed that private sector members need assurance on key issues such as:

- the role and intention of authorities requesting information;
- whether there is exposure to regulatory enforcement action;
- protection of commercially sensitive information; and
- the protection of privacy of consumers.[148]

5.125 The witness proposed that Australia consider enacting legislation to assure private sector participants that confidential, proprietary, and

146 Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.53.

147 Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.53.

148 Symantec, *Supplementary Submission 32.1*, p.8.

business-sensitive information is only used for the purpose for which is it shared. In particular, that the information is protected from public disclosure, regulatory action, and there are uniform procedures for receipt, care and storage of information. Symantec advised that, in the context of critical infrastructure, the US introduced the *Critical Infrastructure Information Act 2002* to improve information sharing. An alternative would be formalised and enforceable data sharing and non-disclosure agreements, however, it was noted that these agreements are likely to still entail the possibility of regulatory and legal action.[149]

5.126 Further evidence from AGD opposed any specific legislation and argued that existing arrangements are adequate, and include legal remedies for breach of confidentiality. Private sector organisations sign a *Deed of Confidentiality*, which set out their obligations:

> This ensures that information is properly managed and reasonably protected from unauthorised disclosure or use. Information that is provided to Government within the TISN is used for legitimate TISN purposes only. This information is not disclosed to other regulatory agencies, unless required by law. In such cases, the owners of the information would be given prompt notice and reasonable details of the circumstances involved should they wish to respond.[150]

5.127 Additionally, public sector officials sign a *Government Representative Confidentiality Acknowledgement,* which acknowledge their statutory and other legal and policy obligations for information handling.[151]

5.128 Symantec also suggested a standardised structure for the exchange of information that describes, categorise, prioritise information and have established channels for the escalation of security incidents. Two examples of messaging standards for information sharing purposes were the EU Messaging Standard for Sharing Security Information (MS3i), and the US National Information Exchange Model (NIEM).[152]

5.129 Symantec also proposed that appropriate house rules be established on participation in sector meetings. This was intended to ensure minimum levels of seniority and the involvement of decision makers to generate

149 Symantec, *Supplementary Submission 32.1*, p.9.

150 AGD, *Supplementary Submission 44.2*, pp.1-2.

151 These include section 70 of the *Crimes Act 1914* (Cth) which deals with disclosure of information by Commonwealth officers, the *Australian Public Service Code of Conduct* set out in the *Public Service Act 1999* (Cth) and the Australian Government's Protective Security Manual.

152 Symantec, *Supplementary Submission 32.1*, p.9.

trust. The Warning, Advice and Reporting Point (WARP) in the UK was given as an example.[153]

5.130 The Committee also heard from Ms Alana Maurushat, Deputy Director, CLPC who advocated the creation of a body similar to the US National Cyber Forensics and Training Alliance (NCFTA).[154] The NCFTA is not a law enforcement agency. It operates as an intelligence hub receiving intelligence from companies and organisations that are victims of cyber crime (DDOS attacks, security breaches, fraud).[155]

5.131 The NCFTA can work across industry sectors to aggregate intelligence, assisting organisations to mitigate attacks, preserve digital evidence, and work with law enforcement to support prosecutions.[156] In her view, the creation of an 'intelligence hub' is 'really important for Australia and what is grossly lacking'.[157]

5.132 Dr Paul Brooks, Director, Internet Society of Australia made the distinction between real time operational information and the longer term analysis:

> When somebody notices that their equipment, their ISP or their home PC has been hacked, it requires different tools, a different level of investigative ability and a different organisations structure for them to be able to pick up the phone and get on a hotline to somebody who can within minutes identify what is going on a try and tack that back in real time to where it is coming from so you can actually catch the guys that are doing it.[158]

5.133 From an industry perspective, Mr Richard Johnson, Westpac Banking Corporation, submitted that in the US the Information Sharing and Analysis Centres (ISACs) are industry based centres that provide a real time information sharing network. This is operational intelligence on threats that are underway:

> That is the kind of operation level intelligence we … need to develop which then, for a strategic analysis purpose, could be fed into the research alliances.[159]

---

153 Symantec, *Supplementary Submission 32.1*, p.9.

154 CLPC, *Submission 62*, p.11.

155 Ms Alana Maurushat, CLPC, *Transcript of Evidence*, 8 October, 2009, p.33.

156 CLPC, *Submission* 62, p.11.

157 Ms Alana Maurushat, CLPC, *Transcript of Evidence*, 8 October, 2009, pp.32-33.

158 Dr Paul Brooks, Internet Society of Australia, *Transcript of Evidence,* 9 October 2009, p.13.

159 Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, pp.54-55.

5.134 Mr Johnson also advised the Committee that the company has been involved in creating the Internet Commerce Security Laboratory, a joint research alliance with the Victorian Government, the University of Ballart and IBM, with support of the AFP. The Internet Commerce Security Laboratory is a research facility that performs data mining, data analysis and correlation to provide better leads, intelligence and information to support arrests.[160]

Committee View

5.135 The Committee considers that public-private cyber crime intelligence coordination is vital to achieve a more resilient Internet and ICT environment and ensure confidence in the digital economy. This view is also reflected in the Australian Government's recent *Cyber Security Strategy*.

5.136 Under the *Cyber Security Strategy*, the new DSD Cyber Security Operations Centre is geared to detect and respond to aggressive cyber attacks on the 'National Information Infrastructure'.[161] It supports non-government critical infrastructure through ASIO, AFP and AGD. CERT Australia obtains cyber threat intelligence and, through the three sector exchanges, shares technical information with the banking, utilities and communications sectors. This is in the context of national security and critical infrastructure protection.

5.137 However, the evidence to the Committee was that there is also a need to either:

- widen the remit of CERT Australia and TISN to encompass a broader range of cyber time types; or, alternatively;
- create separate and additional capacity through a joint public-private organisation to obtain, analyse and share technical real time actionable information.

5.138 The evidence indicates that Government leadership with significant private sector participation is needed to address the current lack of coordinated response to a wider range of cyber crime types that impact Australian society more generally.

---

160 Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, pp.54-55.

161 The national information infrastructure is made up of those key communications and information technology systems that support critical industries and government services, such as the telecommunications, transport, distribution, energy, utilities, banking and finance industries and defence and emergency services.

5.139 A Government led initiative to develop a more coordinated approach to accessing and sharing real time operational data was a high priority for several witnesses. There was also consistent advocacy for some form of 'intelligence hub(s)' for analysis of methodologies and trends, and, where possible, support targeted prosecutions in Australia and internationally.

5.140 At first glance it might appear logical to integrate these functions into the same organisation. However, the evidence indicates that these functions are distinct and require different types of organisations albeit with close links. The former must be genuinely responsive and operate through a network of pre-sanctioned relationships in a clearly visible and accepted trust environment. This may require special legislation to provide the visibility necessary to build trust between government and the private sector and between competitors.

5.141 The latter is focused on the deeper and longer term analysis of methodologies and trends that can support industry preparedness. This could include cross industry intelligence sharing, private sector education on the preservation of digital evidence, and, where possible, support to targeted law enforcement action in Australia and overseas.

5.142 The Committee is aware that other countries face the same challenges and have useful experience to draw on. In the US, for example, a network of public-private Information Sharing and Analysis Centres provide real time operations intelligence for critical infrastructure. This approach might provide an effective model for intelligence sharing on the wider cyber crime types in Australia. The NCFTA is also a model for cross industry intelligence gathering and analysis. However, some steps have been taken in that direction with the creation of the Internet Commerce Security Laboratory.

Recommendation 7

That the Australian Government consult with major IT security vendors, academia and key industry stakeholders to develop:

- **options for establishing a coordinated public-private capacity to provide real time operational information on a wider range of cyber crime types that impact on Australian consumers;**
- **an 'intelligence hub' that facilitates information sharing within and across industry sectors and provides:**
  - ⇒ **longer term analysis on cyber crime methodologies across a range of cyber crime types;**
  - ⇒ **education on the preservation of digital evidence; and**
  - ⇒ **support to law enforcement agencies for targeted prosecutions in Australia and overseas.**

6

Criminal and Law Enforcement Framework

Introduction

6.1 The chapter discusses the existing criminal law framework intended to combat cyber crime and canvasses Australia's possible accession to the Council of Europe Convention on Cybercrime. The chapter concludes that Australian criminal law (substantive and procedural) is well developed but that legal policy in this field must ensure an appropriate focus on the transnational nature of cyber crime and particular challenges of digital evidence. There is also a strong case for a more strategic focus on the disruption of botnets and prosecution of botherders that will require intense international cooperation.

Criminal Law

6.2 Over the last decade, successive Australian Governments have enacted specific offences for the misuse of computers and telecommunications systems and online sexual abuse of children in the *Criminal Code Act 1995* (the Criminal Code).[1]

6.3 The technological aspects of cyber crime also pose particular challenges to the investigation of crimes against computers or that use communication

---

1 AFP, *Submission 25*, p.13.

technologies.[2] In response to these challenges the law now provides police authorities with specific powers to obtain evidence to aid the investigation and prosecution of online offenders.[3]

6.4 The next section outlines some of the key provisions and canvasses witnesses' views on the adequacy of existing offences. The procedural aspects are then discussed in the following sections.

Computer Offences

6.5 The *Cybercrime Act 2001* (Cth) introduced computer offences into the Commonwealth *Criminal Code Act 1995* (Criminal Code) with maximum penalties ranging from two to ten years imprisonment.[4] The offences address the problems of hacking, denial of service attacks and malware intrusions. The offences follow those contained in the Model Criminal Code recommended by the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (MCLOC).[5] A summary of the provisions is set out in appendix D.

6.6 The Constitution does not grant the Commonwealth express power over criminal activity *per se*, however, the Parliament can validly make laws to create criminal offences and provide for their investigation, prosecution and punishment, provided that the offences fall within, or are incidental to the exercise of a constitutional head of power.[6] In the context of cyber crime the Commonwealth offences apply only to the:

- protection of Commonwealth computers and computer systems; and
- the commission of crimes by means of a telecommunications service.[7]

6.7 However, State and Territory computer offences apply generally in the respective jurisdictions and therefore provide national coverage.[8]

---

2 Russell Smith, *Impediments to the Successful Investigation of Transnational High Tech Crime*, Trends and Issues in Crime and Criminal Justice No. 285, Australian Institute of Criminology, October 2004, p.1.

3 Attorney-General's Department, *Submission 44,* p.16; *Telecommunications (Interception and Access) Act 1979* (Cth)*; Crimes Act 1914* (Cth).

4 Part 10.7 Divisions 477 and 478 of the Criminal Code; AGD, *Submission* 44, p.18.

5 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, Chapter 4 Damage and Computer Offences, Report of the Committee, February 2001.

6 Commonwealth criminal law is ancillary to the performance of the Commonwealth of its powers to protect itself, the Constitution, its institutions and to enforce its own laws; Sir Garfield Barwick, Crimes Bill 1960, Second Reading Speech, House of Representatives, *Debates*, 8 September 1960 pp.1020-1021 reported in *Research Paper No.12,* Department of Parliamentary Library, Canberra, 2002, p.4.

7 AGD, *Supplementary Submission 44.2*, p.10.

Identity Fraud Offences

6.8 The computer offences may be combined with Commonwealth or State or Territory provisions that cover identity related crimes, such as fraud, forgery, or dishonest dealing in personal financial information.[9]

6.9 The fabrication or misuse of identity has traditionally been treated as an aspect of these primary offences. In March 2008, the MCLOC recommended the introduction of specific identity fraud offences and a certificate for victims to assist in re-establishing their credit worthiness. The model offences do not require that a crime, such as theft, fraud, forgery or deception be perpetrated but merely that there is an intention to commit or facilitate the commission of an indictable offence.[10]

6.10 At the Commonwealth level, the House of Representatives passed the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008 (the Bill) on 23 February 2009 and, at the time of writing, the Bill remains under consideration by the Senate. The Bill inserts three identity fraud offences into a new Part 9.5 of the Criminal Code. The offences are described in Appendix E.

6.11 The amendments also allow a person who has been the victim of identity crime to apply to a magistrate for a certificate to show they have had their identity information misused. The purpose of the certificate is to assist victims 'negotiating with financial institutions to remove fraudulent transactions, and other organisations such as Australia Post, to clear up residual problems with identity theft'.[11]

6.12 At the State level, both South Australia (SA) and Queensland have specific identity theft/fraud offences.[12] In March 2009, the Victorian Parliament passed the *Crimes Amendment (Identity Crime) Act 2009* (Vic). By December 2009, NSW had passed the *Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009* (NSW). The WA Criminal Code Amendment (Identity

8 AGD, *Supplementary Submission 44.2*, p.10; Microsoft Australia, *Submission 35*, p.7.

9 For example, section 480.4 of the Commonwealth Criminal Code makes it an offence to dishonestly obtain or deal in personal financial information without consent of that person to access funds, credit or other financial benefits.

10 MCLOC, *Final Report: Identity Crime*, Commonwealth of Australia, 2008.

11 AGD, *Supplementary Submission 44.1*, p.3.

12 AGD, *Submission 44*, p.4; *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA); *Criminal Code and Civil Liability Amendment Act 2007* (Qld); Note that under section 144B of the *Criminal Law Consolidation Act 1935* (SA) it is an offence to assume a false identity or falsely pretend to be entitled to act in a particular capacity. Unlike the model provisions this offence does not require proof of an intention to commit a serious criminal offence.

Crime) Bill 2009 is currently before the WA Parliament.[13] There was no evidence indicating whether Tasmania, the Northern Territory or the Australian Capital Territory have or are soon to adopt the model offences.

Commentary

6.13 The Australian Federal Police expressed the view that criminal offences to tackle cyber crime are sufficient, the difficulty lies more in enforcement and the trans-national nature of most cyber crime.[14] The AGD also said that while some aspects of the law and law enforcement could be strengthened existing Australian laws are 'appropriate'.[15] Nevertheless, some questions were raised about the breadth and uniformity of the computer offences.

Technology Neutral Language

6.14 The Committee was told that computer offences need to be drafted in technology neutral language to minimise repeated amendment of the Criminal Code.[16] According to AGD, the Part 10.7 offences are drafted so as to apply as technology evolves:

> For example, the term "computer" was not defined to ensure the computer offences will encompass new developments in technology, for example, mobile phones that allow access to the Internet.[17]

6.15 The Internet Industry Association (IIA) were satisfied that legitimate investigations carried out to determine the level of security of a client's system would not be caught by the offence provisions.[18] However, Symantec were concerned that legitimate software suppliers must not be inadvertently committing offences when 'using tools/devices for

13 The WA Bill 'utilises and builds upon (but does not specifically implement) the model provisions'; WA Legislative Council, *Standing Committee on Uniform Legislation and Statutes Review Report No 44*, March 2010, p. 14, viewed 17 March 2010, <http://www.parliament.wa.gov.au/parliament/commit.nsf>.

14 AFP, *Submission 25*, p.9.

15 AGD, *Submission 44*, p.7; The E-Security Review did recommend: agency collaboration to address 'legal issues associated with the blocking of user access to Internet sites by law enforcement and other agencies'; better coordination of crime reporting; and training and information for the legal profession.

16 AGD, *Supplementary Submission 44.2*, p.10.

17 AGD, *Submission 44*, p.4.

18 IIA, *Submission 54,* p.2.

legitimate business purposes, e.g. conducting research, penetration testing, and/or supplying patches for vulnerabilities'.[19]

6.16 It was suggested that ss.478.3 and 478.4 clarify that it is only a criminal offence when the 'device has been developed primarily, deliberately and for the sole purpose of committing an offence'.[20] Other factors that should be considered include:

- whether the device is available on a wide scale commercial basis and sold through legitimate channels;
- whether the device is widely used for legitimate purposes with a substantial installation base; and
- the context in which the device was used to commit the offence compared with its original intended purpose.[21]

6.17 Symantec also questioned the scope of the term 'data' and argued that it should be clarified so it is clear that it includes malicious devices and tools and toolkits.[22]

6.18 A further question arose as to whether the placing and later exploitation of a latent functionality in computer hardware or software without the owner's knowledge or consent was caught by existing criminal provisions. The AGD assured the Committee that the computer offences adequately cover such conduct.[23]

Uniformity of Commonwealth, State and Territory Provisions

6.19 Some witnesses raised concern about the apparent inconsistency of computer offences across Australian jurisdictions. For example, Microsoft Australia submitted that New South Wales, Victoria, South Australia, the Northern Territory and the Australian Capital Territory have implemented the Model Criminal Code and established computer offences materially similar to the federal provisions.[24]

6.20 However, Queensland, Tasmanian and Western Australian regimes were described as 'less aligned with the Model Criminal Code; they appear to focus on computer hacking and misuse offences'.[25] The Tasmanian

19 Symantec, *Supplementary Submission 32.1*, p.2.
20 Symantec, *Supplementary Submission 32.1*, p.2.
21 Symantec, *Supplementary Submission 32.1*, p.2.
22 Symantec, *Supplementary Submission 32.1*, p.2.
23 AGD, *Supplementary Submission 44.1*, p.1.
24 Microsoft Australia, *Submission 35*, p.7.
25 Microsoft Australia, *Submission 35*, p.7

Government also noted that as most e-security threats involve the use of communications technology, most of the reforms have been at the national level.[26] The Australian Banker's Association (ABA) said that:

> Various provisions of the Model Criminal Code have, we believe, been sporadically and not necessarily consistently implemented across the Australian jurisdictions.[27]

6.21 In 2004 the Parliamentary Joint Standing Committee on the Australian Crime Commission recommended that the Commonwealth, State and Territory Attorneys-General give priority to implementing consistent cyber crime offence and evidence legislation.[28] The ABA was critical that this has not yet been fully realised.[29]

Committee View

6.22 The evidence to the Committee indicated that there has been considerable reform in the criminal law to adapt Australia's legal framework to the growth of malicious attacks against computers and computer systems. More recently the Attorneys-General have initiated improvements to ensure that identity theft/fraud is properly criminalised.

6.23 However, there is a need to maintain responsiveness to cyber crime and a dedicated cross jurisdictional working group is probably warranted. The idea for a working group is discussed at the end of this chapter.

6.24 The Committee is concerned with the current issue of uniformity of computer offences and those relating to identity fraud, which appears to be a continuing matter of concern. Lack of uniformity in Australian law makes both domestic and international cooperation more complex and inefficient. This is an issue that requires attention by the Attorneys-General of the Commonwealth and the State and Territory Governments.

6.25 On the scope of the existing provisions, the Committee believes that Symantec has expressed a legitimate concern that IT corporations and their staff could be exposed to possible criminal liability for possession, control, production or supply of 'data' (ss.478.3 and 478.4). However, each of these offences requires the prosecution to prove to the criminal standard (beyond reasonable doubt) that the possession, control,

---

26 Tasmanian Government, *Submission 51*, p.4.

27 ABA, *Submission 7*, p.7.

28 Parliamentary Joint Committee on the Australian Crime Commission, *Cybercrime,* March 2004, p.vii and p.15.

29 ABA, *Submission 7*, p.7.

production or supply of data was with intent to commit a computer offence. The Committee considers that, when all the elements are read together, the risk of mistaken prosecution or wrongful conviction is extremely remote.

6.26 On a related point, the Committee notes that intercepting communications is criminalised by the *Telecommunications (Interception and Access) Act 1979* (Cth). Recently proposed amendments are intended to ensure public and private network owners and operators can carry out 'computer network protection' activities such as using virus protection software without violating the prohibition on interception.[30]

Recommendation 8

That the Federal, State and Territory Attorneys-General review the existing computer and identity fraud provisions and, if necessary, introduce or amend provisions to ensure consistency across all Australian jurisdictions.

Law Enforcement Powers to Obtain Digital Evidence

6.27 The AFP told the Committee that the major challenge to domestic and foreign law enforcement agencies (LEAs) is the dynamic and trans-national nature of cyber crime. Some of the current key issues are:

- the ability to identify offenders who may be located in a different country to the victim and who can use technology to disguise their identity;
- the ability to quickly preserve, search and seize digital information, especially that protected by encryption or located in another country; and

30 *Telecommunications (Interception and Access) Amendment Bill 2009*; see also, AGD, *Discussion Paper and Exposure Draft Legislation: Computer Network Protection*, July 2009; The Senate Legal and Constitutional Affairs Legislation Committee, *Telecommunications (Interception and Access) Amendment Bill 2009 [Provisions]*, November 2009.

- the need for higher levels of international cooperation than that generally required for more traditional offline crimes.[31]

6.28 The convergence of new technologies, in particular, the growth of peer to peer and mobile phone technology was also identified as an additional challenge to shutting down botnets and collecting digital evidence for prosecution.[32] In particular, the AFP said that the ability of criminals to commit or facilitate offences through the use of disposable ICTs - such as prepaid mobile and wireless communications and free g-mail electronic addresses - will also restrict the ability of LEA's to obtain evidentiary material.[33]

Crimes Act 1914 (Cth) – Investigative Powers

6.29 Part IAA of the *Crimes Act 1914* (Cth) contains provisions which allow a law enforcement officer to search and seize electronic data. This includes provision for police to obtain an order to compel a suspect to access or provide assistance to access data that is evidence of the suspected offence. For example, revealing encryption keys or decryption data to enable police to obtain crucial evidence.[34]

6.30 It is currently an offence to fail to provide reasonable assistance to an LEA officer to access data stored on a computer at a search warrant premises (e.g. where the data is password protected or encrypted). The penalty is a maximum of six months imprisonment. The AGD advised that the Crimes Legislation (Serious and Organised Crime) Bill No.2 will amend the offence and increase the penalty from six months to two years.[35]

6.31 The *Crimes Act 1914* (Cth) also facilitates 'undercover' investigations. Part IAB allows a law enforcement officer to commit criminal offences as part of a controlled operation to investigate offences (including computer offences).[36] Part IAC allows law enforcement officers to use a false identity to investigate computer and telecommunications offences.[37]

---

31 AFP, *Supplementary Submission 25.1*, p.8; Russell Smith, *Impediments to the Successful Investigation of Transnational High Tech Crime*, Trends and Issues in Crime and Criminal Justice No. 285, Australian Institute of Criminology, October 2004, pp.1-6.

32 CLPC, *Submission 62*, p.3.

33 AFP, *Supplementary Submission 25.1*, pp.8-9.

34 Section 3LA of *the Crime Act 1914 (Cth).*

35 AGD, *Supplementary Submission 44.2*, p.8.

36 The offence must carry a maximum penalty of three or more years.

37 AGD, *Submission 44*, p.19.

Telecommunications (Interception and Access) Act 1979 (Cth)

6.32 The *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) has also undergone significant reform and allows for the interception of communications and access to historic and real time data.[38] However, the AFP said the capacity of some telecommunications carriers to meet their obligations under the TIA Act is insufficient and inhibits police investigations. In particular, some carriers have limited technical capacity to provide information required of them under the TIA. This information includes subscriber details, call log details and IP addresses.[39]

6.33 The TIA Act is administered by the Telecommunications and Surveillance Law Branch of the AGD. The TIA Act created the Communications Access Coordinator (CAC), who is the first point of contact for the telecommunications industry, LEAs and national security agencies:

> To assist industry to comply with their obligations, they are required to provide an interception capability plan on an annual basis which is assessed by law enforcement and national security agencies before being approved by the CAC. These plans outline how industry will meet their obligations under the TIA Act. The plans for 2009 have been approved and carriers range from very large organisations such as Telstra or Optus to smaller operators like Clear Networks. While some carriers have less capability, the CAC works with carriers to ensure they improve their capabilities as they grow their business.[40]

6.34 The Branch also administers an outreach program which 'provides extensive liaison and education for industry':

---

38 In 2005 the TIA was reviewed by Mr Anthony Blunn AO. The report, tabled in Parliament on 14 September 2005, recommended that legislation dealing with access to telecommunications data for security and law enforcement purposes be established, viewed 23 March 2010, <http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Blunnreportofthereviewoftheregulationofaccesstocommunications-August2005>. The TIA was amended in 2006 to establish a warrant regime for access to stored communications. In 2007 the TIA was further amended to implement a two-tier regime for access to historic and prospective (real-time) telecommunications data. The provisions of the *Telecommunications Act 1997* (Cth), that regulated access to telecommunications data for national security and law enforcement purposes, were also transferred to the TIA. See, Sue Harris-Rimmer, Telecommunications (Interception) Bill 2006, Bills Digest No. 102, 2005–06, 28 February 2006, Parliamentary Library; and, Bronwyn Jaggers, Telecommunications (Inception and Access) Amendment Bill 2008, Bills Digest No. 71, 7 March 2008 for further detail.

39 AFP, *Supplementary Submission 25.1*, p.9.

40 The Communications Access Coordinator is a statutory position performed by the First Assistant Secretary of the National Security Law and Policy Division in AGD; AGD, *Supplementary Submission, 44.2*, p.3.

> The program involves the provision of legal advice to industry on their obligations under the Act. Additionally, TSLB provides face to face assistance for carriers, carriage service providers and ISPs. These programs enable AGD to assist industry meet their obligations under the legislation and provide a foundation of co-operation in the provision of assistance to law enforcement.[41]

Surveillance Devices Act 2004 (Cth)

6.35 The NSW Police argued that remote access under warrant would allow for surveillance at the point before encryption occurs:

> A broader issue relating to cyber crime is police powers, such as 'remote access powers'. By allowing a warrant to be obtained for remote access, law enforcement is more likely to be able to decipher encrypted data by conducting surveillance at a point between the user and the encryption interface. This would involve remotely accessing (or 'hacking into') a computer via the internet to obtain transmissions of product passing over that computer at a point at which it is unencrypted. This would require legislative amendments both at a State and Commonwealth level.[42]

6.36 According to AGD this form of surveillance raises a range of technical, legal and privacy issues which have to be assessed against existing laws. For example, the use of a remote surveillance device may amount to interception under the TIA Act or violate the Criminal Code.

6.37 Additionally, it is the TIA Act which provides a national regime to regulate highly intrusive investigative powers, whereas the *Surveillance Devices Act 2004* (Cth) does not provide a national regime. In turn, this raises jurisdictional issues when such devices are deployed across inter-state boundaries.[43]

6.38 The Committee was told that a working group, which includes NSW law enforcement, government and other bodies, is currently considering these issues.[44] There was no evidence as to the timeframe for this work.

---

41 AGD, *Supplementary Submission 44.2*, p.3.

42 NSW Government, *Submission 49*, p.6.

43 AGD, *Supplementary Submission 44.2*, p.7.

44 AGD, *Supplementary Submission 44.2*, p.7.

Admissibility of Evidence

6.39 The AFP also identified the need to demonstrate the chain of handling of digital evidence and the lack of uniformity in evidence laws across Australian jurisdictions as two challenges to the admission of digital evidence in Australian courts. In particular, the ability to store, review and analyse voluminous data and a lack of tools/systems to 'robustly demonstrate chain of evidence handling of digital media' was an issue from a law enforcement point of view.[45]

6.40 The AGD agreed that practical handling of large volumes of complex material takes time and resources to conduct the necessary analysis. The analysis and presentation of digital evidence in court is made more complex if it has been subject to encryption.[46] Nevertheless, cyber crime, like other forms of crime must be established by admissible evidence. The AGD said:

> This includes proving continuity of digital evidence by presenting evidence of the chain of handling. Such evidence may be detailed given the involvement, for example, of computer forensic analysts, but this forms a necessary part of proving matters before criminal courts.[47]

6.41 In relation to uniform evidence law, the AGD advised that the Commonwealth, NSW, Victoria, Tasmania the ACT and Norfolk Island have adopted a harmonised approach under the Uniform Evidence Acts regime developed through the Standing Committee of Attorneys-General (SCAG).[48] The Department said that SCAG has an ongoing role in the harmonisation of evidence law.[49] There was no assessment of the status of that work or the likelihood of achieving uniformity in the near future.

Foreign business records

6.42 The NSW Police raised concern about the admissibility of records from, for example, Microsoft and Gmail, which are classed as 'business records'. It was suggested that such evidence should be admissible by 'information and belief' only rather than strict proof. Part 3 of the *Foreign Evidence Act 1993* (Cth) provides a means of adducing foreign evidence obtained through mutual assistance in Australian criminal proceedings. The AGD

45 AFP, *Supplementary Submission 25.1,* pp.9-10.
46 AGD, *Supplementary Submission 44.2*, p.7.
47 AGD, *Supplementary Submission 44.2*, p.7.
48 AGD, *Supplementary Submission 44.2*, p.7.
49 AGD, *Supplementary Submission 44.2*, p.7.

advised the Committee that amendments to that Act, currently before the Senate, would provide more flexibility in the testimony requirements but it will not go so far as to only require admission on the basis of the 'information and belief' of a law enforcement officer.[50]

6.43 The Department stressed the importance of preserving 'an appropriate balance' between individual rights and sufficient legal and judicial flexibility to secure international crime cooperation. The Department also said that its International Crime Cooperation Central Authority is experienced in working closely with the US Department of Justice to ensure evidence obtained from ISPs complies with the requirements for admission in Australian proceedings.[51]

International Cooperation

6.44 In the context of international cooperation, the AFP's evidence highlighted two particular issues:

- lack of timely access to evidence to identify offenders and for court proceedings; and
- inconsistent legislation in different countries that undermine investigative methods and prevent extradition and prosecution.[52]

6.45 AusCERT emphasised the importance when dealing with cyber crime for LEAs to be able to quickly secure digital evidence, often in multiple jurisdictions, to ensure that it is retained and the forensic quality of the evidence is preserved.[53] However, the AFP noted that getting information for forensic analysis from overseas ISPs and telecommunication services is often too slow to indentify an offender. Data is generally not received in time to be submitted to court and, in some cases, has taken up to eighteen months unless the investigation is high profile. Much of the international cooperation is done on a police to police basis because the formal mutual assistance regime is slow and makes it difficult to obtain evidence to identify offenders fast enough to enable a prosecution.[54]

6.46 Inconsistent legislation across countries can also mean that LEAs methods are sometimes thwarted. For example, inconsistent telecommunications intercept data retention laws can mean that evidence that would be

50 Foreign Evidence Amendment Bill 2008; AGD, *Supplementary Submission 44.2*, p.8.

51 AGD, *Supplementary Submission 44.2*, p.8

52 AFP, *Supplementary Submission 25.1*, pp.8-9.

53 AusCERT, *Submission 30*, p.15.

54 AFP, *Supplementary Submission 25.1,* pp.8-9.

available in Australia is not available where the service or data holdings are based in a foreign country.[55]

6.47 Inconsistent legislation or a lack of cyber crime offences can also mean that individuals based overseas escape extradition and prosecution for cyber offences because there is no similar offence in the country of origin (double criminality test).[56]

6.48 According to AGD the government to government processes for mutual assistance in criminal matters can take:

> … from a few days or weeks in very urgent or less complex cases, to several months or years in cases which require the collection of extensive material, or which relate to complex investigations. In contrast, requests for police-to-police assistance can sometimes be acted on much more quickly.[57]

6.49 The AGD told the Committee that Australia is already a party to approximately 25 bilateral treaties on mutual assistance in criminal matters.[58] Further, a comprehensive review of Australia's mutual assistance legal regime was completed recently and an exposure draft of the Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Bill released for public consultation in July 2009:

> A key intent of the reforms in this Bill is to streamline and modernise Australia's laws to ensure the mutual assistance regime is able to respond to advances in technology.[59]

6.50 Some of the proposed reforms include:

- provision for a warrant to covertly access stored communications (such as email records) for foreign law enforcement purposes; and
- allow the disclosure of existing data, such as subscriber details and call charge records without the need for a formal request from the foreign country (i.e. on a police to police basis).[60]

6.51 The draft exposure Bill was said to contribute to Australia's ability to meet Convention obligations and the Department is assessing whether any

---

55 AFP, *Supplementary Submission 25.1,* pp.8-9.
56 AFP, *Supplementary Submission 25.1*, pp.8-9.
57 AGD, *Supplementary Submission, 44.2*, p.4.
58 AGD, *Supplementary Submission 44.2*, p.4.
59 AGD, *Supplementary Submission, 44.2*, p.5.
60 AGD, *Supplementary Submission, 44.2*, p.5.

additional changes are needed to meet the international cooperation obligations.[61]

6.52 In addition to these reforms, AGD agreed that participation in the Council of Europe Convention on Cybercrime would increase Australia's ability:

> … to obtain international assistance from other parties to the Convention in investigating potential cyber crime offences, particularly in relation to accessing telecommunications.[62]

6.53 The Council of Europe Convention on Cybercrime is discussed below.

Committee View

6.54 The evidence indicated that there has been a considerable expansion in police powers to ensure that LEAs are able to adapt investigative methods to the high tech environment. There appears to be an ongoing program of legal policy development in response to problems as they are identified. Some of those reforms (identity fraud, foreign business records) were before the Parliament during this inquiry. Reform of the mutual assistance regime to respond to new technology was released for public consultation in July 2009. These measures go some way to strengthening law enforcement capability in relation to high tech crime.

6.55 However, the Committee is concerned that many Australian ISPs and telecommunications carriers appear to be unable to meet their statutory obligations under the TIA Act. The role and responsibilities of ISPs are discussed in the next chapter, where it is noted there are between 500-600 ISPs currently in operation in Australia alone. This problem is magnified when dealing with ISPs overseas, especially where the laws on the retention of data vary.

International Legal Framework

6.56 As has been noted throughout this report, a significant portion of cyber crime experienced by Australians originates from overseas. This makes international cooperation critical to efforts to criminalise, detect, disrupt, prevent, and ultimately to pursue effective law enforcement action.[63]

---

61 AGD, *Supplementary Submission, 44.2*, p.5.

62 AGD, *Supplementary Submission, 44.2*, p.4.

63 Internet Safety Institute, *Submission 37*, p.7; Microsoft Australia, *Submission 35*, p.1.

6.57 The UN International Telecommunications Union (ITU) is active on the issue of cyber crime but there is no UN sponsored international treaty dedicated to this specific subject matter. The Australian Bankers Association (ABA) advocated a more proactive stance by Australia in international fora for the development of an international legal regime targeting cyber crime.[64]

6.58 In particular, it argued for a review and, if necessary, an extension of the existing UN Convention on Transnational Organised Crime (and relevant bilateral agreements), to address the problem of cyber crime. The ABA also expressed concerns about the adequacy of the implementation of that treaty, including in the area of mutual legal assistance.[65]

Council of Europe Convention on Cybercrime

6.59 The most relevant international treaty on this subject is the Council of Europe Convention on Cybercrime (the Convention), which is designed to promote the harmonisation of national laws on cyber crime and to aid international law enforcement cooperation.[66]

6.60 Mr Alexander Seger, Head of the Economic Crime Division, Council of Europe informed the Committee that, although the Convention was developed by the Council of Europe, it was designed to have global scope and Non-member States of the Council of Europe have been encouraged to sign and ratify the treaty.[67] The USA, Canada, Japan and South Africa participated in the treaty's preparation and have signed, and in the case of the USA, have ratified the treaty:

> By the end of June 2009, 26 countries were full parties to the Convention, while an additional 20 had signed it and another 5 had been invited to accede. A further 50 to 70 countries are using the Convention as a guide and have or are in the process of adapting their cybercrime legislation along the lines of this treaty.[68]

---

64 ABA, *Submission 7*, pp.9-12.

65 ABA, *Submission 7*, pp.9-12.

66 Convention on Cybercrime, European Treaty Series No.185 (opened for signature Budapest 23.11.2001 entered into force 1.7.2004).

67 Directorate General of Human Rights and Legal Affairs, Council of Europe, *Submission 31*, p.3.

68 Council of Europe, *Submission 31*, p.3; at the time of writing 27 countries had signed and ratified or acceded to the treaty and 19 had signed the treaty but not yet proceeded to ratification, viewed 11 March 2010, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=11/03/2010&CL=ENG>.

6.61 Any country can seek accession and then be invited to accede. Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines have been invited to accede and it is expected that by the time of accession these countries will have harmonised their national law with the Convention.[69]

6.62 Several witnesses urged the Committee to recommend that the Australian Government seek accession to the Convention.[70] The Council of Europe emphasised that efficient international cooperation is crucial to combat cyber crime and to secure evidence on computer systems:

> For that reason, the Convention contains a range of general and specific measures to facilitate cooperation and allow the use of domestic measures (such as the expedited preservation) also in relation to international cooperation.[71]

6.63 To support the implementation of treaty obligations, the Council of Europe has produced Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime.[72]

6.64 The Council of Europe also pointed out a number of other benefits including the ability of States parties to participate in the Cybercrime Convention Committee, which monitors treaty implementation and initiates future work, such as the elaboration of additional protocols.[73] Australia's accession to the treaty would also serve as a positive example to other countries in the Asia Pacific region.[74]

6.65 In preliminary comments on Australian law, the Council of Europe observed that substantive offences appear to be already covered:

> …although – perhaps due to the specifities of the Australian legal system – a different approach seems to have been followed for some of them. For example, in some Australian legal provisions different types of conduct listed in the Convention have been combined (e.g. illegal access, data interference, system interference) or individual provisions of the Convention are reflected in several different provisions in Australia. This is

---

69 Council of Europe, *Submission 31*, p.3.

70 Microsoft Australia, *Submission 35*, p.9; Queensland Government, *Submission 67*, p.7; AIIA, *Submission 22*, p.3; AusCERT, *Submission 30*, p. 15.

71 Council of Europe, *Submission 31*, p.4.

72 Project Cybercrime, viewed 23 March 2010 <www.coe.int/cybercrime>. Adopted by the Global Conference Cooperation against Cybercrime, Council of Europe, Strasbourg, 1-2 April 2008.

73 Council of Europe, *Submission 31*, p.5.

74 Council of Europe, *Submission 31*, p.5

> compatible with the Convention but may create difficulties in international cooperation when applying dual criminality.[75]

6.66 In relation to procedural law and practice the Council of Europe commented that:

> …it seems that some tools (search and seizure, production order etc) are available, while others are not (e.g. expedited preservation).[76]

6.67 The AGD told the Committee that Australia is already compliant with some obligations contained in the Convention but:

> There remain a number of complex issues that the Government will need to consider, some of which may require significant legislative amendment. The Australian Government is currently reviewing existing domestic legislation to identify what action may be necessary to implement the Convention in Australia's domestic law, should it decide to become a party to the Convention.[77]

6.68 Specifically, the AFP suggested that some amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) may be necessary.[78] The Committee noted, for example, that intercept material obtained by police under the TIA Act cannot be shared with foreign countries.[79]

6.69 The Council of Europe offered its assistance in conducting a detailed analysis to assess whether Australian legislation and practice is fully in line with the Convention.[80] Microsoft Australia also provided the Committee with a study of computer security, privacy, spam and online child safety laws in 14 countries across the Asia Pacific Region. The study included analysis of Australian cyber crime laws benchmarked against the Convention.[81]

---

75 Council of Europe, *Submission 31*, p.4.

76 Council of Europe, *Submission 31*, p.4.

77 AGD, *Submission 44*, p.14.

78 AFP, *Transcript of Evidence,* 9 September 2009, p.11.

79 Section 13A of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) expressly excludes material obtained under the TIA from being provided to a requesting foreign country to assist in an investigation or proceedings for a serious offences against that country's domestic law.

80 Council of Europe, *Submission 31*, p.4.

81 Microsoft Australia, *Submission 35,* pp. 6-10; Microsoft Corporation Ltd, *Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws: A Study by Microsoft*, November 2007, viewed 10 March 2010, <www.microsoft.com/asia>.

6.70 The study found there was a strong alignment of Australia's current cyber crime framework with the Convention's 'core offences' of data interference; computer related forgery and fraud offences; and corporate criminal liability for cyber crime.[82] However, it found that there is scope to strengthen provisions on illegal access, system interference and misuse of device offences.[83] Specifically, Microsoft Australia said:

> The Code's unauthorised access offence only applies in respect of data that is protected by an access control system (this qualification is permitted by the Convention).
>
> The Code's data interference offence is likely to regulate a broader range of conduct than its Convention counterpart due to its application to reckless data interference as well as that caused intentionally.
>
> …
>
> The Code does not contain an equivalent to the Convention's system interference offence, but its unauthorised impairment of electronic communications offence is targeted at denial of service attacks in the same way that the Convention system interference offence is (at least in part).[84]

6.71 Finally, in respect of producing, supplying, possessing or procuring data (which is defined as including computer programs) with intent to commit a computer security offence, Microsoft said these 'are best viewed as a partial implementation of the Convention's misuse of devices offence'.[85]

6.72 Overall, however, Microsoft Australia concluded that:

> … Australia has demonstrated a solid commitment to robust legislation, but could further strengthen some of these provisions in closer alignment with the Cybercrime Convention. Australia has already been playing an important role in achieving regional and global consistency. It is effectively functioning as a policy bellwether for the region.[86]

6.73 Finally, the Cyber Space Law and Policy Centre (CLPC) pointed out that some of the special evidence gathering obligations of the Convention raise significant privacy issues. As Australia does not have a domestic Charter

82 Microsoft Australia, *Submission 35*, p.7.
83 Microsoft Australia, *Submission 35*, p.7.
84 Microsoft Australia, *Submission 35*, p.8.
85 Microsoft Australia, *Submission 35*, p.7.
86 Microsoft Australia, *Submission 35*, p.8.

of Rights and Freedoms against which such provisions can be independently assessed, the CLPC advised that these provisions should be subject to careful scrutiny before being implemented in Australia.[87]

Committee View

6.74 The transnational nature of cyber crime and the importance of consistency in both the substantive offences and procedural law to strengthen international cooperation make the review and, if necessary, amendment of Australian laws an important priority for all Australian governments. The Convention was finalised in 2001 and entered into force in 2004. At the time of writing in 2010, 46 countries had either signed or signed and acceded or ratified the Convention, including the USA, Australia's major partner in fighting transnational cyber crime.

6.75 The majority of evidence to the Committee indicates that Australian law is already substantially aligned with the offence provisions and some procedural aspects of the Convention. However, the Committee is concerned that Australia's progress has been too slow and is disappointed that AGD's evidence lacked a clear framework for action and specific timetable for seeking accession to the Convention.

6.76 There is general agreement that Australians are benefitting from the high level of ICT penetration into the Australian economy and increasing IT literacy across the community. In light of the importance of ICTs, the Committee believes that Australia governments should give priority to finalising the internal review and necessary reforms and move expeditiously toward seeking accession to the Convention. The shaping of Australian law to comply with the Convention should also take into account Australia's existing obligations under the International Covenant on Civil and Political Rights.

6.77 Overall, however, the Committee believes that Australia's participation will strengthen international law enforcement cooperation and enable Australia to participate in future treaty development and influence global legal regimes. Participation in the treaty will also support Australia's work in other international fora and the Asia Pacific Region.

87 CLPC, *Submission 62.1*, p.3.

Recommendation 9

That the Federal Attorney-General, in consultation with State and Territory counterparts, give priority to the review of Australian law and practice and move expeditiously to accede to the Council of Europe Convention on Cybercrime.

Tackling Botnets

6.78 There is wide agreement among police, researchers, IT security companies and governments around the world that botnets are the key tool for the commission of cyber crime:

> Botnets are said to be involved in most forms of cybercrime and civil wrong ranging from sending spam, to denial of service attacks, to child pornography distribution, to worm propagation, to click fraud, to keylogging technology and traffic sniffing which captures passwords and credit card information, and to mass identity theft.[88]

6.79 Similarly, Microsoft Australia emphasised that:

> As online criminals increasingly access and control protected networks of computers remotely and without authorisation, creating "botnets" of literally hundreds of thousands of machines that are used to attack other machines, perpetrate identity theft, spread spyware and malware, or disrupt Internet functions, more needs to be done to identify, stop and prosecute these criminals ("botherders").[89]

6.80 The IIA argued that since the passage of the *Cybercrime Act 2001* cyber crime has become more sophisticated and moved from one-off events to organised crime on an industrial scale. Cyber crime now relies on thousands of infected home computers exposing more general weaknesses in the current regime.[90] From IIA's perspective the problem is not the lack of a legal framework but the inability of traditional institutions to respond to the complexity of cyber crime. It was argued that tackling botnets

88 CLPC, *Submission 62*, p.3; Rychlicki T., *Legal Issues of Criminal Acts Committed Via Botnets* (2006) Computer and Telecommunications Law Review 12 (5), p.163 as cited CLPC, *Submission 62*, p.3.

89 Microsoft Australia, *Submission 35*, p.

90 For example, IIA, *Submission 54*, p.2.

requires a more concerted effort, and the lack of prosecutions and light sentences has contributed to a lack of community awareness of the problem.[91]

6.81 The IIA were not alone in this view. The CLPC, Microsoft and Sophos also stressed the importance of tackling the botnet infrastructure, by identifying and neutralising botnets and targeting botnet herders.[92]

6.82 As noted in Chapter 5, the CLPC was critical that law enforcement strategy puts little emphasis on prosecuting botherders or addressing botnets run by organised crime.[93] The CLPC said that 'cyber crime policy should place a significant emphasis on the disruption and dismantling of botnets, as opposed to the mere prosecution of botnet herders'.[94]

6.83 In one case, the AFP identified distributed denial of service attacks committed by botnets containing more than 100,000 compromised computers across more than 120 countries:

> …the ability of law enforcement to investigate and prosecute individuals behind such attacks is often thwarted by the transnational nature of the Botnet make up and control systems.[95]

6.84 The Committee was also told that to prosecute a person running a botnet the police would need statements from potentially thousands of individuals that the perpetrator did not have authority to enter and operate their computer.[96] However, AGD disagreed and told the Committee that the Commonwealth Director of Public Prosecutions is able to prosecute on the basis of representative charges, which establish a course of conduct by the defendant together with forensic evidence to show how the botnet operated.[97]

6.85 Fujitsu told the Committee, that in their view, there are gaps in the law and policy that would support a more strategic approach. For example:

- insufficient legislation that targets the criminal underground economy, the people involved, and the tools they use to write malware;
- restrictions on the deployment of tools to identify suspects; and

---

91 IIA, *Submission 54*, p.5.

92 See CLPC, *Submission 62*; Microsoft Australia, *Submission 35*; Sophos, *Submission 66*.

93 CLPC, *Submission 62*, p.3.

94 CLPC, *Submission 62*, p.3.

95 AFP, *Submission 25,* p.9.

96 AFP, *Supplementary Submission 25.1,* pp. 9-10.

97 AGD, *Supplementary Submission 44.2,* p.8.

- lack of legislation that allows law enforcement or other entities to deploy technical capability to remove virus/trojans/malware from victims.[98]

6.86 David Jones, ThreatMetrix Pty Ltd also argued for a fresh look at cyber crime laws to better respond to the current environment of botnets and compromised hosts.[99]

6.87 In response to a question from the Committee about the ability to conduct network wide strategies, the AGD advised that existing Criminal Code Part 10.7 computer offences would be violated if an anti-malware program intended to disinfect PCs were released to combat a widely distributed virus.[100]

Committee View

6.88 Since the introduction of computer offences the problem of cyber crime has moved onto an industrial scale organised through loose networks. There was a clear message that the IT security companies are unable to entirely protect their customers and traditional law enforcement methods are unlikely to get on top of this problem. Legal policy and law enforcement strategy also needs to:

- target the underground cyber crime economy;
- target the botherders;
- tackle botnets through disruption; and
- remediate compromised computers (See Chapter 7).

6.89 The Committee noted concerns that police lack sufficient tools to identify offenders or deploy technical capability to remove malicious software. In the Committee's view, Australian LEAs must have the tools needed to work with international partners in a concerted effort to tackle the botnet problem and prosecute the members and leaders of organised criminal networks.

98 Fujitsu, *Submission 13*, p.7.

99 ThreatMetrix Pty Ltd, *Submission 19*, p.14.

100 AGD, *Supplementary Submission 44.2*, p.2.

Recommendation 10

That Australia's cyber crime policy strategically target the underground economy in malicious IT tools and personal financial information; the disruption of botnets and the identification and prosecution of botherders .

Future Initiatives

6.90 The NSW Government argued that, while it had introduced specific computer and identity crime offences, this should 'only be the beginning of legislative reforms to tackle cyber crime'.[101] In particular, NSW argued that the computer offences are 'focused on the hardware rather than cyberspace more generally' and the identity crime offences are aimed at the members of syndicates rather than the head of those organisations/networks that develop the means to obtain the information.[102]

6.91 To maintain a coordinated and ongoing legislative reform effort, the NSW Government recommended that a national cyber crime working group be established to develop legislative initiatives for cyber crime for both Commonwealth and State jurisdictions to implement.[103] The working group would report to the appropriate Ministerial Council. It was suggested that this group could also give further consideration as to whether Australia should become a signatory to the Council of Europe Convention on Cybercrime. From NSW's perspective, the group should include a cross section of policy staff from justice and law enforcement agencies, including significant input from the AFP High Tech Crime Operations Centre.[104]

Committee View

6.92 There does not appear to be any existing dedicated cross jurisdictional working group on cyber crime, although the Commonwealth may consult on specific initiatives. Many issues would be dealt with via the Model Criminal Code Officers Committee, which reports to SCAG. As noted

101 NSW Government, *Submission 49*, p.5.
102 NSW Government, *Submission 49,* p.5.
103 NSW Government, *Submission 49*, p.6.
104 NSW Government, *Submission 49*, p.6.

above, the Committee is satisfied there have been significant reforms in this area.

6.93 However, there is a need to remain responsive to the evolving nature of cyber crime. Consequently, the Committee sees some merit in a specialist working group dedicated to cyber crime that can be focused and responsive. In particular, this group should put a high priority on facilitating international cooperation in the investigation of organised criminal networks and the problem of botnets.

Recommendation 11

That the Commonwealth, State and Territory governments establish a national working group on cyber crime to maintain an ongoing, dedicated mechanism for the review and development of legislative responses to cyber crime.

That the working group take a whole of cyberspace perspective and consider relevant IT industry, consumer protection and privacy issues as well as the criminal law.

7

Protecting the Integrity of the Internet

Introduction

7.1 This chapter discusses current and future initiatives for promoting a more secure Internet environment. In particular, it considers the role of the Australian Communications and Media Authority (ACMA), Internet Service Providers (ISPs), and Domain Name Registrars and Resellers in promoting greater resilience within the Australian Internet networks.

7.2 The chapter focuses on six key issues:

- the effectiveness of the Australian Internet Security Initiative (AISI) to detect and drive the remediation of bots;
- the role of ISPs in the AISI and the proposed Internet industry e-security code of practice;
- remediation of infected computers;
- ACMA's capacity to respond to the threat of compromised websites;
- ACMA's spam reporting initiative and the role of ISPs under the *Spam Code of Practice*; and
- e-security and the Domain Name Registration System.

Australian Internet Security Initiative

7.3 The ACMA is a statutory authority within the Australian Government portfolio of Broadband, Communications and the Digital Economy. The

ACMA is responsible for regulating broadcasting, the Internet, radio communications and telecommunications.[1]

7.4 The ACMA developed the AISI in 2005. The AISI identifies computers operating on the Australian Internet that have been infected by malware and are able to be controlled for illegal activities.[2] The Committee was told that AISI has been progressively expanded over time and has attracted international interest.[3]

7.5 As noted previously in this report, 99 per cent of spam is sent from botnets.[4] Spam email is one of the primary vectors of malware and the dissemination of scams and phishing attacks on end users. By detecting malware infected computers, regulators can address the problem of spam and make strategic in roads into the problem of botnets. The AISI recognises that link and is intended to target the source of the spam problem by detecting compromised machines and botnet activity.[5]

7.6 In essence, AISI is a 'data handler' system that collates data into one central database and enables ACMA to standardise the information. ACMA issues daily reports to ISPs about types of compromises detected in their customers' machines.[6] ACMA explained:

> Through the AISI, the ACMA collects data from various sources identifying IP address that have been detected as exhibiting 'bot' behaviour on the Australian internet. Using this data, the ACMA provides daily reports to participating … ISPs identifying IP addresses on their networks that have been reported as compromised (infected with malware) in the previous 24-hour period.[7]

7.7 There has been a steady increase in the number of compromises reported daily through the AISI, and 'a marked increase since March 2009'.[8] In June 2009, ACMA was reporting more than 10,000 individual compromises per day to Australian ISPs. At the hearing on 21 October 2009, Mr Bruce Mathews, Acting Executive Manager, Strategy and Coordination Branch, ACMA, submitted that the prevalence of botnets on the Australian

1 The ACMA was established on 1 July 2005 by the merger of the Australian Broadcasting Authority and the Australian Communications Authority.

2 ACMA, *Submission 56*, p.3.

3 Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October, 2009, p.2.

4 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.10.

5 ACMA, *Submission 56*, p.3.

6 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.7.

7 ACMA, *Submission 56*, p.3.

8 ACMA, *Submission 56*, p.5.

internet remains of considerable concern and warrants the attention of the Committee.[9]

7.8 The data obtained through AISI is expanding due to:

- an increase in the number of sources and improvements in compromise data resulting in the identification of more malware types and infected machines;
- an expansion in the number of ISPs participating in AISI providing greater coverage of Australian IP addresses;
- an expansion of IP address ranges by ISPs to provide for customer growth; and
- more comprehensive IP address range information provided to ACMA.[10]

7.9 The Committee was also told that the increased number of reported compromised machines has required a 'substantial increase in ACMA resources':

> ACMA's interaction with ISPs and their customers – the latter being usually via the ISP – has increased markedly since March 2009. These most generally involve the ACMA providing further information on individual compromise reports in response to enquiries.[11]

7.10 The effectiveness of the AISI depends on three elements:

- access to information on zombie computers and botnet activity;
- the willingness and capacity of ISPs to take action; and
- the ability of end users to remediate infected computers and protect themselves in the future.

7.11 These issues are discussed in the following sections.

Access to Network Data

7.12 Access to network data is vital to detecting IP addresses of compromised machines and botnet activity. ACMA told the Committee that network

9 Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October, p.2.

10 ACMA, *Submission 56*, p.5.

11 ACMA, *Submission 56*, p.8.

data comes from a range of sources, including some on a confidential basis:

> The AISI collects data from a number of parties who run honeypots, spamtraps, sinkholes and other mechanisms for the purpose of identifying compromised hosts or other malicious activities on the internet.[12]

7.13 To ensure access to this information ACMA often agrees 'not to disclose the operations, tools, methods and infrastructure utilised by its partners'.[13] The publicly acknowledged sources are The Shadowserver Foundation[14], The Australian Honeynet Project,[15] and SORBS (Spam and Open Relay Blocking System).[16] The ACMA also operates its own honeypots and spamtraps.[17]

7.14 The Committee heard there is also a vast wealth of network intelligence available from global IT companies that could be tapped by government. As noted in Chapter 5, Symantec told the Committee that it possesses a rich repository of intelligence data. The issues raised by Symantec in relation to sharing real time cyber threat intelligence are also relevant to the sharing of network data in the context of AISI. In particular, the extent to which authorities monitor the data, who the data is shared with, where the data is stored and legal implications regarding privacy are all pertinent.

7.15 Sophos also pointed out the high commercial value of data from filtering technologies that identify the IP addresses of botnets. The Committee was told that this data is not likely to be shared openly between competitors.[18]

7.16 Sophos said:

> Although ACMA/AISI is already tackling this problem, with additional co-operation … Australia could be seen to be leading the world in anti-botnet activity, and to encourage such a process to be rolled out as worldwide best practice.[19]

---

12 ACMA, *Supplementary Submission 56.1*, p.2.
13 ACMA, *Supplementary Submission 56.1*, p.2.
14 <http://www.shadowserver.org/>.
15 <http://www.honeynet.org.au/>.
16 <http://www.au.sorbs.net/>.
17 ACMA, *Supplementary Submission 56.1*, p.2.
18 Sophos, *Submission 66*, p.6.
19 Sophos, *Submission 66*, p.6.

7.17 As a step toward greater cooperation with the private sector, Sophos proposed that interested security vendors, together with government, should consider mechanisms to increase data sharing on botnets.[20]

Internet Industry Participation

7.18 The Internet industry has grown rapidly over the past decade and it was estimated there are now between five to six hundred ISPs currently operating in Australia.[21] Although large companies such as Telstra and Optus have the largest share of the market, a significant proportion of the industry is made up of small providers. Elsewhere it has been estimated that more than a quarter of ISPs have an annual turnover of less than $3 million.[22]

7.19 The Committee heard that ISPs occupy a unique position as the only party that can link an individual user to an IP address identified by AISI.[23] And ACMA emphasised the importance of this role in the overall national strategy to combat cyber crime.[24]

7.20 The AISI started as a pilot project in 2005 with six ISPs. The Committee was told that 'the 2007 Budget allocated approximately $4.7 million (over four years) to enable the expansion of the AISI to all Australian ISPs who wish to participate'.[25] There are now 71 ISPs participating in the scheme, which ACMA estimated covers 90 per cent of Australian residential customers.[26]

7.21 ACMA's published statement to the ISPs states:

> There are no costs to ISPs associated with participation in the AISI. It is a free service provided by ACMA to assist in reducing spam and to improve the security level of the Australian internet. By participating, you will contribute to the overall reduction of spam and e-security compromises, thereby reducing costs for all ISPs.[27]

7.22 The ACMA also states that:

---

20 Sophos, *Submission 66*, p.6.

21 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.6.

22 See *ALRC Report 108*, pp.1330-1331; see also, Office of the Privacy Commissioner, *Submission Draft Internet Industry Association eSecurity Code of Practice*, p.3.

23 Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, 25 November, 2009, p.9.

24 ACMA, *Submission 56*, p.23.

25 IIA, *Submission 54*, p.7.

26 ACMA, *Submission 56*, p.3; Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.1.

27 <http://www.acma.gov.au>, viewed 27 May 2010.

> The number of compromises listed in the daily AISI reports will vary considerably for each ISP, depending on the customer base of the ISP and the quantity of the information feeding into the AISI on a given day. Large ISPs may receive hundreds (and in some cases thousands) of compromises per day, whereas some smaller ISPs may rarely get any reports.[28]

7.23 In the absence of Australian data, ACMA pointed the Committee to a 2008 survey by Arbor Networks of 66 IT network operators from North America, South America, Europe and Asia that 'indicated considerable support from ISPs in combating botnets':

> We also asked if respondents believe that ISPs should be responsible for detecting and monitoring botnets. Sixty-one percent said Yes, while 23 percent disagreed, and another 17 percent responded Yes, with some criteria.[29]

7.24 The Committee was also told that ISPs are dedicating resources to addressing compromised computers, and, as ACMA pointed out, have a commercial interest in addressing bot malware.[30] Some ISPs utilise independent sources of compromise data separate to those fed into the AISI system, and some have developed their own internal systems to identify compromised IP addresses. Although the volume of IP addresses identified this way was unknown, ACMA expects it to be a significant number.[31]

7.25 Mr Peter Coroneos, CEO, Internet Industry Association (IIA), informed the Committee that ISP members see a 'win-win benefit' because malware infected machines are a 'threat to the integrity of the network itself'.[32]

7.26 It was also suggested that ISPs could benefit further from selling a remediation service or getting commission from the sale of anti-virus products at the point of selling the Internet connection.[33]

7.27 The Committee was told that 'best practice' requires that an ISP identify the customer, reduce their access to the Internet, provide the support and advice to remove the compromise, and then reinstate the normal service.[34]

---

28 <http://www.acma.gov.au>, viewed 27 May 2010.

29 Arbor Networks, *Worldwide Infrastructure Security Report,* Volume IV, October 2008, p.23 as cited in ACMA, *Submission 56*, p.23.

30 ACMA, *Submission 56*, p.22.

31 ACMA, *Submission 56,* p.5.

32 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.15.

33 Mr Mike Rothery, AGD, *Transcript of Evidence*, 25 November 2009, p.10.

34 Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, 25 November, 2009, p.10.

However, in practice, there is considerable variation in the way ISPs respond to compromised machines operating across their networks.[35]

7.28 Mr Bruce Mathews, ACMA, said the level of assistance provided by ISPs to end users varies 'very significantly':[36]

> ISPs are prepared to voluntarily take actions to combat bots and botnets. The AISI is not a mandatory program and … ISPs currently participate in the program at the level they consider appropriate to their own resources, systems and processes for customer interaction.[37]

7.29 AISI is a purely voluntary scheme. There is no mechanism for monitoring ISP action, or whether the infected machine has been remediated.[38] Consequently, there is no data to show how many AISI reports actually result in clean-up of infected computers. Nor does ACMA have any power to order the quarantining or disconnection of a machine if an ISP declines to take action or an end user fails to remediate the problem.[39]

7.30 While the best approach is said to be contacting the customer by phone, this is not 'economically feasible' given that some large ISPs can 'receive 2,000 reports per day'.[40] An alternative is to notify customers by email and then monitor whether there is a response. In some instances, the ISPs do not notify customers at all, some take AISI data and correlate it to their own information, other ISPs take a graduated approach and, in a severe case, will disconnect a customer (see below).

7.31 The IIA advised the Committee that some of the larger ISPs have already developed automated systems for notifying their customers as a way of dealing with the volume of reports received, while smaller ISPs may call their customers and use it as an opportunity to maintain their customer relationship. One example of how some ISPs are responding to the problem of zombie computers is Queensland based ISP, Dreamtilt, which has a clear statement informing customers about their participation in AISI and what to do in the case of a notification:

> What if I receive an notification from Dreamtilt?

---

35 Mr Keith Besgrove, DBCDE, *Transcript of Evidence,* 25 November 2009, p.9; ACMA, *Submission 56*, p.3.

36 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.6.

37 ACMA, *Submission 56*, p.22.

38 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, pp.3-4.

39 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.3.

40 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.4

> As part of our commitment to the Australian Internet Security Initiative, Dreamtilt aims to inform all customers which may have a zombie computer. If you receive an email from Dreamtilt in regards to an infected zombie computer, follow the instructions in the email. If the problem continues please review our Support section or call us on ... . If the problem cannot be rectified by support from Dreamtilt you may need to visit a computer technician. We have a number of resellers that can offer such a service and can be viewed here. Under our Terms and Conditions, if a computer is found to be affected or vulnerable you will be given 7 days to cleanse your computer. If the problem has not been rectified during this time, we may put your connection on hold until the problem is rectified.[41]

7.32 Telstra, the largest ISP in Australia, explained their approach to the issue:

> Telstra gathers lists of potentially infected systems from a large number of sources including from the ACMA AISI. This provides Telstra with a variety of information which it can use to verify that such reports are not false positives or other errors.
>
> All information gathered is processed in Telstra systems to allow tracking of which subscribers are potentially infected, what they are infected with and when and how Telstra has contacted them. The majority of contact made with customers is done via email as this is the preferred method of communication specified by our customers, this is also an automated process to allow tracking of who has received the email and what emails have not been delivered for various reasons.[42]

7.33 In 2009, ACMA undertook 'a brief survey of a subset of AISI participants (those who had received a threshold level of AISI reports)'.[43] The responses indicate a diverse range of actions including:

- limiting the data rate for accessing the Internet, and emailing the customer advising of the infection and the need for remediation;
- temporary suspension of accounts of re-offenders;
- placing the customer's internet service in a 'walled garden';[44]

---

41 <http://www2.dreamtilt.com.au/index.php/internet-services/wireless-broadband/installation/159-aisi.html>, viewed 27 May 2010.

42 Correspondence to the Committee, Jamie Snashall, Senior Adviser Government Relations,Telstra Corporation Ltd, 1 June 2010.

43 ACMA, *Submission 56*, p.22.

- temporary suspension to the 'offending ports and protocol activity'; and
- regenerating account passwords (thereby preventing customer access to the Internet) in order to prompt a call to the ISP's helpdesk.[45]

7.34 These measures are being incorporated in a new voluntary Internet Industry *E-Security Code of Practice,* which is discussed in more detail below.

End User Attitudes

7.35 The evidence on end user attitudes was also mixed. Sophos told the Committee that anecdotally some customers are dismissive or defensive when contacted.[46] The IIA described notifying an end user their computer is infected as akin to telling someone they have 'digital bad breath' although many ISPs subscribers appreciate receiving the information.[47]

7.36 The Committee also heard that:

> Anecdotal information from ISPs … indicates that some customers are continually identified in the AISI reports, which has resulted in the adoption of escalated procedures by many ISPs for these 'repeat offenders', including termination of their internet accounts in the most extreme cases.[48]

7.37 In 2008, AusCERT commissioned research into end user attitudes towards a range of personal Internet security issues. The AusCERT *Home Users Computer Security Survey 2008* found that 92 per cent of the 1,000 respondents wanted their ISP to let them know their computer was compromised. The survey also found that:

- 29 per cent were prepared for their ISP to disconnect them completely from the Internet until the computer was fixed;
- 89 per cent said they would want the ISP to provide them with assistance to fix the problem; and

44 In this context, placing an end user in a 'walled garden' means restricting Internet access from that computer only to approved IP addresses.

45 ACMA, *Submission 56*, p.22.

46 Sophos, *Submission 66*, p.6.

47 IIA, *Submission 54,* p.8.

48 ACMA, *Submission 56*, p.8.

- 61 per cent thought it preferable for the ISP to reduce their access to a few websites to help correct the problem.[49]

7.38 AusCERT concluded that end users recognise that remaining connected to the Internet while compromised 'is neither in their best interests nor in the interests of the Internet community more generally'.[50] A smaller but still significant proportion of 14 per cent took no action, even when a malware infection had been confirmed. While this latter finding is worrying, overall the survey results were considered positive and suggest that end users want information, advice and assistance.

Committee View

7.39 The AISI is an innovative and world leading initiative that illustrates the benefit of public-private cooperation to address a significant societal problem. However, the Committee is concerned that, in this current form, the AISI is unlikely to realise its full potential unless there is a clearer commitment to notify an end user when their PC is operating as a zombie computer. The impact of AISI on remediation by end users is ad hoc and difficult to measure because of the wide variation in ISP responses. The Committee also noted there was no evidence that AISI data is shared with CERT Australia to support other threat assessment or emergency response functions.

7.40 As Chapter 2 demonstrates, there is wide agreement that end users are highly vulnerable to being coopted into botnets that are the primary tools of mass automated global cyber crime. The problem of malware has grown as cyber criminals become increasingly sophisticated and this trend is predicted to continue. The expansion in the number of residential and business Internet connections will also continue to impact on the scope of the problem.

7.41 In the Committee's view, the size, nature and complexity of malware infections and the problem of botnets warrants a more concerted effort led by government but involving all parties in a cooperative effort to reduce the number of zombie computers operating in Australia. A more integrated model built on AISI, involving ISPs, IT security specialists, and end users in a more tightly coordinated scheme will, in our view, yield better results. That said, the Committee recognises that some ISPs will obtain their network data from their own sources.

---

49 AusCERT, *Home Users Computer Security Survey 2008*, p.30.

50 AusCERT, *Home Users Computer Security Survey 2008*, p.30.

7.42 Nevertheless, as part of an expanded but more integrated scheme, the Committee recommends that ACMA should further increase its access to network data. This should include:

- active consideration of how to increase access to network data held by global IT security companies;
- whether legal reform is desirable to protect the commercial sensitivity of data, and address the regulatory, privacy concerns and other related issues raised by IT security vendors who participated in this inquiry;
- how best AISI network data might be used to support other threat assessment and emergency response functions of government.

Recommendation 12

That the Australian Communications and Media Authority further increase its access to network data for the purpose of detecting malware compromised computers. This should include active consideration of how to increase access to network data held by global IT security companies and, in consultation with relevant departments, whether legal protections to address commercial, regulatory and privacy concerns are desirable.

Recommendation 13

That the Australian Communications and Media Authority consider how best the Australian Internet Security Initiative network data might be used to support the threat assessment and emergency response functions of government.

Internet Service Providers – E Security Code of Practice

7.43 As a result of the *E Security Review*, the Australian Government has encouraged the Internet industry to develop an e-security code of practice for ISPs. The Committee heard that the e-security code of practice is being developed by IIA as a 'voluntary industry best practice document' and

that ACMA is '… only tangentially involved as an observer, despite the focus on the AISI reports present in the Code'.[51]

7.44 Mr Keith Besgrove, First Assistant Secretary, Department of Broadband Communications and Digital Economy (DBCDE), reinforced the view that getting ISPs involved is essential. He suggested that developing a voluntary code is faster than regulation:

> We have always said that if this does not work then government will have to consider firmer options because this is really serious stuff. This is damn dangerous and we have got to do something about it.[52]

7.45 Mr Peter Coroneos, CEO, IIA, asserted that the new code will encourage ISPs to address what is a 'large and growing problem' of botnets operating across their networks.[53] A consultation draft was released on the day that IIA appeared before the Committee. The Committee was advised the code would be launched by 1 December 2009; take effect in 2010 and be reviewed in 2011.[54]

7.46 The e-security code of practice is intended to coexist with the existing *Spam Code of Practice*, and, related Commonwealth, State and Territory laws on crime, consumer protection, and privacy. The new code is proposed to be voluntary, which means that ISPs are free not to participate in AISI or any other form of bot detection. It also means that ACMA lacks power to give a direction to any section of the industry in respect of these matters.

7.47 The Committee was told the voluntary code is intended to promote greater consistency in the Internet industry by:

- encouraging ISPs to be involved in the AISI scheme or use other sources to detect infected machines;
- setting out options on what might be done to notify the subscriber and reduce Internet access; and
- providing ISPs with standardised information to promote consistent basic plain English e-security messages to their subscribers.[55]

---

51 ACMA, *Supplementary Submission 56.1*, p.3.

52 Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, 25 November, 2009, p.9.

53 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, pp.15-16.

54 IIA, *Submission 54*, p.8; Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, Wednesday 25 November, 2009, p.9.

55 IIA, *Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security*, (Consultation Version 1.0), September, 2009, p.9.

7.48 In effect, the intention is to codify existing practice and provide basic standardised information for use by ISPs with subscribers.[56] An ISP will have to take at least one of the listed actions to be considered code compliant. These include, for example, simply notifying the customer of the problem, a reduction in connection speed, placing the computer in a 'walled garden', temporary suspension, and, in extreme cases, disconnection of the service.[57]

7.49 The Committee noted that neither the ISPs nor IIA are expected to provide scanning software to detect malware or technical assistance to remove the bot (see discussion of remediation below). However, the ISPs can refer a subscriber to an IT security company via the IIA website.[58]

7.50 The IIA is creating an e-security branding scheme.[59] Code compliant ISPs are entitled to use the IIA Security Friendly ISP Trustmark. The brand icon (a small tortoise) will lead to a standardised information page, which in turn links to the IIA security portal.[60] The IIA security portal provides links to companies that specialise in anti-virus and e-security. The Committee was told this approach is intended to alleviate the workload for small ISPs.[61]

7.51 There was a range of views on the importance of ISP action. One witness said that, by definition, ISP action will always be reactive rather than pre-emptive, and ISPs have a limited role in protecting network integrity.[62] Another viewpoint was that ISPs could play a preventative role if they required their customers to adopt security measures before being connected to the Internet.[63]

7.52 There was also advocacy for a more integrated approach that would require an ISP to notify and refer their subscriber to a publicly funded centre for malware detection and removal. The aim would be to provide a

---

56 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.15; see also, Ben Grubb, ZDNet.com.au, *Privacy Commissioner delays zombie code*, 27 January 2010.

57 IIA, *Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security*, (Consultation Version 1.0), September, 2009, p.9.

58 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.17.

59 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.16.

60 <www.tortoise.iia.net.au>.

61 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.16.

62 Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.54.

63 Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, pp.60-61.

more effective response to end user needs.[64] The issue of remediation is discussed in more detail below.

Liability of ISPs

7.53 The Committee was informed that ISPs were concerned about potential liability for losses caused by restricting or denying access to the Internet. Telstra, for example, said that:

> Under current telecommunications regulations, Telstra is required to provide and protect its cyber infrastructure from attack, but if Telstra was to take action against a retail or wholesale customer who has been identified as the sources of a cyber attack, then that customer may initiate civil court action if Telstra disconnected that customer in order to protect its infrastructure and other customers.[65]

7.54 It was recommended that carriers and ISPs be provided with immunity from third party claims for actions taken in good faith or agreed with government or industry, to protect their networks and services and customers from being used in, or in relation to, the commission of criminal offences.[66] Another contributor suggested that, in the US, some companies are already denying service to end users with infected machines and liability may not be such a significant issue.[67]

7.55 The Committee was advised that s.313 of the *Telecommunications Act 1997* (Cth) places several obligations on ISPs. These obligations arise in connection with the ISP's operation of telecommunications networks and facilities, and their supply of 'carriage services'.[68] In summary, the obligations include:

- doing the carrier's 'best' to prevent telecommunications networks and facilities from being used to facilitate a criminal offence; and
- giving Commonwealth, State and Territory authorities 'such help as is reasonably necessary' to enforce the criminal law, protect the public revenue, and safeguard national security.[69]

64 AusCERT, *Submission 30*, pp.14-24.

65 Telstra, *Submission 43*, p.5.

66 Telstra, *Submission 43*, p.5.

67 Ms Alana Maurushat, CLPC, *Transcript of Evidence*, 8 October 2009, p.27.

68 DBCDE, *Supplementary Submission 34.1*, p.2.

69 Subsections 313 (1)(2)(3) of the *Telecommunications Act 1997* (Cth).

7.56 If an ISP does an act in 'good faith' as part of fulfilling one of the duties it will be immune from civil action for damages in relation to that action.[70] A similar immunity is extended to the officers, employees and agents of a carriage service provider.[71] The immunity also applies to circumstances where an ISP undertakes action in compliance with a direction by ACMA.[72]

7.57 The DBCDE suggested that:

> … it could be argued that the act of responding to reports on compromised computers (e.g. computers with trojans/malware) could be considered to be reasonable action undertaken by the ISP to prevent its telecommunication networks and facilities from being used to commit cyber crimes under Commonwealth laws.[73]

7.58 The implication was that ISPs have an existing positive duty to prevent a malware infected computer from operating across the Internet. If this is correct, the existing immunity from civil action for losses arising from slowed or denied Internet access would also apply.

7.59 The Committee also sought views from ACMA on this point. The ACMA referred the Committee to the *Spam Code of Practice*, which requires each ISP to have an 'acceptable use policy' in its contract with each customer. The contract must include a clause that allows for immediate account disconnection or suspension when an ISP becomes aware a customer's computer is used for sending spam emails.[74]

7.60 The ACMA stated that, in its view, in circumstances where the ISP exercises a contractual right, such as that required by clause 7.3 of the *Spam Code of Practice*, the ISP should 'generally be able to terminate or suspend the service without adverse legal consequences'.[75]

Committee View

7.61 The industry codification of existing practice is a useful tool to promote greater participation by the many hundreds of ISPs that are not yet part of the AISI. It also encourages ISPs to access other sources of network data to

---

70 Subparagraph 313(5)(a) of the *Telecommunications Act 1997* (Cth).

71 Subsection 313(6) of the *Telecommunications Act 1997* (Cth).

72 DBCDE, *Supplementary Submission 34.1*, p.2; subparagraph 313(5)(b) of the *Telecommunications Act 1997* (Cth).

73 DBCDE, *Supplementary Submission 34.1*, p.3.

74 Clause 7.3 of the IISCP; as cited, ACMA, *Supplementary Submission 56.1*, p.1.

75 ACMA, *Supplementary Submission 56.1*, p.1.

detect zombie computers. However, the Committee is concerned that in its present form the code is not a sufficient advance on the current state of play.

7.62 First, the consultation draft merely codifies the existing range of practices, leaving the widest possible discretion to the ISP. To be code compliant an ISP need only notify a subscriber of the compromised machine to be entitled to adopt the trust mark icon. As noted above, the Committee understands that many ISPs already have either an automated system of notification, provide email advice to the customer or, in some instances of smaller ISPs, have a policy of making contact by phone to explain the problem. However, because of the wide discretion in the existing code, there is no guarantee that a compromised machine will not simply continue to operate with full access and infect other Internet users. The Committee considers that, in this respect, the proposed code sets the bar too low.

7.63 In the Committee's view, the industry code should reflect the seriousness of the situation and the unique role of ISPs as commercial gatekeepers to the Internet. The continued operation of zombie computers exposes the owner to a higher risk of identity theft and fraud, with all its attendant financial and emotional costs. If left unchecked the zombie computer continues to support criminal activities and is a public nuisance to other Internet users. The inter-connected nature of the Internet infrastructure, which is often compared to a public highway, means there is a shared responsibility for protecting the security and safety of the wider community. The Committee believes there is a strong public interest in:

- a mandatory obligation to inform end users when their IP address has been identified as linked to a compromised machine(s);
- a clear policy on graduated access restrictions and, if necessary, disconnection until the machine is remediated; and
- basic advice and referral for technical assistance for remediation (see below).

7.64 Second, the Committee is also disappointed the industry has not yet taken a more comprehensive approach to the issue. While many ISPs do provide e-security products, the code itself does not, for example, promote the use of anti-virus software at the point of connection to the Internet or other security advice or software services. This is a missed opportunity that could provide some benefits to ISPs and make a real contribution to promoting a culture of e-security

7.65 The e-security code of practice should include additional matters, such as:

- that the ISP provides basic security advice when the account is set up to assist the end user to protect themselves from hacking and malware infections; and
- acceptable use policies that include a requirement that the subscriber agree to:
  - ⇒ install anti-virus software and firewalls before the Internet connection is activated;
  - ⇒ endeavour to keep e-security software protections up to date; and
  - ⇒ take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.

7.66 The inclusion of these terms would assist an ISP which is subject to a complaint before the Telecommunications Ombudsman. It also sends a clear message that end users also have a responsibility to protect themselves and other Internet users.

7.67 Third, the Committee is concerned that, although the industry and the regulator co-regulate in other areas of industry practice, this code is proposed to be voluntary. In 2003 the IIA released a draft *Cyber Crime Code of Practice,* which did not eventuate into a general cyber crime code of practice for the industry.[76] In 2004, the Parliamentary Joint Committee on the Australian Crime Commission expressed concern about the voluntary nature of that proposed code.[77] This Committee agrees with that view.

7.68 The registration of the e-security code of practice would be consistent with existing law and policy, and will ensure a greater consistency across the industry.[78] It would provide a more certain basis to the contractual relationship with subscribers and reduce uncertainty about liability. Registration would also enable ACMA to make an order if it was necessary to do so as a measure of last resort.

---

76 That draft code set out to establish guidelines for cooperation in criminal and civil investigations and to promote positive relations between industry and law enforcement. It was also intended to give users confidence their privacy and the confidentiality of their transactions will be protected from unlawful intrusion; Internet Industry Code of Practice, paragraph 1.11, as cited, Joint Parliamentary Committee on the Australian Crime Commission, *Cybercrime*, March 2004, p.17.

77 Joint Parliamentary Committee on the Australian Crime Commission, *Cybercrime*, March 2004, p.17.

78 See, for example, existing law regulating ISPs: *Telecommunications Act 1997* (Cth), *Telecommunications (Intercept and Access) Act 1979* (Cth); and, the *Spam Code of Practice.* In relation to prohibited classified content, the Internet industry *Content Services Code* was registered under the *Broadcasting Act 1992* (Cth) in 2008; to block access to foreign online gambling sites, the IIA *Interactive Gambling Industry Code* was registered by ACMA in 2001.

Recommendation 14

That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to immediately elaborate a detailed e-security code of practice to be registered under the *Telecommunications Act 1997* (Cth).

That the code of practice include:

- **an obligation that the Internet Service Provider provides basic security advice when an account is set up to assist the end user to protect themselves from hacking and malware infections;**
- **a mandatory obligation to inform end users when their IP address has been identified as linked to an infected machine(s);**
- **a clear policy on graduated access restrictions and, if necessary, disconnection until the infected machine is remediated;**
- **the provision of basic advice and referral for technical assistance for remediation; and**
- **a requirement that acceptable use policies include contractual obligations that require a subscriber to:**
  - ⇒ **install anti-virus software and firewalls before the Internet connection is activated;**
  - ⇒ **endeavour to keep e-security software protections up to date; and**
  - ⇒ **take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.**

7.69 Finally, the Committee considers that it may be the better policy view that s.313 of the *Telecommunications Act 1997* (Cth) already imposes a positive duty to take action in response to compromised machines. However, the matter is not entirely free from doubt, and, in the absence of judicially binding authority, there is merit in reviewing the legislative provisions. The Committee notes, for example, that most subscribers are innocent victims of malware and are not knowingly or intentionally distributing malware infections to other Internet users.

Recommendation 15

That the Australian Government, in consultation with the Internet industry, review the scope and adequacy of s.313 of the *Telecommunications Act 1997* (Cth) to promote Internet Service Provider action to combat the problem of malware infected machines operating across the Internet.

Remediation of Infected Machines

7.70 As noted above, it was put to the Committee that a model that integrates AISI, ISPs and IT specialists and IT security vendors is needed to ensure ready and cost effective access to technical assistance to deal with the problem of malware infected computers.[79]

7.71 The Committee has recommended that scanning software be a feature of a centralised cyber crime reporting centre (see Chapter 5). However, the Committee was made aware that scanning software is often unable to detect malware, which has the 'ability to hide, obfuscate and subvert anti-virus scanning programs'.[80] Mr Graham Ingram, AusCERT, explained that once the malware is on the computer, it usually requires professional expertise to remove it.[81] This involves taking the computer off line, and contracting an IT technician, which can be time consuming and expensive.[82]

7.72 The Internet Engineering Task Force draft *Recommendations for the Remediation of Bots in ISP Networks* also recognises that bot removal often requires '…specialised knowledge, skills and tools, and may be beyond the ability of average users and often beyond the capabilities of IT staff.'[83]

7.73 Similarly, IIA agreed that scanning software has limits:

> Online scanning websites offer some remote scanning possibilities for users, but scanning is limited to browser's security settings.

79 See, AusCERT, *Submission 30*, pp.14-24; AusCERT, *Exhibit 13*, *Internet Industry Code of Practice*, pp.1-16.

80 AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.13.

81 AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.13.

82 AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.13.

83 Internet Engineering Task Force, *Draft Recommendations for the Remediation of Bots in ISP Networks,* September 15, 2009; see also, AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.3.

> The prior installation of a 'root kit' may render such scanning ineffective. Online scans are not to our knowledge able to detect if a computer is part of a botnet, only whether it may have software installed that could render it susceptible to such. And even then, this is not infallible. The increasing sophistication and funding of the zombie threat seems to be reducing the effectiveness of such approaches.[84]

7.74 The Committee was advised of a number of overseas initiatives, including the publicly funded Japanese Cyber Clean Centre (CCC) and the recently announced German initiative (see below), that include remediation as part of a more coordinated model.

7.75 The Japanese CCC is a cooperative effort between government, ISPs and a number of IT security companies (e.g. Trend Micro, McAfee and Symantec). Symantec explained:

> Set up in 2006, the CCC initiative analyses bot characteristics, provides information on bot-infestation, promotes bot cleaning and prevention amongst Internet users in Japan. A cooperative effort between the Japan government with ISPs and security vendors, it functions along a five-step process whereby botmalware samples are collected; 'cleaners' (or anti-malware tools) are developed; infected users are identified and instructed to 'clean' their computers; 'cleaners' are downloaded by users; and the bot-malware samples are sent to participating security vendors for creation of malware signatures.[85]

7.76 The CCC conducts the malware analysis and IT specialist companies develop specific file signatures to clean the computers.[86] The CCC also allows for:

> … statistics and metrics to be developed which can then be used to track the success of the program over time and provide insights into how the malware problem is evolving and changing.[87]

7.77 IIA commented that the publication of rates of botnet infections and responses to inform policy and education campaigns is particularly useful.[88] Symantec agreed that one of the benefits is that:

---

84 IIA, *Supplementary Submission 54.1*, p.1.

85 Symantec, *Supplementary Submission 32.1*, p.6.

86 AusCERT, *Exhibit 13*, *Internet Industry Code of Practice,* p.12.

87 AusCERT, *Exhibit 13*, *Internet Industry Code of Practice,* p.11.

88 IIA, *Supplementary Submission 54.1*, p.4

> A clearer understanding of the nature of bot infections within the local environment also seems to have been developed. An initiative like the CCC could lead to better situational awareness of the local bot landscape, more proactive remediation of end-users' bot-infected computers and increased public awareness.[89]

7.78 Japan's CCC FY2008 report states that the project has 'accomplished "concrete results" and gained "wide acceptance", although the number of bot infections still remained large and further effort was needed to clean up infected computers'.[90]

7.79 The IIA stressed that the Japanese model could work provided there are adequate resources to fund its operations, research and promotion. The Japanese CCC, which is fully funded by the Japanese Government and managed by a Steering Committee chaired by two Ministers, is better funded as a public body than the current approach in Australia.[91]

7.80 It was proposed that Australia adopt a similar model to 'provide practical assistance and tools to help Australian Internet users recover from serious forms of malware attacks'.[92] The ACMA concurred that while it may not clear all infections this 'would be a very good initiative'.[93]

7.81 Mr Bruce Mathews, ACMA, concluded that:

> I think that would be a good movement. I am not sure that any software is going to ever be able to disinfect everything, but certainly software is very important in part of the overall approach to this problem. Of course, there are many economic competitors in what is a very large industry, the anti-malware industry, and they may also have views on such a centre in relation to their own activities.[94]

7.82 The German Government is also working with ISPs in a similar way to Japan. The Association of the German Internet Industry, with support

89 Symantec, *Supplementary Submission 32.1*, p.6.

90 Cited in Symantec, *Supplementary Submission 32.1*, p.6.

91 See <https://www.ccc.go.jp/en_ccc/index.html>; see also <http://blog.cytrap.eu/?p=287>; IIA *Supplementary Submission 54.1*, p.3.

92 AusCERT, *Exhibit 13*, *Internet Industry Code of Practice,* p.11

93 Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October 2009, p.14.

94 Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October 2009, p.14.

from Germany's Federal Office for Information Security, has announced a help service that includes a telephone hotline for customers.[95]

7.83 Once a customer's computer has been identified as malware infected, the ISP can send a message to their subscriber, guiding them to the Association's website that shows them how to remove the malware. The botnet cleanup hotline gives consumer access to anti-virus specialists who provide personal assistance if it is necessary.[96]

7.84 Some individual large ISPs have also taken their own initiatives. In the US, the ISP Comcast Corporation has announced a trial of an in-browser notification 'Service Notice', that alerts a subscriber whose computer appears to be infected. The notice requests that they go to an Anti-Virus Centre for instructions on removing the bot from their computer.[97]

Committee View

7.85 As stated above, the Committee is of the view that a more integrated model built on AISI, involving ISPs, IT security specialists, and end users in a more tightly coordinated scheme will yield better results in the detection and remediation of compromised machines. A more coordinated approach would also ensure a reliable source of data from which to tackle the botnet problem in Australia.

7.86 The Committee has addressed each element of this scheme in the sections above with recommendations to:

- expand ACMA's access to network data to detect malware infected machines;
- a mandatory e-security code of practice for the ISPs to address compromised machines operating across their networks; and
- new contractual obligations for end users to strengthen prevention and cure of infected machines.

7.87 The scheme would be incomplete without addressing the fourth element – the issue of remediation. There was a clear message to the Committee that

95 *AusCERT, Exhibit 23*, p.3; Eco-Association of the German Internet Industry, *Quick remedy for botnet infections*, 14 December 2009; John Leyden, *German ISPs teams up with gov agency to clean up malware*, The Register, 9 December 2009.

96 *AusCERT, Exhibit 23*, Eco-Association of the German Internet Industry, *Quick remedy for botnet infections*, 14 December 2009; John Leyden, *German ISPs teams up with gov agency to clean up malware*, The Register, 9 December 2009.

97 *AusCERT, Exhibit 23,* Comcast, *Comcast Unveils Comprehensive 'Constant Guard' Internet Security Program*, Press Release, 8 October 2009.

end users and small and medium sized businesses would benefit from direct and cost effective assistance to not only detect malware but also to remediate malware infected computers. The Committee considers that there needs to be a more direct pathway for end users to access malware detection software and bot removal services that are readily available, cost effective and provide a timely solution to the problem.

7.88 This will necessarily involve closer public and private partnerships, with one or more IT vendors and/or not for profit specialist service providers such as AusCERT. It could involve IIA in providing the technical helpline service, as is the case in Germany. Alternatively, a model that is closer to the Japanese approach may be more effective and, if designed correctly, appropriate to the needs of Australian end users. It may also be possible to integrate such a scheme with the national cyber crime reporting centre recommended in Chapter 5.

Recommendation 16

That a more integrated model for the detection and removal of malware, built on the Australian Internet Security Initiative, be implemented. The new scheme should involve the Australian Communications and Media Authority, Internet Service Providers, IT security specialists, and end users in a more tightly coordinated scheme to detect and clean malware infected computers.

Compromised websites

7.89 As noted in Chapter 2, the corruption of legitimate websites has taken over from spam as the main way malware is spread to innocent end users.[98] For example, Symantec told the Committee that:

> Most web based attacks are launched against users who visit legitimate website that have been compromised by attackers in order to serve malicious content. A popular, trusted site with a large number of visitors can yield thousands of compromises from a single attack, thus providing an optional beachhead for distributing malicious code.[99]

98 ACMA, *Submission 56*, p.15; Symantec, *Submission 32*, p.2.

99 Symantec, *Submission 32*, p.2.

7.90 Given the 'role of compromised websites as the primary vector for cyber crime' ACMA said that:

> Developing a comprehensive and timely response to this problem needs to be a key and urgent focus of all areas of internet governance and by key internet industry stakeholders.[100]

7.91 ACMA expressed its concern that website owners are not aware that this is 'one of the most significant e-security problems on the Internet':

> …there needs to be a much greater focus on maintaining the e-security on websites, particularly websites that have forms for entering data onto the website, because they are the most vulnerable to being infected.[101]

7.92 The education of 'website owners would help raise awareness of this problem and how to rectify the compromise'.[102]

7.93 The Committee asked ACMA to consider in more detail what proactive strategies Australia could take; and, what legal powers and technical and personnel resources are needed to implement a more strategic response to infected websites. In supplementary evidence, ACMA advised that a range of options exist for addressing the problem of infected websites.[103]

7.94 These include a web compromise reporting and detection system:

> Such a system could operate under a similar framework to that of the AISI, that is, the ACMA could obtain data on compromised web pages from various sources (including developing an internal capability), collate this data, and provide daily aggregated reports to ISPs identifying infected web pages residing on their networks. In addition to ISPs, domain owners and hosting companies could also be included.[104]

7.95 The reporting and detection system could be supported by a registered industry code outlining industry procedures for dealing with infected websites and notifications of infected websites could apply:

> As the ACMA has the power to enforce the provisions of registered codes, this could be pertinent in cases where there was a need to direct a service provider to remove malicious content. A

100 ACMA, *Submission 56*, p.15.

101 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.5.

102 ACMA, *Submission 56,* p.15.

103 ACMA, *Supplementary Submission 56.1*, p.5.

104 ACMA, *Supplementary Submission 56.1*, p. 5.

registered code would also serve the purpose of indemnifying ISPs who act on reports of infected websites.[105]

7.96 The Committee was told the problem of compromised websites was considered during the *E-Security Review*. AGD said the 'Cyber Security Policy and Coordination Committee agencies will further explore the legal issues of infected websites' and this 'work will guide any allocation of new resources and powers as required'.[106]

7.97 In the meantime, it has been reported that Microsoft recently joined forces with Symantec, The Shadowserver Foundation and International Secure Systems to obtain a US District Court order to compel Verisign, the .com domain registry, to sever 273 'malicious domain names'.[107] This civil action was part of Operation b49 to dismantle the Waledac botnet that, according to Microsoft, has the capacity to send 1.5 billion spam emails a day. The civil action highlights the integral role of Domain Name Registrars in a more strategic approach to tackling the problem of botnets.

Committee View

7.98 The Committee is concerned that the targeted infection of legitimate and trusted websites is now the number one vehicle for distributing malware, and poses a significant threat to the integrity of the Internet. The evidence indicated that it is practically impossible for any ordinary consumer to detect when a website has been infected, leaving them exposed to malware infection, identity theft and fraud. This is an area in which consumer education is less useful. However, an education program geared toward small and medium sized businesses would be useful, especially for businesses that transact with clients online and, in that process, take personal and financial information. Education initiatives are discussed in Chapter 10.

7.99 It is also a matter of concern that the regulator, ACMA, lacks technical capacity to detect infected websites or powers to order the remediation or the take down of an infected website. The Committee sees considerable merit in building on the success of the AISI to tackle the problem of infected websites supporting malicious code. The problem was identified

105 ACMA, *Supplementary Submission 56.1*, p.5.

106 AGD, *Supplementary Submission 44.2*, p.4.

107 Nick Wingfield, *Microsoft wins 'botnet' order,* The Wall Street Journal Asia, 26 February 2010, p.6; William Jackson, *Microsoft unplugs spammer botnet with legal strategy*, Government Computer News, 1 March 2010 http://gcn.com/Articles/2010/03/010, viewed 3 March 2010.

by the *E Security Review*, but the process and timeframe for developing a legal and a technical response is unclear.

7.100 The Committee is also aware there are a range of complex issues to be worked through and some potential overlap with the problem of fraudulent sites established to launch phishing attacks. This raises a range of related issues about the responsibilities of domain name registries, registrars and resellers to verify the identity of applicants, cooperate with law enforcement authorities, and provide procedures for rapid takedown of illegitimate infected sites or those spreading spam or that are part of a botnet. The Domain Name System and the role of registries, registrars and resellers are discussed in more detail below.

Recommendation 17

That the Australian Communications and Media Authority be funded to develop a system that can obtain data on compromised web pages from various sources (including developing an internal capability). This data be collated and provided as daily aggregated reports to Internet Service Providers identifying infected web pages residing on their networks.

That in addition to Internet Service Providers, domain owners and hosting companies also be included in the new scheme.

Recommendation 18

That the system for reporting and detecting compromised web pages proposed in recommendation 17 be supported by a registered industry code that outlines industry procedures for dealing with infected websites.

That the Australian Communications and Media Authority be empowered to enforce the provisions of the registered code, including, for example, where there is a need to direct a service provider to remove malicious content.

That Internet Service Providers and hosting companies who act on reports of infected websites be indemnified against claims for losses.

Reporting Spam Email

7.101 *SpamMatters* is a software program developed by ACMA that gives end users an easy automated way of reporting of spam email directly to ACMA. There are 290,000 registered users and 41 million reports of spam since the program was launched on 30 May 2006. The total number of Internet connected residences and businesses in Australia has been estimated by the Australian Bureau of Statistics (ABS) in 2008 to be at eight million.[108] Against this background, while the number of registered *SpamMatters* users is significant, it remains a small proportion of the total number of end users in Australia.

7.102 The software can be downloaded from the ACMA website. It installs a plug-in to Microsoft Outlook or Outlook Express. Once installed a button appears in the subscriber's email system that allows the user to select the spam email and click the button to send the spam directly to ACMA 'in a forensically intact manner'.[109] This means the headers are intact, which is important for investigative purposes.

7.103 There is a form of *SpamMatters* that appears as a button in the Telstra webmail client. ACMA advised that a very large number of the 290,000 registered for *SpamMatters* are Telstra webmail subscribers:

> This is a great initiative. We get lots of very good data from that button, and we have been encouraging other ISPs as well to move in that direction and install a similar button. We hope to be successful in encouraging more ISPs to participate over time.[110]

7.104 ACMA wants to encourage more ISPs to install a spam button in their webmail systems, because this is easier to maintain than updating the *SpamMatters* software with each successive release of Microsoft operating and email systems.[111]

7.105 The spam reported via *SpamMatters* is the spam email that has got through ISP filters and any spam filtering software, so it is not representative of general spam on the Internet.[112] It is used to identify 'campaigns of spamming activity' such as phishing email campaigns, which are reported regularly to the AFP.[113] In the US, the US CERT located in the Department

108 Australian Bureau of Statistics, *Internet Activity*, Australia, Cat. No. 8153.0, December 2008.
109 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.
110 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.
111 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.
112 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.
113 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.

of Homeland Security is the central location for the online reporting of phishing emails.[114]

7.106 The Committee was told that ACMA is also working on the next generation of *SpamMatters,* which will include an 'interrogation system' to 'improve the analysis of the data'.[115] This will enable ACMA to 'identify trends within that data and also use it to extract information on what we consider to be infected IP addresses, which will feed back' into the AISI in a more 'sophisticated manner than is currently done through the *SpamMatters* software'.[116]

7.107 There was also evidence that spamming is occurring via social networking sites as commercial operators seek to find new ways of messaging potential consumers.[117] The *Spam Act 2003* (Cth) applies to emails, and there is a question mark about its application in the context of social networking media and in a range of other instant electronic messaging systems. This issue is discussed in Chapter 6.

Committee View

7.108 The Committee commends ACMA on developing an automated reporting system that gathers useful intelligence and can be used to feed into law enforcement efforts. In particular, it looks forward to a future briefing on the development of *SpamMatters* that links this intelligence to AISI data.

7.109 However, the Committee is disappointed this innovation has not been widely taken up by ISPs, which would, in the Committee's view, provide the most effective way of increasing the reach of *SpamMatters*. The wider adoption of the *SpamMatters* button by ISPs would substantially increase the level of spam reported to ACMA.

7.110 The Committee understands it is a requirement of the *Spam Code of Practice* that ISPs give their customers spam filter options, and advise customers how to report spam, as well as accepting spam reports from their own customers.[118]

7.111 In 2006, the then Department of Communications, Information Technology and the Arts (DCITA) reviewed the *Spam Act 2003* and recommended that no change be made to the role of ISPs under the

114 <http://www.us-cert.gov/nav/report_phishing.html>, viewed 1 March 2009.

115 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.9.

116 Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.9.

117 Australian Computer Society, *Transcript of Evidence,* 9 October 2010, pp.34-35.

118 Clauses 6, 10.1 and 10.4, *Spam Code of Practice.*

Telecommunications Act 1997 (Cth) or the *Spam Code of Practice*.[119] However, there was limited opportunity to evaluate the effectiveness of the *Spam Code of Practice*, which only came into force on 16 July 2006.[120]

7.112 Since then spam has developed as a vector for the distribution of malware and the proliferation of scams and phishing attacks. It would be timely for ACMA and the IIA to review the *Spam Code of Practice*. In particular, the reporting of spam via *SpamMatters* through the ISPs email services should be considered for inclusion in any revised code. That review should include consumer representatives such as the Australian Communications Consumer Action Network and the Australian Competition and Consumer Commission as well as the Internet industry.

Recommendation 19

That the Australian Communications and Media Authority and the Internet Industry Association review the *Spam Code of Practice* to assess the effectiveness of current industry standards for the reporting of spam.

That serious consideration be given to obliging Internet Service Providers to include the Australian Communications and Media Authority's *SpamMatters* program as part of their email service to subscribers.

Domain Name System

7.113 The Domain Name System (DNS) is a hierarchy for the naming of computers and other devices connected to the Internet. The authority to allocate and sell the licence to use a domain name is distributed via a system of registries, registrars and resellers.[121]

119 DCITA, Report on the *Spam Act 2003* Review, June 2006, p.77.

120 DCITA, Report on the *Spam Act 2003* Review, June 2006, p.104.

121 Domain name servers (DNS) convert web addresses into Internet Protocol addresses and routes the computer user to the correct location. Thirteen root DNS servers cover the entire Internet along with a number of local servers. Once reconfigured, the DNS can send users to any number of websites and seriously compromise the entire Internet system. In the case of Domain Name Server poisoning, the list of addresses in a DNS server are altered so that a legitimate URL address points to an illegitimate Internet Protocol address, the fraudulent web

7.114 The Internet Corporation for Assigned Names and Number (ICANN) explained that:

> … every domain name around the world ends with a top-level domain (TLD); these are the 2 or more letters that come after the dot. There are currently two types of TLDs: generic top-level domain (gTLDs) such as .com, .mobi, and .info, and country code top-level domains (ccTLDs) such as .uk, .br, and .cn. A gTLD or a ccTLD is managed by a registry operator, an organization that maintains the registry database, including the nameserver information for names registered in the TLD.[122]

7.115 The ease of access to domain names, the hijacking of domains, and hijacking of the DNS raise e-security issues in both the technical and management aspects of DNS.

7.116 Some witnesses argued that the regulation of Domain Name Registrars and Resellers should be reviewed and, in particular, a 'know your customer' regime instigated.[123] For example, the Australian Computer Society expressed the view that ICANN should raise the performance of registrars and require more vigilance over the way domain names are allocated.[124] While ABACUS - Australian Mutuals recommended legislation to prevent criminals obtaining domain names to engage in phishing:

> Abacus urges the committee to examine in detail the regulation of domains and to consider stronger regulation of domain registration and the internet generally. The ease of establishment and hijacking of sites for criminal purposes has affected mutual ADIs since 2003 and the threat is growing. In 2009 two mutual ADIs experienced sustained cyber attacks that affected service delivery to members.[125]

7.117 AusCERT also stressed the important role of DNS registration and said that:

> "Self-regulation" exists among ISPs and Domain Name Registrars but can be problematic as potential conflicts of interest arise

---

site (Brody, R.G., Mulig, G., and Kimball, V. 2007, '*Phishing, pharming and identity theft*', Academy of Accounting and Financial Studies Journal) as cited AFP, *Submission 25,* p.4.

122 <http://www.icann.org/en/topics/new-gtlds/strategy-faq.htm>, viewed 1 March 2010.

123 See, for example, AusCERT, *Submission 30*, p.15; Abacus – Australian Mutuals, *Submission 55*, p.4; Australian Computer Society, *Transcript of Evidence*, 9 October 2009, p.39.

124 Australian Computer Society, *Transcript of Evidence*, 9 October 2009, p.39.

125 Abacus – Australian Mutuals, *Submission 55*, p.4.

> between taking action that is in the interests of the external community to what may be perceived to be detrimental to their own commercial interests. For example, Domain Name Registrars could be more discerning and adhere to more stringent processes before registering domains designed to support criminal activity. The deregistration of domains used for fraudulent activity could also be substantially improved.[126]

7.118 The Committee was advised that the Anti-Phishing Working Group[127] (APWG) has developed *Anti-Phishing Best Practices Recommendations for Domain Name Registrars.* AusCERT argued that if registrars around the world adopted the APWG best practice guide, this would help prevent some types of cyber crime.[128] The APWG recommendations address three core issues:

- evidence preservation for investigative purposes;
- proactive fraud screening; and
- phishing domain takedown.[129]

Generic Top Level Domain

7.119 The ICANN is the international not for profit, multi-stakeholder body which is responsible for coordinating the DNS. Mr Paul Twomey, Senior President, ICANN explained that ICANN is not 'the governor of the internet' but coordinates the domain name system and, among other things, allocates the protocols for the IP addressing system.[130]

7.120 ICANN sets the policy for all generic top level domains such as .com, .net, .org, and .info but does not set policy for the country code top level domains. In practice, this means that ICANN sets the rules for registries and accredits registrars for the gTLDs. For example, VeriSign Inc. is the domain name registry for .com and .net under a binding agreement with ICANN.

7.121 ICANN has no authority to accredit the registrars that operate in the country code Top Level Domains (ccTLDs), such as '.au', '.nz' and '.uk' as each country has different systems in place regulating their country code top level domain. The regulation of country code level domains is a matter

126 AusCERT, *Submission 30*, p.15.

127 The APWG is an international industry association focused on eliminating phishing.

128 AusCERT, *Submission 30*, p.15.

129 APWG, *Best Practices Recommendations for Registrars*, October 2008, p.1.

130 Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.1.

for each country. In the Australian context, the registry is called AusRegistry and is administered by .auDA.[131]

7.122 Mr Paul Twomey, ICANN, explained that security was not part of the design of the Internet, which originated as a research network in the university sector. ICANN has:

> … increasingly observed the use of the DNS as an aspect of how botnets operate within the Internet ecosystem – as a means of pointing attacks at targets; as a mechanism for malware to receive commands and updates; and the DNS itself as a target of such attacks.[132]

7.123 ICANN said it was faced with 'retrofitting security back inside the protocols' through the installation of a 'domain name system security extension protocol' (known as the Root Server DNSSEC):

> DNSSEC is basically a way of digitally signing a domain name so that, if you were to go to a particular site and the site showed that it had been signed, you would have confidence that was authoritative material and had been put in by the owners of the site. It does not fix all of the security issues but it certainly diminishes the risk of spoofing.[133]

7.124 The DNSSEC is discussed in Chapter 11. During evidence, ICANN said that the DNSSEC may not prevent the misuse of domain names but it will assist 'police, the banks and other technical people who work in this area' to identify 'domain names literally within minutes when they're being used for … attacks.'[134] Mr Twomey also said that, as part of the planned expansion of the gTLDs, ICANN will require all new top-level domain applicants to implement DNSSEC.[135]

7.125 ICANN maintains legally binding contracts with the gTLD registrars, which outline a number of obligations. For example, the registrar Accreditation Agreement (RAA) provides that registrars must submit to ICANN data such as the name and addresses of registrants and the IP

---

131 In fact, there are five country codes associated with Australia - .au for Australia, .cc for Cocos Islands, .cx for Christmas island, .hm for Heard and MacDonald Island and .nf for Norfolk Island.

132 ICANN, *Submission 40*, p.1.

133 Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.2; the domain name system security extension protocol is discussed in Chapter 11 of this report.

134 ICANN, *Supplementary Submission 40.1*, p.1.

135 Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.2

addresses of the primary and secondary name servers used by the registered name. The DBCDE said, however, that:

> At present there is no requirement on ICANN accredited registrars to verify the identity of registrants, although in many cases the use of an alias would be a breach of the terms and conditions of registration.[136]

7.126 Elsewhere it has been noted that gTLDs are:

> … subject to fewer exclusions based on where the registrant resides or does business. For example, most gTLD's do not require the registrant to indicate residency, in or a business connection with, a particular country.[137]

7.127 Ms Holly Raiche, Executive Director, Australian Internet Society also explained that identity verification standards vary across the industry:

> If you want to be a .com.au, you have to [provide] an ABN which proves that you are not only an individual but that you are also a company. To get a .com you just have to produce a credit card number and name.[138]

7.128 The evidence also indicated that simple measures such as requiring the three digit security code that appears at the back of a credit card are not mandated but would eliminate a lot of 'card not present' fraud on the DNS.[139]

7.129 In relation to, for example, domain name hijacking, ICANN's own Security and Stability Advisory Committee (SSAC) identified weaknesses in the registration and administration processes as far back as 2005.[140] The SSAC found that:

> … domain name hijacking incidents are commonly the result of flaws in registration and related processes, failure to comply with

---

136 Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.1-12; DBCDE, *Submission 34.1*, p.1.

137 Mr Neil Brown QC, *The New Internet – The Expansion of Top Level Domains – An Update*, Domain Times, <http://www.domaintimes.info/>, viewed 1 March 2010.

138 Ms Holly Raiche, Executive Director, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

139 Ms Holly Raiche, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

140 As noted in Chapter 2, 'domain hijacking' is where a cyber criminal takes control of a domain name by stealing the identity of a domain name owner, then uses this domain name to host a malicious website. 'Typo-squatting' is also sometimes known as website hijacking. This where a person registers domain names with a common typographical error in an established domain name to divert traffic to an illegitimate site.

> the transfer policy, and poor administration of domain names by registrars, resellers, *and*, registrants.[141]

7.130 A widespread lack of security measures has been identified as one of the risks that will accompany the introduction of hundreds, and, possibly, thousands of new websites when ICANN increases the number of gTLDs to accommodate the demand for domain names.[142] In response to e-security concerns, ICANN said that contracts with new gTLDs will require new measures including:

- an anti-abuse policy that details procedures for addressing reports of malicious conduct occurring via registered domain names including how rapid takedown/suspension of those names would occur;
- a publicly identified designated anti-abuse point of contact responsible for taking action in support of these policies; and
- "thick WHOIS" data available at the registrar level which will facilitate action by specifying domain names and identifying individuals involved in potential malicious conduct.[143]

7.131 The Committee was assured that ICANN's proposed measures will be mandatory, and are intended to address a range of malpractice and malfeasance problems. ICANN has also proposed 'voluntary verification programs' for 'high security zones' that will establish criteria for how:

> …registries and registrars will establish stronger controls over who gets to register domain names in those TLDs, as well as operational IT security controls to improve trust that registered names will not support malicious code.[144]

7.132 The policy for the new agreements and some of these technical measures are currently under debate in the DNS community.

7.133 Finally, ICANN informed the Committee that it continues policy development on the basic Registrar Accreditation Agreement (RAA) between itself and existing registrars.[145] Ms Holly Raiche, Australian

---

141 ICANN, Security and Stability Advisory Committee, *Domain Name Hijacking: Incident, Threats, Risks and Remedial Actions*, July 2005, p.5.

142 ICANN, New gTLD Program Explanatory Memorandum, *Process for Amendments to New gTLD Registry Agreements*, 15 February 2010; ICANN, New gTLD Explanatory Memorandum, *Mitigating Malicious Conduct*, 3 October 2009.

143 More detail is available at <http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>; ICANN, *Supplementary Submission 40.1*, p.1.

144 Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.9-10.

145 ICANN, *Supplementary Submission 40.1*, p.3.

Internet Society, also said there is progress toward better protection for registrants:

> In terms of what registrars do, there is now cooperation between the 'At-Large' community and the generic names organisation to develop a registrants charter of rights, which is going to focus on what registrars should do to look after registrants.[146]

Country Code Top Level Domain Name

7.134 In Australia, the .au Domain Administration (.auDA) is a private company responsible for the accreditation of registrars, and regulates numerous registrars and resellers of website names in the .au space.[147] The Committee invited .auDA to make a submission to the Inquiry but none was forthcoming.

7.135 Currently there are approximately thirty companies accredited by .auDA as registrars selling second level domain names under the .au TLD (.com.au, .edu.au etc). In 2003, .auDA estimated there were approximately 725 registrar appointed resellers and other companies selling .au domain names without a formal agreement with an accredited registrar.[148] DBCDE explained that neither:

> .auDA nor ICANN have direct contractual relationships with resellers. However, in both the gTLDs and .au resellers operate under an agreement with their registrar, which must include minimum terms and conditions.[149]

7.136 The *.au Domain Name Suppliers Code of Practice* explicitly applies to all registrars and their 'appointed resellers' and forms part of the *Registrar's Agreement*.[150] The *Registrar's Agreement* requires that any subsequent 'contract, arrangement or understanding' between a registrar and reseller for a Reseller's Licence must require the reseller to comply with .auDA's published policies.[151] The Australian system was said to be more advanced

146 Ms Holly Raiche, Executive Director, Internet Society of Australia, *Transcript of Evidence,* 9 October 2009, p.1; see also, ICANN, *Supplementary Submission 40.1*, p.3.

147 For example, the gov.au Domain Name Registrar function is delegated to the Australian Government Information Management Office.

148 .auDA, *Proposed Changes to the Regulation of Registrar-Appointed Resellers*, October 2003, pp.1-3.

149 DBCDE, *Supplementary Submission 34.1*, p.1.

150 See, clause 3 of the *.au Domain Name Supplies Code of Practice,* 2004-04, 14 October 2004.

151 Clause 15.4 of the .auDA *Registrar Agreement* (Approved Version 3-1 June 2008).

than in many countries and the *Domain Name Supplies Code of Practice*, which applies in Australia, does not apply internationally.[152]

7.137 The Committee was told that under subclause 9.1.2 of .auDA's non-negotiable *Registrar Agreement*, registrars must 'use reasonable endeavours' to verify the information provided in domain name applications. Equally, under .auDA's published policies registrants must 'warrant that the information that they provide is true, accurate and complete'. [153]

7.138 The DBCDE said that '… .auDA has advised that a "warranty"provided by the Registrant is considered sufficient' and there are a range of mechanisms used in the industry, 'some for instance ask for ACN or ABN numbers'.[154] However, DBCDE said that even where a business or company name is produced it is not known whether this information is checked against the Federal and State databases.[155]

7.139 The DBCDE agreed that identity verification in the .au name space is an important issue and .auDA has undertaken to consider how identity verification procedures could be improved.[156]

7.140 There is no statute law that deals specifically with domain name registration although the *Trade Marks Act 1995* (Cth) will affect the choice of name. The Committee asked what enforceable legal obligations exist to require an Australian Domain Name Registrar to remove a domain name that is associated with phishing or some other forms of illegal activity. DBCDE advised that:

> General domestic Australian laws, such as the *Crimes Act 1900*, the *Criminal Code 1995*, and the *Trade Practices Act 1974*, may apply to the conduct of registrars, depending on the specific jurisdictional circumstances. Provisions relating to theft, unauthorised access and misleading and deceptive conduct may apply to registrars that are complicit in a breach of these laws.[157]

7.141 The importance of Domain Name Registrars cooperating to refrain from registering or to disable websites involved in fraud or misleading and

---

152 Ms Holly Raiche, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.39.

153 DBCDE, *Supplementary Submission 34.1*, p.1.

154 DBCDE, *Supplementary Submission 34.1*, p.1.

155 DBCDE, *Supplementary Submission 34.1*, p.1.

156 DBCDE, *Supplementary Submission 34.1*, p.1.

157 DBCDE, *Supplementary Submission 34.1*, p.1.

deceptive conduct was highlighted by the Australian Competition and Consumer Commission (ACCC).[158] The ACCC told the Committee that in:

> Late 2008, the activities of the Designer Brand Outlet website were brought to the ACCC's attention by the US Federal Trade Commission, after reviewing complaints made by a number of overseas consumers to the eConsumer.gov website.[159]

7.142 The Committee was told that the 'Domain Name Registrar disabled the website and the bank where the website's merchant facility was held, suspended the service after conducting its own inquiries'.[160] In another example, a website that purported to be the official booking site for the Sydney Opera House was hosted and administered in the USA by US Domain Name Registrar NameSecure Inc. In that case, the offending material was removed but there was no order to take down the entire site, which was part of other legitimate business activity.[161]

7.143 Cooperation to deregister domain names that host malware is also important for dealing with the problem of botnets. As mentioned previously, recent civil action by Microsoft and Symantec resulted in an order compelling Verisign to sever over 200 domain names in the US as part of a strategy to dismantle the Waledac botnet.

Committee View

7.144 The Committee agrees with the principle expressed by the APWG that organisations that are part of the infrastructure of the Internet—ISPs, registries, registrars and resellers—have an obligation to take reasonable steps to protect the stability and security of the Internet.

7.145 There are a range of potential risks that Domain Name Registrars and Resellers should guard against in the sale, renewal and transfer of domain names. Preventing fraudulent acquisition of a domain name to conduct phishing attacks requires stringent identity verification. Preventing the reservation and sale of domain names for websites intended to be used for

158 ACCC, *Submission 46*, p.7.

159 ACCC, *Submission 46*, p.7.

160 ACCC, *Submission 46*, p.7.

161 *ACCC v Chen* [2003] FCA 897 at 25; ACCC, *Submission 46*, p.7; Justice Sackville granted declaratory relief and an injunction under the *Trade Practices Act 1952* (Cth) to mark its disapproval. The injunction in this case was granted to facilitate cooperation with the US Federal Trade Commission to take measures under US law to prevent Mr Chen from publishing misleading or deceptive material relating to the Sydney Opera House.

scams also requires more stringent regard for the rights of others.[162] In these instances the domain name is part of the misleading and deceptive conduct enabling fraud.

7.146 The Committee notes that the existing gTLD system is relatively small, with only 21 gTLDs, but the proposed expansion of the gTLD will lead to hundreds and eventually thousands of new registries worldwide. Internationalised Domain Names will appear in global languages including Chinese, Russian, Thai and so forth. The Committee urges ICANN and the Internet community to adopt robust measures to ensure the DNS registration system is not used to undermine the legal protection of consumers and businesses from phishing attacks and fraud.

7.147 In the current gTLD policy development process, ICANN should ensure that the APWG *Anti-Phishing Best Practices Recommendations* are incorporated and implemented in the gTLD Agreements. It is vital that these issues are addressed and clear policy on e-security measures are settled and adopted *before* ICANN massively expands the gTLD system.

7.148 The Committee supports proposals for new measures such as the vetting of registry operators and the deployment of DNSSEC technology. The Committee believes these agreements should also include:

- measures to prevent the registration of fraudulent sites;
- requirements for rapid take down of fraudulent domain names;
- requirements for the take down of domain names that host malware; and
- cooperation with law enforcement, consumer protection agencies and national regulators, such as ACCC, Australian Securities and Investment Commission (ASIC) and ACMA.

7.149 At the country code level, the Committee recognises that .auDA policies may be more advanced than in some other counties. For example, .auDA requires an applicant to have a registered trade mark, company or registered business. However, the Committee is still concerned that the existing *Registrar Agreements* and the *Domain Name Suppliers Code of Practice* does not impose more stringent requirements for:

- identity verification;

---

162 The standard definition of 'phishing' is fraudulent activity to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

- cooperation with law enforcement authorities;
- clear procedures for the deregistration of fraudulent sites; or
- deregistration of compromised sites persistently identified as part of a botnet.

7.150 As the APWGP has pointed out, better fraud protection at the registration end of the process will contribute to combating phishing, improve the protection of customers and reduce operating costs. Without better front end processes there is likely to be a growing number of reports of abuse and requests to take down sites identified as phishing sites.[163]

7.151 The same principle also applies in the wider context of scams and trade mark infringements that are increasingly committed over the Internet. In the Committee's view, there should be clear rules that prevent the reservation, sale and registration of domain names that are intentionally similar to established companies and other websites.[164]

7.152 The problem of websites that intentionally host malware or are unknowingly infected also needs to be addressed in an industry code of conduct. Such sites must be remediated or, if necessary, severed from the Internet as part of a strategy to tackle botnets.

7.153 In Australia, as elsewhere, the domain name registration system is a self regulated industry involving numerous registrars and many hundreds of resellers. The DNS is a critical element of the digital economy that intersects with established common law and statutory regimes in trademarks, trade practices, privacy, consumer protection, crime prevention and law enforcement. There is no statute law that deals specifically with domain name registration or regulates the rights and obligation of Domain Name Registrars, resellers and registrants.

---

163 The APWG best practice guide applies only to domain names registered solely for a fraudulent or criminal purpose. The procedures recommended do not apply to websites of a legitimate domain that is compromised and used by criminals to attack or compromise other computers; APWG, *Best Practices Recommendations for Registrars*, October 2008, p.3.

164 *British Telecommunications plc v One in a Million Ltd* [1998] 4 All ER 476, [1999] 1 WLR 903, [1999] FSR 1, [1998] NLJR 1179, [1998] All ER (D) 362 (Held: the court has jurisdiction in a passing off action to injunct the registration of a domain name calculated to infringe the rights of others. The registration was regarded as having equipped another with an instrument of fraud. A threat to infringe the trade mark of another was established because the defendant (registrant) sought to sell domain names which were confusingly similar to registered trademarks); see also *.auDomain Administration Ltd v Network.com.au Pty Ltd* [2004] ATMO 36 (29 June 2004) where the registration of www.network.com.au as a trade mark was opposed on the grounds that the company was not the licence holder of the domain name.

7.154 The Committee did not take detailed evidence on all aspects of the regulation, standards and practices in the domain name registration system generally. The Committee believes that a wider parliamentary inquiry into the operation of this relatively new sector is justified to examine industry practices. That inquiry should include an examination of the:

- nature, scope and interaction of rights and obligations of registrars, resellers and registrants in relation to each other and other rights holders; and
- the powers of law enforcement authorities, and regulators such as the ASIC, ACCC, ACMA and IP Australia.

Recommendation 20

That the Australian domain name registration industry be subject to a code of conduct that is consistent with the Anti-Phishing Working Group *Best Practices Recommendations for Registrars*.

The code of conduct should:

- **enumerate the type of information that should be collected during the domain name registration process by the registrar, that would help to preserve evidence and assist law enforcement authorities;**
- **identify processes that should be put in place to identify fraudulent activity before the domain name registration takes effect; and**
- **provide clear procedures for responding to requests for rapid take down of fraudulent sites and sites that host malware.**

Recommendation 21

That the Minister for Broadband, Communications and the Digital Economy make a reference to the House of Representatives Standing Committee on Communications to inquire into the regulation, standards and practices of the domain name registration industry in Australia.

8

Consumer Protection

Introduction

8.1 This chapter canvasses aspects of the consumer protection regime that relate to cyber crime. The Federal, State and Territory consumer protection bodies are increasingly dealing with the violation of consumer protection laws perpetrated over the Internet. The first section focuses on the Australian Competition and Consumer Commission's role in the enforcement of the *Trade Practices Act 1974* (Cth). In particular, the challenge of international enforcement of domestic consumer protection laws.

8.2 The discussion in the remaining sections move beyond the status quo and discuss strategic consumer protection interventions that have the potential to better protect ordinary end users from cyber crime:

- a requirement for informed consent and penalties for unauthorised installation of software;
- IT vendor information standards to promote e-security;
- the problem of insecure IT products; and
- industry standards to promote higher level security settings to better protect consumers.

Australian Competition and Consumer Commission

8.3 The Australian Competition and Consumer Commission (ACCC) administers the *Trade Practices Act 1974* (Cth) and has a responsibility to

protect consumers from economic harm: 'This includes conduct that is fraudulent and has the purpose of misleading consumers for financial gain'.[1]

8.4 The ACCC received 77,000 complaints in the 2008-2009 financial year. Of these, 18,000 related to scams of all types. Scams perpetrated over the Internet accounted for 12,000 of these complaints.[2]

8.5 The Committee noted that many complainants reported fraudulent conduct that also involved the proliferation of malware, such as via phishing emails.[3] As has been noted throughout this report, the combination of cyber crime techniques involving crimes and civil wrongs is often difficult to disentangle and requires strategic policy and enforcement intervention.

8.6 Finally, in line with the Government's overall strategy, the ACCC emphasise the importance of consumer education (see Chapter 10). The ACCC also hosts the *SCAMwatch* website, which provides public information, alerts and access to complaints mechanisms on a wide range of consumer scams, including scams perpetrated online (see Chapter 5).

International and Domestic Cooperation

8.7 The ACCC identified cross agency information sharing and cooperation and, where appropriate, enforcement action, as key elements of their approach.[4] Where online scams impact on consumers in multiple jurisdictions, domestic and international cooperation was described as crucial.[5]

8.8 To this end, the ACCC chairs the Australasian Consumer Fraud Taskforce (ACFT), which includes 20 Commonwealth and State agencies, departments and research institutes as well as the New Zealand Ministry of Consumer Affairs and the NZ Commerce Commission.[6] The Committee was told that the ACFT provides a mechanism for sharing information on enforcement activities as well as educative and information campaigns, and is also involved in research on consumer fraud.[7]

---

1 ACCC, *Submission 46*, p.2.
2 ACCC, *Submission 46*, p.3.
3 ACCC, *Submission 46*, p.3.
4 ACCC, *Submission 46*, p.2.
5 ACCC, *Submission 46*, p.6.
6 ACCC, *Supplementary Submission 46.1*, p.7.
7 ACCC, *Submission 46*, p.5.

8.9 In 2009 the ACCC worked with a number of other agencies:

> Domestically, the ACCC has worked with the Australian Federal Police, Australian Communications and Media Authority, Australian Securities and Investments Commission, Queensland Police, Australian Taxation Office and the state and territory offices of fair trading. Internationally, the ACCC has worked with the United States Federal Trade Commission and the Washington State Attorney-General's office.[8]

8.10 The Committee was told that the ACCC will often refer alleged scam matters to other agencies or organisations. This may occur at the first point of contact or be more formal or take place in one of the less formal forums for discussion and information sharing.[9] However, while the ACCC 'records the handling of each complaint' there were no statistics that differentiate the different types of referrals. Consequently, the Committee was unable to ascertain the number of matters referred for criminal prosecution by Australian authorities.[10] It was noted in Chapter 5, that the NSW Police believed that while a lot of resources are devoted to online scams, there are few criminal prosecutions (as opposed to civil enforcement action).[11] A more centralised approach to complaint handling across a wider range of cyber crime types is discussed in Chapter 5.

8.11 Broader international liaison is facilitated through the International Consumer Protection and Enforcement Network (ICPEN), a network of over 30 national fair trade agencies mainly from OECD countries. The ACCC took over the Presidency of ICPEN in August 2009 for 12 months.[12] The objectives of ICPEN include sharing best practices in legislative and other measures for effective consumer protection enforcement; taking action to combat cross border breaches of consumer protection laws; and facilitating effective cross border remedies.[13]

8.12 The ACCC also has a bilateral agreement with the US Federal Trade Commission on Mutual Enforcement Assistance in Consumer Protection Matters. This MOU provides a detailed elaboration of the obligations of

---

8 ACCC, *Supplementary Submission 46.1*, p.1.

9 ACCC, *Supplementary Submission* 46.1, p.1.

10 ACCC, *Supplementary Submission 46.1*, p.1.

11 Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

12 ACCC, *Submission 46*, p.6.

13 See Article 4 (a) to (f) of Memorandum on the Establishment and Operation of the International Consumer Protection and Enforcement Network, agreed to at the Conference in Jeju, Republic of Korea, 26-28 March 2006.

both parties to cooperate to ensure effective enforcement of consumer protection laws in both countries.[14] On the question of Australia – US cooperation, the ACCC advised that the US passed the *Undertaking Spam, Spyware and Fraud Enforcement with Enforcers Beyond Borders Act 2006*, which broadened the US powers to reciprocate information sharing and collection of information and evidence for foreign agencies.[15] It was submitted that the bilateral agreement did not require any strengthening at this stage.

8.13 In addition to the US, the ACCC also has MOUs to facilitate international cooperation with other counterparts, including with agencies in the UK, Korea and New Zealand.[16]

Litigation Issues – Online Scams

8.14 The Committee was told that whether enforcement action under the *Trade Practices Act 1974* (Cth) is taken in Australia will often depend on jurisdictional and evidential issues. Jurisdictional issues arise when the offender is located outside Australia, and, in some cases, the difficulty of ascertaining the identity and location of scam promoters can make enforcement more difficult.

8.15 Some of the issues identified were:

- if the ACCC requires further evidence it would ordinarily use its statutory powers but cannot serve those notices in other jurisdictions;
- court documents need to be served on parties outside the jurisdiction. This requires leave of the court and then service of documents in the relevant country once the relevant respondent is located; and
- the utility of orders the ACCC may seek from a court may be undermined by the difficulty in enforcing those against the respondent.[17]

8.16 While these challenges are present in a number of consumer protection genres, the ACCC said such problems are particularly prevalent in the online scam environment.[18]

---

14 Available at <http://www.ftc.gov/os/2000/07/ftcacccagrmnt.htm>, viewed 10 April 2010.

15 ACCC, *Supplementary Submission 46.1*, p.14.

16 ACCC, *Supplementary Submission 46.1*, p.14.

17 ACCC, *Supplementary Submission 46.1*, p.1.

18 ACCC, *Submission 46*, p.1.

8.17 Out of approximately 12,000 complaints of online scams in the 2008-2009 financial year there were only two matters in 2009 concluded by the ACCC. The two cases categorised by the ACCC as 'cyber crime or cyberscam activity', were referred to the ACCC from the US. The ACCC said that 'assistance in providing information about conduct based in Australia affecting consumers more generally' was influential in the decision to pursue the matters.[19]

8.18 One earlier example where the ACCC had a measure of success was the 2003 *Sydney Opera House Case,* which involved a fraudulent website hosted and administered from overseas that purported to be the official booking site for the Sydney Opera House. Consumers in the UK and Europe had been caught by the fraudulent site. In August 2003, the Federal Court declared that the site was illegal and, although the injunction could not be formally registered in the US, the court accepted that Australian orders would support Australia's request for assistance from the US Federal Trade Commission.[20]

8.19 Even where an alleged perpetrator is outside the country there are sometimes opportunities to use Australian enforcement orders against them within this jurisdiction. The ACCC said:

> The ability to quickly transfer funds and the propensity to morph and phoenix without the same reputational issues mainstream traders have make effective enforcement orders very important. Court orders may be sought to secure assets in Australia, such as funds in bank accounts, to ensure money is available for consumer redress.[21]

8.20 In 2009, the *Designer Brand Outlet Case,* a matter referred by the US Federal Trade Commission (FTC) in June 2008, was concluded and serves as a useful case study (see below).[22]

---

19 Mr Scott Gregson, Group General Manager, Enforcement Operations, ACCC, *Transcript of Evidence,* 18 November 2009, p.6.

20 ACCC, *Submission 46*, p.7.

21 ACCC, *Supplementary Submission 46.1*, p.3.

22 *ACCC v Bindert (Ben) Loosterman & Ors* FCA 1391/2008; Resolved by consent with final orders available on the Federal Court Website at: <https://www.comcourts.gov.au/file/Federal/P/NSD1391/2008/3549912/event/25652026/document/150771>, viewed 10 April 2010.

ACCC v Bindert (Ben) Kloosterman & Ors

The FTC provided the ACCC with a number of consumer complaints. In addition, the ACCC also received complaints from consumers in the United Kingdom and a number of Australian states. The complaints variously related to Designer Brand Outlet accepting payment and not delivering the goods, goods received not matching the goods ordered (including issues relating to authenticity), refunds not provided and consumers unable to contact the company.

The investigation included liaison with international counterparts, a major Australian bank responsible for the credit merchant facilities for the website and Australian Domain Registrar, Netregistry Pty Ltd, in relation to the registration of the website.

In September 2008, the ACCC sought interim injunctions against the operators of the website, Mr Bindert (Ben) Kloosterman and Ms Xin Fang (Lucy) Shi, and asset preservation orders to ensure the assets of the company and individuals were not sent off shore.

In December 2008 final orders were made, with the Court declaring that the alleged conduct was in breach of ss. 52, 53(a), 53(d), 53(g), 55 and 58 of the *Trade Practices Act 1974.* Injunctions restraining the operators of the website from engaging in similar conduct in the future on any website were also made, and a timeframe for negotiating a compensation scheme for affected consumers was also set out.

In April 2009, the ACCC reached agreement with the respondents as to terms of compensation for affected consumers. In June 2009 the monies received by the respondents was returned to consumers that had provided a valid claim for compensation.

Reciprocal registration and enforcement of judgements

8.21 The reciprocal registration and enforcement of overseas judgments is dealt with under the *Foreign Judgements Act 1991* (Cth) but the scheme only applies to 'enforceable money judgments' unless the regulations also provide for 'non-money' judgements. At the commencement of this inquiry pecuniary penalties were not available in relation to consumer protection matters under the *Trade Practices Act 1974* (Cth). And, to date declarations of breaches of the *Trade Practice Act 1974* (Cth) and injunctions to prevent future violations are not covered by the scheme.

8.22 The *Australian Consumer Law* is intended to replace provisions of the various State and Territory Acts and *Trade Practices Act 1974* (Cth) and to be fully implemented nationally by 31 December 2010.[23] Part of these reforms includes stronger remedies, including empowering regulators to seek civil and pecuniary penalties, injunctions, damages, and compensation orders for contravention of the *Australian Consumer Law*.

Committee View

8.23 The availability of money judgments under the new *Australian Consumer Law* means that the *Foreign Judgments Act 1991* (Cth) will have greater potential for utility in the field of consumer protection.[24] However, whether non-money orders should be provided for by regulation under the *Foreign Judgments Act 1991* (Cth) remains an outstanding question.

8.24 In the Internet age national governments need to utilise all the mechanisms available to enforce their consumer protection regimes. In the *Sydney Opera House Case*, Justice Sackville took the opportunity to comment that:

> While domestic courts can, to a limited extent, adapt their procedures and remedies to meet the challenges posed by cross border transaction in the Internet age, and effective response requires international co-operation of a high order. As the evidence in this case shows, some steps have been taken to secure that cooperation ... [but] much more needs to be done if Australian consumers are to be adequately protected against fraud or misleading conduct perpetrated over the Internet.[25]

8.25 This Committee is of the view that combating the globalisation of online scams and other forms of cyber crime requires a comprehensive and integrated approach to enforcement. As Australia moves into an era of stronger and nationally consistent consumer protection law it makes sense to pay attention to the international cooperation and enforcement aspects of the new regime.

---

23 The Trade Practices Amendment (Australian Consumer Law) Bill 2009 passed both Houses of Parliament on 17 March 2010. State and Territory Governments will introduce application legislation to apply the entire Australian Consumer Law in each jurisdiction.

24 The *Foreign Judgments Act 1991* (Cth) provides a mechanism for the registration and enforcement of overseas judgments on the basis of 'substantial reciprocity of treatment' (s.5(1)).

25 *ACCC v Chen* [2003] FCA 897 at 62.

8.26 The bilateral MOUs with the US and other countries and the ICPEN Memorandum are intended, among other things, to improve the effective enforcement of consumer protection laws and have benefits for consumers everywhere. Further institutionalising enforcement through formal court procedures will also enable the Australian regulator to assertively and efficiently enforce Australian law to protect Australian consumers. This is not a substitute for administrative cooperation, which remains of vital importance and in many cases will be the most appropriate way forward. However, closing the gap between the *Australian Consumer Law* and the *Foreign Judgments Act 1991* (Cth) is one area of legislative reform that can strengthen the protection of consumers in the Internet age.

Recommendation 22

That the Australian Government ensure that:

- **remedies available under the new Australian Consumer Law can be effectively asserted against perpetrators outside Australia; and**
- **the *Foreign Judgments Act 1991* (Cth) be amended to allow for the reciprocal registration and enforcement of non-money judgments made under the Australian Consumer Law.**

Consumer Privacy and the Problem of Spyware

8.27 The evidence has demonstrated the complex interplay between different crime methodologies that combine activities crossing criminal and civil law boundaries. The Cyberspace Law and Policy Centre (CLPC) argued that regulatory and policy analysis tends to focus on one or two elements (DDOS and malware or spam and phishing) creating artificial distinctions that result in wrongly targeted approaches.[26]

8.28 For example, the installation of unwanted software without the user's informed consent was said not to be 'expressly illegal in Australia'.[27] The CLPC said the existing approach misses the connection between legitimate

26 CLPC, *Supplementary Submission 62.1*, p.4.

27 CLPC, *Supplementary Submission 62.1*, p.5.

and illegitimate conduct, which if properly targeted could cut through the fragmentation in the Australian system.[28]

8.29 The *Trade Practices Act 1974* (Cth) does not explicitly address the problem of unauthorised installation of software *per se*. Whether an unauthorised installation of software contravenes the *Trade Practices Act 1974* (Cth) will depend on whether the conduct takes place within the context of misleading and deceptive conduct or false representation.

8.30 The problem of spyware illustrates the inherently complex relationship between legitimate commercial and criminal online conduct:

> … the distinction between spyware and adware can turn on the issue of informed consent: Spyware is software that is installed on a computing device and takes information from it without the consent or knowledge of the user and gives that information to a third party.[29]

8.31 Spyware can be deployed through various means, for example, through free software that includes browser toolbars and personal organisers, downloaded accidentally via an email attachment or simply clicking onto a website.[30] Adware is software that supports the automatic download and display of advertisements and is generally bundled as part of a software package. With permission it also often tracks the end users web browsing activity, this personal information is then used to tailor the display advertisements.

8.32 Where adware is deployed through a third party that bundles the software with its own product, liability is transferred to the third party affiliate through an online contract.[31] In this complex arrangement the adware is less visible, the ability to avoid liability greatly enhanced and the prospect of genuine or informed consent probably redundant.

8.33 In 2005 a Spyware Bill was introduced to the Parliament which sought to ensure that no program, cookie or tracking device could be installed without the user being given full and clear information about the purpose of the program or tracking device.[32] However, in a review of the legislative framework the then Government concluded that spyware is like other forms of malware and existing criminal offences adequately deal

---

28 CLPC, *Supplementary Submission 62.1*, p.5.

29 DCITA, *Taking Care of Spyware*, September 2005, p.3.

30 K Howard, Mallesons Stephen Jacques, *Computers and Law*, March 2006, p.17.

31 CLPC, *Submission 62*, p. 7.

32 Paul Clarke, *Do we need a Spyware Act?*, Internet Law Bulletin, Volume 8 Issue 4, p. 58.

with the problem.[33] In addition, the *Privacy Act 1998* (Cth) prohibits the unlawful collection of personal information; the *Trade Practices Act 1974* (Cth) applies where spyware is downloaded in the context of misleading or deceptive conduct and the *Australian Securities and Investments Commissions Act 2001* (Cth), *Corporations Act 2001* (Cth), and the *Telecommunications Act 1997* (Cth) also apply.[34]

8.34 It was contended that Australia's legal framework is convoluted and works against investigation and prosecution.[35] The ACCC said that:

> Careful consideration is needed to determine whether ... [it] would be appropriate to apply industry specific regulations rather than general prohibitions.....[36]

8.35 The CLPC argued that:

> From the legal perspective, charges and fines have not been made against *a single* corporation or organisation for spyware or malware distribution in Australia. Contrast this finding to jurisdictions that have mandated an authority such as OPTA or the United States Federal Trade Commission, where over 100 fines and charges have been made against spyware and malware distribution companies such as DollarRevenue in the United States, Canada and Europe.[37]

The DollarRevenue Case

8.36 The CLPC cited the example of Dutch company DollarRevenue, an advertising company, held responsible for the illegal installation of spyware on 22 million computers. The company used an affiliate business model where third parties agreed to deploy DR Software through ActiveX and software bundling (Active payouts in Northern America average $.25c per installation).[38] According to CLPC, the affiliates use a variety of means to trigger DR software downloads including spam, botnets, and chatroom sessions. Although the company is structured legally, in practice the model is intended to transfer liability to third party affiliates through an online contract.[39]

---

33 DICITA, *Outcome of the Review of the Legislative Framework on Spyware*, 2004

34 DICITA, *Outcome of the Review of the Legislative Framework on Spyware*, 2004.

35 CLPC, *Supplementary Submission 62.1,* p.8.

36 ACCC, *Supplementary Submission 46.1*, p.11.

37 CLPC, *Supplementary Submission 62.1,* p.8. Emphasis added.

38 CLPC, *Supplementary Submission 62.1*, p.7.

39 CLPC, *Supplementary Submission 62.1*, p.8.

8.37 The CLPC submitted that DollarRevenue is or has also been involved with 'malicious spam, iframe injections and Trojan downloads, which initialise information capturing software (such as passwords or browser histories)'. The CLPC also stated that IT security company Sunbelt Malware Research Labs identified over 2,000 additional adware/spyware programs downloaded in a single DR software application.[40]

8.38 Installing software without a user's informed consent is a violation of the Dutch *Telecommunications Act 2004*, and the Dutch Telecom Regulator has powers to investigate, fine and issue penalties and compliance notices. The regulator also works with the Dutch police 'to bring criminal charges where it is warranted'.[41] In this case, the company was fined by the regulator for installing unsolicited software without the informed consent of computer owners. The company directors are reported to be subject to separate criminal investigation.[42]

8.39 The AGD reiterated to the Committee that the computer offences would 'generally apply in cases where software, such as spyware, is installed in a PC without the owner's informed consent' (s.477.2 makes it an offence to use the Internet to infect a computer with spyware).[43] However, the CLPC's main point was that legitimate adware makes consumers more vulnerable to illegitimate spyware, and other malware applications such as Trojans that 'collect usernames and passwords for Internet banking and e-commerce websites'.[44]

Committee View

8.40 The Committee believes that while there must be appropriate criminal offences, traditional criminal law enforcement will not always be the most effective approach. Tackling the problem through clear consumer protection measures will help to protect consumer privacy, reduce the opportunities for cyber crime and support criminal law enforcement goals.

8.41 This approach will also support consumer education on the importance of reading the terms and conditions of user agreements and licences, which are often given little or no attention. The browser activity and online

40 CLPC, *Supplementary Submission 62.1*, p.6.

41 CLPC, *Supplementary Submission 62.1*, p.8.

42 CLPC, *Supplementary Submission 62.1*, p.5.

43 Note also that corporate liability can apply where the fault element is attributable to a body corporate that has expressly, tacitly or impliedly authorised the commission of the offence. See Chapter 2 of the Criminal Code.

44 CLPC, *Submission* 62, p. 6.

purchasing habits of an end user are, in our view, a form of personal information and is unlikely to be consented to in the offline world. While there are technical solutions, not all anti-virus and spyware detection software works all the time. Additionally, consumers may be being surreptitiously tricked into 'consenting' to the download. There is also a problem of young people, including children, agreeing to downloads that they not understand or do not have legal capacity to consent to.

8.42 In theory, the Criminal Code applies to the unauthorised installation of spyware, but the lack of enforcement action (domestically or in concert with international partners) suggests Australian agencies are not making inroads into this particular problem. In any event, the existence of a criminal offence on the statute book does not negate the role that a more strategically positioned consumer protection measure can play in preventing further criminal activity. It also empowers ordinary citizens to respond to privacy violation in a commercial context and strengthens regulators – in this case the ACCC and the Privacy Commissioner.

Recommendation 23

That the Treasurer amend the Australian Consumer Law to include specific protections against the unauthorised installation of software programs:

- **the reform should target the unauthorised installation of programs that monitor, collect, and disclose information about end users' Internet purchasing and Internet browsing activity;**
- **the authority to install a software program must be based on informed consent; and**
- **to obtain informed consent the licence/agreement must require clear accessible and unambiguous language.**

Information Standards

8.43 A common theme in the inquiry has been how to best get the e-security message across to ordinary consumers. The evidence canvassed in Chapter 4 highlighted that, although general levels of awareness are reasonable among the Australian public, this does not always translate

into action. The value of a national e-security awareness strategy is discussed in Chapter 10.

8.44 Some witnesses argued that providing e-security information at the point of sale may be the best time to prompt consumers to take protective action.[45] The Australian Computer Society (ACS) said:

> The ACS believes that governments should look to developing agreements with vendors to ensure that computer systems and mobile devices are not sold without supplying adequate e-security and cyber safety information that covers not only current threats but also emerging threats.[46]

8.45 The Australian Senior Computer Clubs Association (ASCCA) was clear that senior Australians must get consistent messages from both government and industry. The ASCCA said:

> That anti-virus software and a firewall should be pre-installed on all new computers purchased. An easy to understand brochure, written in plain English, outlining how to be safe online should also be provided with each purchase. Translating this brochure into relevant community languages should also be considered.[47]

8.46 Mr Peter Coroneos, CEO, Internet Industry Association (IIA) agreed that the industry needs to look at every point of contact with the consumer to get across the e-security message. He said:

> Absolutely. This is where we need to be lateral in our thinking. We need to look at every point in the chain from the initial purchase of the computer through the setting up of the computer to the ongoing usage of the computer. Each of those points represents an opportunity for awareness raising and behavioural change.[48]

8.47 The IIA used the example of routers and modems, which are vulnerable to being hijacked and the home user would have no way of knowing that it had occurred. Mr Peter Coroneos said that more needs to be done to promote router and modem security.[49] The IIA is working directly with

45 ACCAN, *Submission 57*, p.11.

46 ACS, *Submission 38*, p.4; ACCAN, *Submission 57*, *Surfing on Thin Ice: Consumers and Malware, Adware, Spam & Phishing,* p.11.

47 ASCCA, *Submission 63,* p.4.

48 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.19.

49 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.20.

manufacturers and distributors to develop standardised information to give to consumers at point of sale of these devices.[50]

Committee View

8.48 There was general agreement that point of sale information is a useful step in getting out the e-security message to consumers. This will take different forms depending on the product. There is no impediment to the IT industry creating an industry wide e-security messaging standard that applies to the point of sale but none has yet emerged. The Committee is conscious of IIA's efforts in this regard, but considers that a more comprehensive approach is needed if we are to see any real gains in promoting an e-security culture.

8.49 The Australian consumer protection legal framework provides for information standards that industry must comply with in order to protect consumers for known risks. Under the new *Australian Consumer Law*, there will be a national approach and new information standards will be created by the Commonwealth Minister.

8.50 The Committee is of the view that the problem of cyber crime, which is predicted to continue to grow in volume and sophistication, poses a sufficiently serious risk of economic and social harm to Australian consumers that a national information standard is warranted. The ACCC should, in consultation with manufacturers and distributors of personal computers, mobile phones and related IT devices such as modems and routers, develop information standards to address the e-security vulnerabilities of these products and the provision of e-security information to consumers at the point of sale.

50 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.19.

Recommendation 24

That the Australian Competition and Consumer Commission, in consultation with manufacturers and distributors of personal computers, mobile phones and related IT devices such as modems and routers, develop information standards to:

- **address the e-security vulnerabilities of these products and the provision of e-security information to consumers at the point of sale; and**
- **require that the information is presented in a manner that is clear and accessible to a non-IT literate person.**

IT Vendor Responsibilities

Security of IT Products

8.51 The Committee was told that the problem of cyber crime can largely be traced to the lack of adequate testing of hardware and software products before they are released onto the market.[51] There has been a steady climb in the number of vulnerabilities reported, which was illustrated to the Committee by the IBM *Internet Security Systems X Force 2008 Trend and Risk Report* published in January 2009.[52]

8.52 The IT vendors usually follow up with security updates and patches, which consumers can often receive automatically, but these may not follow for many months and can involve additional cost and inconvenience. Major vendors, such as Microsoft, provide options for automatic updates but as the evidence has indicated many consumers do not make use of the updates.

8.53 As AusCERT pointed out, the lack of security in technology products exposes all end users (including government, business and the home users) to e-security risks:

51 ACS, *Submission 38*, p.10; AusCERT, *Submission 30*, p.4; Internet Safety Institute, *Submission 37*, p.6; see also, C Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Congress Research Paper, Updated January 29, 2008, p.26.

52 Internet Safety Institute, *Submission 37*, p.6; viewed 13 April 2010, <http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf page 18>.

> We have built vast networks and information systems using technology that cannot be properly or easily secured, ... despite the fact that the software security industry is big business in its own right.[53]

8.54 In 1998, the National Security Agency (NSA), in its paper *The Inevitability of Failure: The flawed assumption of security in modern computing environments* (1998), summarised a key aspect of the problem as follows:

> The goal of this paper is to motivate a renewed interest in secure operating systems. [The NSA] argues that the threats posed by the modern computing environment cannot be addressed without support from secure operating systems and, [...] any security effort which ignores this fact can only result in a "fortress built upon sand".[54]

8.55 The problem extends beyond operating systems to software applications, which AusCERT said need to be securely designed because vulnerabilities in applications such as browser plug-ins, for example Adobe Flash and Shockwave, can compromise entire computer systems. The general point was made that NSA analysis remains valid but in fact the threat environment has 'substantially worsened and the modern software environment has not kept pace.'[55]

8.56 The ACS concurred with this overall assessment:

> Ultimately, many cyber crime risks can be mitigated by industry developing more secure hardware and software and integrating improved security into the software and hardware development cycles. Technology must become more trustworthy in terms of its security vulnerabilities.[56]

8.57 There has been a trade off in the market between security with speed, interoperability and the desire to allow an openness that will foster innovation. However, as ACS said, the downside is that:

> The competitive nature of computing and the rush to market to achieve first mover advantages appear to be driving a less thorough testing of code, system and hardware vulnerabilities.[57]

---

53 AusCERT, *Submission 30*, p.4.
54 AusCERT, *Submission 30*, p.4.
55 AusCERT, *Submission 30*, p.4.
56 ACS, *Submission 38*, p.10.
57 ACS, *Submission 38*, p.10.

8.58 According to ACCAN's research the cost and inconvenience to consumers is significant and warrants specific research, perhaps by the Productivity Commission. In ACCA's report *Surfing on Thin Ice: Consumers and Malware, Adware, Spam & Phishing* it was found that:

> More than 1 out of every 10 consumers surveyed had suffered financial loss or unexpectedly high bills as a result of security problems, with the majority of these losses exceeding $100. These results, combined with written comments we received, highlight the significant burden consumers face as a result of online security issues and hints at their impact on the economy, consumer satisfaction and productivity. Projected to the wider Australian population, consumers as a whole may be experiencing hundreds of millions of dollars of financial loss as a result of security problems, and many may be experiencing emotional distress and spending significant amounts of time dealing with security issues.[58]

8.59 The lack of IT security and the risks and costs of cyber crime are also a factor that inhibits the growth of e-commerce. It has been reported that although over 90 per cent of small and medium sized businesses are connected to the Internet, the risk that company systems can be hacked into is the number one concern in relation to e-commerce.[59]

8.60 The ACS would like to see vendors embrace secure development of applications more fully. In their view, this should be done on a voluntary basis and 'consistent with the international standards to which all hardware and software developers and suppliers sign up to comply with'.[60]

8.61 A voluntary security assurance scheme based on an International Common Criteria Framework already exists. In Australia, the Defence Signals Directorate (DSD) provides evaluation and testing of products as part of this scheme in its role of providing technical security support to government departments and agencies.[61] Lists of certified products are available online but the audience is generally IT security professionals working within government.

---

58 ACCAN, *Surfing on Thin Ice: Consumers and Malware, Adware, Spam & Phishing,* p.24.

59 Sensis, *E-Business Report: The Online Experience of Small and Medium Enterprises*, July 2008, p.5; Sensis, *E-Business Report: The Online Experience of Small and Medium Enterprises*, August 2009, pp.5 and 11.

60 ACS, *Submission 38*, p.11.

61 Australasian Information Security Evaluation Program.

8.62 Microsoft Australia advocated a wider take up of the existing framework for testing and evaluation of the security features of IT products.[62] However, as AusCERT pointed out, although software assurance occurs as part of the Common Criteria program there is no requirement for products to undergo security assurance checking before being released to the market. Nor is there any requirement for those that do undergo the testing process to display the level of security assurance obtained to consumers.[63]

8.63 According to AusCERT most products do not achieve a level of security that is sufficient for the purposes of reducing cyber crime:

> Hence, a lot more work needs to be done by software manufacturers to attain a software evaluation that allows consumers to have confidence that they are buying products that are relatively secure to deploy, ie are able to reliably defend themselves from attack. This applies to both operating systems manufacturers and application software, both proprietary and open source.[64]

8.64 The ACCC confirmed that there is no code of practice or standards under the *Trade Practices Act 1974* (Cth) that require IT manufacturers to build security into their products. As Mr Nigel Ridgway, Group General Manager, Compliance, Research, Outreach and Product Safety, ACCC, pointed out, the problem of e-security vulnerabilities in hardware and software products have been responded to by the growth of anti-virus products.[65]

8.65 The ACS suggested that to drive greater trustworthiness of the technology manufacturers should advertise their compliance with security standards (for example the Common Criteria). This would enable consumers to make more informed choices about the security of the product.[66] AusCERT took a similar approach and advocated a software labelling scheme.[67] This would require national regulation requiring software manufactures to display consumer labels with independent evaluation of the product's security.[68]

---

62 <http://www.commoncriteriaportal.org/theccra.html>

63 AusCERT, *Submission 30*, p.21.

64 AusCERT, *Submission 30*, p.21.

65 Mr Nigel Ridgway, ACCC, *Transcript of Evidence,* 18 November 2009, p.7.

66 ACS, *Submission 38*, p.11.

67 AusCERT, *Submission 30*, p.20.

68 AusCERT, *Submission 30*, p.20.

8.66 As noted above, Microsoft advocated a greater take up of the existing testing and evaluation scheme under the Common Criteria. However, they argued that any legislative reforms should protect innovation in the IT industry and government should fund research into security issues.[69] Symantec also argued that a healthy competitive market in security solutions was vital to promote innovation and combat the fast pace of the changing threats.[70]

Committee View

8.67 Throughout this inquiry liability has been a key issue that many stakeholders appeared reluctant to address directly. When considering the same problem in the UK, the House of Lords Science and Technology Committee concluded that efforts to promote better security standards have been hampered by a lack of commercial incentives and that IT vendors can too easily shift the risks and costs onto consumers through licensing agreements.[71] The consumer group, ACCAN, has indicated that it believes the cost to consumers is such a significant issue that it should be looked into by the Productivity Commission.

8.68 The question is what is the best way to drive manufacturers toward greater security in hardware and software applications? The Committee agrees with the House of Lords' general view that industry should be making security a much higher priority. While it has been important to foster innovation and competition the Committee queries whether the market may have gone too far in this direction at the expense of the security of consumers. The widespread claim that innovation and interoperability will suffer if security is given a higher priority is not entirely convincing.

8.69 The Committee accepts that, to a significant extent, there is an 'arms race' to discover and exploit vulnerabilities by highly sophisticated criminal networks. Vulnerabilities cannot be entirely eliminated because of the complexity of these products and the importance of interoperability with third parties. However, in our view, manufacturers must start taking their duty of care to their customers more seriously.

8.70 The costs to end users, especially ordinary consumers but also small and medium size businesses, have been largely hidden. A more secure online

69 Microsoft Australia, *Submission 35*, p.1.

70 Symantec, *Submission 32*, p.12.

71 Science and Technology Committee, *Personal Internet Security*, Volume 1 Report, House of Lords, August 2007, pp.41-42.

environment is needed to build and maintain trust, protect vulnerable end users as much as possible from cyber crime and support the expansion of e-commerce and the digital economy.

8.71 It is the Committee's view that consumers should not have to rely on the general prohibition on false representation or misleading or deceptive conduct. A more direct approach would be to require by law that IT manufacturers that sell product in Australia should disclose known vulnerabilities so that a consumer can make an informed choice at the point of purchase. To improve security standards manufacturers should adopt best practice to testing and evaluation *before* release to market. There is a case for specific industry regulation through a code of practice on security standards based on the internationally accepted standards regime. This framework could then provide the basis for a security labelling scheme.

8.72 However, the Committee is conscious there are difficulties with developing a single national regulation for the IT products industry that is global in nature. One issue is the need for such a regime to be consistent with Australia's international trade obligations.

8.73 The Productivity Commission is an appropriate body to conduct in depth investigation into the economic and social costs of the systemic security issues in the IT hardware and software market, and its impact on efficient functioning of the Australian economy. At this stage the Committee recommends that this in depth investigation be carried out to provide more comprehensive analysis to support future policy development.

Recommendation 25

That the Treasurer direct the Productivity Commission to conduct an in depth investigation and analysis of the economic and social costs of the lack of security in the IT hardware and software products market, and its impact on the efficient functioning of the Australian economy.

That, as part of its inquiry, the Productivity Commission address the merits of an industry specific regulation under the Australian Consumer Law, including a scheme for the compulsory independent testing and evaluation of IT products and a product labelling scheme.

8.74 That said, inadequate security is a systemic problem in the IT market and the risks and many of the costs of cyber crime are widely accepted and known. The Committee believes that IT manufacturers have an obligation to make products as secure as possible (subject of course to the rules of anti-competitive conduct). As an interim step, end users should have statutory cause of action against manufacturers who release products to market with known vulnerabilities that result in losses that could not otherwise have reasonably been avoided. The courts are well equipped to apply principled reasoning to complex facts and work out the liability between respective multiple parties.

Recommendation 26

That the Treasurer consult with State and Territory counterparts with a view to amending the Australian Consumer Law to provide a cause of action for compensation against a manufacturer who releases an IT product onto the Australian market with known vulnerabilities that causes losses that could not have reasonably been avoided.

Security Settings

8.75 One of the issues raised with the Committee was the lack of sufficient prompting to end users to adopt more secure settings when setting up new products. A case in point is the vulnerability of routers to being hacked and compromised, which affects the security of an entire computer system. It is widely known and accepted that consumers often do not change router settings and this is a risk factor that could be addressed without significant expense to manufacturers.[72] But despite industry knowledge that consumers often do not change the default settings, no industry wide practice has yet emerged to address it.

8.76 The question was why manufacturers do not make default settings as secure as possible or ensure that when setting up there are automatic prompts or actually require the consumer to adopt the strongest possible setting? For example, in the case of a router, a prompt that requires the user to change the setting with a strong password before it can be used would be a simple solution. Secondly, is the failure of industry to provide

72 See discussion, *Transcript of Evidence,* 18 November 2009, pp.12-15.

adequate e-security prompts and secure settings a breach of the *Trade Practices Act 1974* (Cth)?

8.77 Under the *Trade Practices Act 1974* (Cth), consumers are entitled to products that are 'fit for purpose' and 'free of defects'. These entitlements are statutory conditions that are implied into consumer contracts. In essence, this means that goods must match the description given; be fit for the purpose for which they have been sold; and be of 'merchantable quality'.[73]

8.78 A product, such as a router, which is 'fit for purpose' at the point of sale is arguably no longer 'fit for purpose' if the way in which it is set up actually makes the computer system more vulnerable to attack. Some might regard the ability to connect a router to a computer system and the Internet without adequate security setting as an inherent defect in the design of the product.

8.79 The current legal regime does not oblige manufacturers to take any responsibility for designing security into the product.[74] It is not a statutory condition implied into a contract of sale, and nor is it addressed by any industry specific regulation or industry code of practice. As Mr Nigel Ridgway, ACCC, explained:

> We do look at these issues on a case by case basis but, in the hypothetical, something that functions quite well or quite appropriately, absent that malicious attack by a third party, is not, I would think, going to fall foul of the warranty provisions.[75]

Committee View

8.80 It seems likely that the vast majority of end users, whether they are home users, or small or medium sized businesses, lack the knowledge to make an informed choice about appropriate security setting for their operating system, the additional hardware devices or the software applications used on it. This appears to be a widespread and well known problem that neither governments nor industry can ignore, because of the financial and social impacts of cyber crime.

---

73 The latter means the goods should be free from defects not obvious at the time of purchase and be of reasonable quality and performance taking into account the price and description at the time of purchase.

74 Mr Nigel Ridgway, ACCC, *Transcript of Evidence,* 18 November 2009, p.15.

75 Mr Nigel Ridgway, ACCC, *Transcript of Evidence,* 18 November 2009, p.15.

8.81 The Committee believes that IT vendors can do more to prompt and guide consumers to adopt better security without locking consumers into completely secure systems that will prevent interoperability. The industry should be encouraged to take account of the reality that most consumers are not IT literate and are unlikely to understand all the implications of poor security settings.

Recommendation 27

That the manufacturers of IT products adopt a best practice approach that ensures products are designed to prompt and guide end users to adopt more secure settings.

That the Australian Government monitor industry practice in this regard, and promote international standards that put a higher priority on security through product design.

9

Privacy Measures to Combat Cyber Crime

Introduction

9.1 Vast amounts of personal information are increasingly being transmitted over the Internet and stored on digital devices. Contributors to the inquiry argued that this growing amount of digitised personal information places end users at a higher risk of identity theft and fraud, and argued that ensuring the privacy of end users' personal information is central to the prevention of cyber crime.[1]

9.2 The Office of the Victorian Privacy Commissioner (OVPC) submitted:

> The protection of information privacy, and reduction of e-security risks, are closely related concepts. Cyber crimes necessarily involve an invasion of an individual's privacy, through access or fraudulent use of personal information.[2]

9.3 This section briefly describes the legislative framework for privacy protection in Australia, and examines five key areas to further protect the personal information of Australian end users:

- issues relating to the *Privacy Act 1988* (Cth)(the *Privacy Act*);
- consistency between Commonwealth, State and Territory privacy regulation;
- industry codes of practice;

---

1 See for example: Australian Merchant Payments Forum, *Submission 17*, p.1; Internet Industry Association, *Submission 54*, p.4; Internet Society of Australia, *Submission 45*, p.5.

2 OVPC, *Submission 33*, p.2.

- international regulation and cooperation; and
- privacy audits.

Overview of Australian privacy protection legislation

9.4 The *Privacy Act* regulates the protection and use of personal information, including financial details and identity information. This is primarily achieved through two sets of privacy provisions: the Information Privacy Principles, which regulate Australian and Australian Capital Territory Government 'agencies'; and the National Privacy Principles, which regulate all private sector 'organisations' with an annual turnover of over $3 million. The *Privacy Act* establishes the Office of the Privacy Commissioner (OPC), an independent statutory body, to promote and protect privacy in Australia.[3]

9.5 The *Privacy Act* permits organisations to develop and enforce their own privacy codes that, once approved by the OPC, replace the National Privacy Principles for those organisations bound by the code. Codes must have a body established to oversee the operation of the code, and to receive complaints.[4]

9.6 The OPC has further responsibilities under: the *Data-matching Program (Assistance and Tax) Act 1990* (Cth), in regulating government data-matching programs; the *National Health Act 1953* (Cth), in regulating the handling of health information collected under the Medicare and Pharmaceutical Benefits Scheme; the *Crimes Act 1914* (Cth), in regulating information on past convictions; and the *Telecommunications Act 1997* (Cth).[5]

9.7 The OPC's role in relation to the *Telecommunications Act* is of particular relevance to cyber crime, as it deals with the use and disclosure of certain information by telecommunications service providers. These regulations apply to the contents of a communication being transmitted by a carriage service, and information incidental to the delivery of a carriage service, such as Internet Protocol addresses, unlisted telephone numbers or any

3 OPC, *Submission 3*, pp.3-7.

4 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.263-264.

5 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.267.

address.[6] It is unclear whether such information would be considered personal information under the *Privacy Act*.[7]

9.8 It should be noted that the privacy provisions of the *Telecommunications Act* do not extend to information that may be collected by a telecommunications provider for purposes unrelated to the provision of a carriage service (such as a customer list purchased for marketing purposes). In such cases, the *Privacy Act* still plays a central role in protecting information held by telecommunications providers.[8] The Committee did not receive evidence on the adequacy of the privacy provisions of the *Telecommunications Act*, however the issue is discussed extensively in Chapter 71 of the ALRC's review.[9]

9.9 At the State and Territory level, most jurisdictions have additional legislation to regulate their respective public sector organisations, and to establish independent regulators. The exceptions are South Australia and Western Australia, who maintain administrative schemes to protect privacy, but do not currently have specific legislation or an independent regulator.[10]

9.10 In May 2008 the Australian Law Reform Commission (ALRC) completed a review of the *Privacy Act*. The ALRC's report, *For Your Information: Australian Privacy Law and Practice*, made 295 recommendations on a broad range of topics relating to the *Privacy Act* and the privacy legislative framework more broadly, including issues relating to the protection of privacy online.[11]

9.11 The Government is responding to the review in two stages. The first stage dealt with 197 of the recommendations and was released on 14 October 2009. The Government proposes to release draft legislation implementing the first stage response during 2010, and to consider the remaining 88 recommendations once the first stage of reforms has been progressed.[12]

---

6 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.2381-2382.

7 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.2382.

8 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.2382.

9 See: ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.2377-2412.

10 OVPC, *Submission 33*, p.3.

11 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.110-129.

12 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

The Privacy Act 1988

9.12 Submitters to the inquiry endorsed a number of the ALRC's recommendations as measures that would assist in combating cyber crime. These are:

- the removal of certain exemptions that currently apply to the *Privacy Act*;
- mandated reporting of data breaches experienced by organisations; and
- measures to prevent the over collection of personal information.[13]

9.13 The OVPC noted two significant exemptions in the regulation of privacy in the private sector. First, private sector employee records are specifically excluded from the *Privacy Act*.[14] The OVPC argue that employee records often contain detailed personal information which, without mandated protection, may be vulnerable to being compromised.[15] Second, 'small businesses' with an annual turnover of less than $3 million are exempt from the *Privacy Act*. The OVPC note that these businesses may obtain vast amounts of personal information in the course of their activities, but are under no obligation to take precautions to protect this information.[16] The ALRC also cited small ISPs as examples of organisations that handle large amounts of personal information but are currently exempt,[17] (although small ISPs do have limited privacy obligations under the *Telecommunications Act*).

9.14 The ALRC 's 2008 review acknowledged both exemptions as limitations on privacy protection, and concluded that the exemptions were unjustified. The ALRC recommended that the exemptions be removed from the *Privacy Act*.[18] The Government is considering these recommendations in the second stage of its response to the ALRC's review.[19] The OVPC argued that the removal of the exemptions would assist in protecting from cyber crime:

13 OVPC, *Submission 33*, pp.4-8; OPC, *Submission 3*, p.8; Symantec Corporation, *Submission 32.1*, p.3; Australian Communications Consumer Action Network, *Submission 57*, p.72.

14 Employee records are protected by law in some States, such as Victoria.

15 OVPC, *Submission 33*, p.4.

16 OVPC, *Submission 33*, p.4.

17 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.1356.

18 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1392-1398, 1355-1356.

19 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

> Enhancement and expansion of existing privacy laws, to close exemptions and to ensure more organisations are covered, will go a long way to reduce potential data loss or privacy breaches. This in turn will reduce the potential for identity fraud or theft to be committed.[20]

9.15 The reporting of data breaches, or lack thereof, was also raised as a privacy issue. Symantec submitted that large amounts of personal information retained by private businesses continue to be compromised by data breaches, and that such compromises lead to a high risk of identity crime and fraud.[21] Currently, companies are not required to report to a regulator, or to notify individuals, when personal information retained on their system has been compromised by a data breach.[22] Companies may voluntarily report such breaches to a privacy commissioner, or directly to individual victims (the OPC has developed a guide to this effect)[23], however witnesses argued that many organisations continue to have a strong incentive to protect their reputation by not reporting breaches.[24] Both the OPC and OVPC argued that notifying individuals that their details have been compromised may permit individuals to take actions to mitigate the resulting risk of identity theft and fraud.[25]

9.16 The ALRC's 2008 review recommended that the *Privacy Act* should be amended to require an agency or organisation to notify the OPC, and affected individuals, when certain personal information is reasonably believed to have been compromised.[26] The Government is considering this recommendation in the second stage of its response to the ALRC's review.[27]

---

20 OVPC, *Submission 33*, p.4.

21 Symantec Corporation, *Submission 32.1*, p.3.

22 Fujitsu Australia Ltd, *Submission 13*, p.7.

23 OPC, *Guide to handling personal information security breaches*, OPC, August 2008.

24 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.41; Ms Alana Maurushat, Cyberspace Law and Policy Centre, *Transcript of Evidence*, 8 October 2009, p.33; Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.5.

25 OPC, *Submission 3, p.*12; OVPC, *Submission 33*, p.8.

26 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.1696.

27 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

9.17 A range of submitters endorsed this recommendation as a measure that would mitigate the risks of online fraud.[28] RSA further argued that such a requirement would provide certainty to businesses:

> In addition to alerting consumers to potential loss, such legislation would also provide businesses with a degree of certainty around their responsibilities and the protection of consumer data. Businesses are increasingly vulnerable to potentially serious economic, legal and social repercussions simply because they don't know what is required of them with regard to data breach notification. RSA is asking the Government to provide legislation that provides businesses with greater clarity into their responsibilities, while at the same time protecting the private information of individuals.[29]

9.18 Symantec, whilst supporting mandatory breach notification, cautioned that 'a balanced risk-based approach must be adopted to ensure that organizations and individuals do not find the framework overly burdensome'.[30]

9.19 The Committee heard that the overcollection of data further increases the risks of identity theft and fraud. The OVPC argued that there is an increasing trend for organisations to request personal information during a transaction for purposes unrelated to the transaction, such as marketing and advertising. For example, the OVPC cited the wide use of 'mandatory fields' in electronic forms, where users must submit specific (and sometimes unnecessary) personal information in order to access an online service. The OVPC stated that, as a result of overcollection, personal information held by organisations continues to become more comprehensive, and increases the risk of identity crime following a data breach. The OVPC advocated reducing the amount of information collected by organisations.[31]

9.20 The *Privacy Act* already provides that large organisations may only collect information that is necessary for one or more of its functions.[32] Similar regulations are provided by some State jurisdictions.[33] The ALRC's review

---

28 OPC, *Submission 3, p.*12; OVPC, *Submission 33*, p.8; Symantec Corporation, *Submission 32.1*, p.3; Australian Communications Consumer Action Network, *Submission 57*, p.72.

29 RSA, *Submission 28*, p.4.

30 Symantec Corporation, *Submission 32*, p.11.

31 OVPC, *Submission 33*, pp.5-6.

32 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.710.

33 OVPC, *Submission 33*, pp.4-7.

recommended that public and private organisations alike should be required to only collect information if necessary.[34] The Government accepted this recommendation in the first stage of its response to the review.[35] Dr Bendall, OVPC, supported this move and argued that such provisions could be given further efficacy by removing the exemptions relating to private sector employee records and small businesses mentioned above.[36]

9.21 The OVPC also argued that providing individuals with the option to remain anonymous in online transactions would further reduce overcollection.[37] The *Privacy Act* currently provides a limited right to anonymity in some transactions with large private organisations, but not with government agencies. [38] Legislation exists in some States to extend similar provisions to State government agencies.[39] The ALRC recommended that such regulation be expanded to all private organisations and public agencies so that individuals would have the option to interact anonymously, where lawful and practicable.[40]

9.22 The OVPC supported the proposal for anonymity provisions, and argued that such measures would ensure that 'less information is available to would-be cyber criminals in the event of a data breach'.[41] The ALRC's proposal for an anonymity principal has since been endorsed by the Government.[42]

34 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.732.

35 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.39.

36 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.40.

37 OVPC, *Submission 33*, pp.4-5.

38 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.706.

39 OVPC, *Submission 33*, pp.4-5.

40 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.706.

41 OVPC, *Submission 33*, p.5.

42 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.40.

Consistency among Commonwealth, State and Territory jurisdictions

9.23 Both the OPC and the OVPC argued that the current lack of consistency in privacy legislation among different jurisdictions in Australia represents a gap in privacy regulation and impedes the protection of personal information. Dr Bendall, OVPC, told the Committee:

> South Australia and Western Australia do not have any state based privacy legislation and they do not have an independent regulator. That is often an issue for us when Victorian information is being sent to those jurisdictions. There is a principle in our legislation that Victoria is meant to assure itself that the information is going to be as secure as it would be in Victoria. That is a bit difficult to do that there because there is no law, so it usually has to be done under memorandums of understanding or some other mechanism.[43]

9.24 The ALRC's 2008 review of the *Privacy Act* made recommendations to the effect that Commonwealth, State and Territory governments should agree to form an intergovernmental cooperative scheme to enact consistent legislation in each State and Territory for the handling of personal information.[44] The Government has not currently responded to these specific recommendations.[45] The OPC endorsed the proposal and argued that such a move would 'enhance e-security for information flowing across State and Territory boundaries'.[46]

Industry codes of practice

9.25 As mentioned above, the *Privacy Act* permits organisations to develop and enforce their own privacy codes that replace the National Privacy Principles.[47] Such codes are not widespread, and no such codes currently

43 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, pp.39-40.

44 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.219, 224-225.

45 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

46 OPC, *Submission 3*, pp.9-10.

47 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.263-264.

exist in the telecommunications or information and technology sectors.[48] While larger organisations in these sectors (many of which have detailed privacy policies[49]) are currently regulated under the National Privacy Principles, many smaller businesses that hold large amounts of information, such as small ISPs, are currently exempt from regulation.[50]

9.26 While such gaps in regulation would effectively be bridged by the removal of certain exemptions in the *Privacy Act*, the option also exists for organisations to adopt their own privacy codes to ensure the security of personal information.

9.27 In March 2003, the Internet Industry Association submitted a draft privacy code to the OPC for approval.[51] According to the draft version, the code would apply to IIA members, including small ISPs, who choose to adhere to the code.[52] The code is still currently being considered by the OPC.[53]

International cooperation

9.28 Given that digital personal information is increasingly collected or transferred across international boundaries, the OPC submitted that international cooperation on privacy and data protection is integral to mitigating e-security risks.[54]

9.29 Currently, the provisions of the *Privacy Act* and associated industry codes extend to foreign private organisations handling the personal information of Australian citizens. However, no specific provision exists in the *Privacy Act* to overseas government agencies.[55] The ALRC's review recommended that the *Privacy Act* should be amended to clarify that its provisions also

48 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.264.

49 See for example: Yahoo! Group Australia & New Zealand, *Submission 18*, p.2; PayPal, *Submission 60*, pp.8-9.

50 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.1356.

51 IIA, *Privacy Code Draft*, IIA, 2010, viewed 13 April 2010, <http://www.iia.net.au>.

52 IIA, *Internet Industry Privacy Code of Practice Consultation Draft 1.0*, IIA, pp.3-4.

53 OPC, *Privacy Codes Register*, OPC, 2010, viewed 13 April 2010, <http://www.privacy.gov.au>.

54 OPC, *Submission 3*, p.10.

55 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1081-1082.

apply to agencies outside Australia.[56] The Government has accepted this recommendation.[57]

9.30 In addition to these legislative measures, the OPC participates in a number of international forums by which information protection regulators and authorities form partnerships, exchange ideas and pass resolutions on cross-border data protection measures, and privacy issues more generally. These include:

- the Asia Pacific Privacy Authorities forum;
- the annual International Conference of Privacy and Data Protection Authorities;
- the Electronic Commerce Steering Group of the Asia Pacific Economic Community; and
- the Organisation for Economic Cooperation and Development Working Party on Information Security and Privacy.[58]

9.31 Dr Bendall, OVPC, raised concerns that large overseas organisations that retain large amounts of personal information, particularly social networking sites, represent a particular risk to privacy and must be dealt with cooperatively by regulators from different jurisdictions:

> I think [information posted on, and handled by, social networking sites] is a problem for privacy regulators and privacy law, and we are yet to come up with a way of effectively regulating it. It certainly has to be increasingly international. The difficulty is that it is not in one jurisdiction. Often you will be giving your information to a company that is somewhere else. ... those organisations often will claim they can do whatever they like with the information and keep it forever. Even if you cease your Facebook or Youtube site they will still hold the information, so part of it is a conversation with regulators.[59]

9.32 While this discussion may relate to privacy concerns more broadly in relation to social networking, it illustrates the current lack of protection for certain information that is transferred and held overseas. This lack of protection would appear to heighten the risk of identity crime.

---

56 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1104.

57 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.77.

58 OPC, *Submission 3*, pp.10-11.

59 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.45.

Privacy audits

9.33 The *Privacy Act* requires agencies and organisation to take reasonable steps to protect information from unauthorised access, use, modification and disclosure. These steps may include technical measures and organisational processes.[60] Technical measures to protect personal information are examined in Chapter 11.

9.34 Such measures will be particularly pertinent as governments continue to expand the number of services delivered via the Internet, and increasingly exchange and store personal information in digitised form. For example, $467 million of funding was recently announced to form a national e-Health records system.[61] Similarly, the *Government 2.0 Taskforce* has made a number of recommendations encouraging agencies to increase their online engagement with the public.[62] The Committee heard that this growing amount of digitised information, coupled with increased internet speeds, will increase the risks of identity theft and fraud.[63]

9.35 The OVPC suggests that government agencies and private organisations should undertake regular privacy audits to identify breaches of privacy, and risks of such breaches, and to ensure that information is protected at all stages of the information cycle, from collection through to disposal.[64]

9.36 Currently, the OPC encourages, but does not require, government agencies to undertake 'privacy impact assessments' (PIAs) when enacting a new law or starting a new project. Such assessments seek to identify and remedy risks to privacy and personal information during the planning and development stage of such activities. The OPC has not specifically encouraged the use of PIAs by private organisations. The ALRC's review recommended that the OPC should be empowered to direct agencies to provide PIAs on new projects. The ALRC also recommended that the OPC publish guidance on PIAs for organisations and that, in five years, a review should determine if the OPCs directive power should be extended

60 OPC, *Submission 3*, p.6.

61 The Hon Nicola Roxon, *Personally Controlled Health Records for all Australians*, media release, Parliament House, 11 May 2010, viewed 12 May 2010.

62 Government 2.0 Taskforce, *Engage: Getting on with Government 2.0*, Australian Government, December 2009, pp.xvii-xviii.

63 AusCERT, *Submission 30*, p.9; Lockstep, *Submission 36*, p.10; ATO, *Submission 59,* p.4; Mr Michael Cranston, ATO, *Transcript of Evidence*, 16 September 2009, p.2.

64 OVPC, *Submission 33*, pp.7-8.

to also cover organisations.[65] The Government has accepted these recommendations.[66]

9.37 Dr Bendall noted that, while PIAs identify initial risks at the beginning of a project, they do not identify risks that emerge after this initial period, nor do they cover existing projects.[67] Dr Bendall stated that the OVPC would like businesses to be encouraged to conduct their own comprehensive regular privacy audits.[68]

Committee View

9.38 The Committee agrees that privacy protections are integral to mitigating the risks of cyber crime. Where personal information is well protected, the scope for identity theft and fraud is reduced.

9.39 The Committee concurs with the recommendations of the ALRC's review relating to preventing over collection. Specifically, requiring agencies and organisations to only collect necessary information would mitigate the effects of data breaches. Similarly, permitting individuals to remain anonymous where lawful and practicable would reduce the amount of information compromised in a data breach. The Committee commends the Government on its acceptance of these recommendations.

9.40 Identity crime risks would be further reduced by ensuring that private sector employee records are sufficiently protected from unauthorised access and disclosure. The removal of the small business exemption would extend protections to a wide range of personal information held by small business. In the case of small ISPs that offer additional services, the removal of the small business exemption would ensure that information that falls outside of the privacy provisions of *Telecommunications Act* is protected. The Committee encourages the Government to accept the related recommendations in the second stage of its response to the ALRC's review.

9.41 To further ensure broad privacy protections, the Committee sees value in the ALRC's recommendations aimed at encouraging the consistency of privacy legislation among Commonwealth, State and Territory jurisdictions.

---

65 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1569-1570, 1580.

66 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.86.

67 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.41.

68 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.41.

9.42 Similarly, it is important to ensure that Australian privacy laws extend to foreign agencies and organisations that handle the personal information of Australian citizens and residents. Thus the Committee endorses the ALRC's proposal to extend the *Privacy Act* to cover overseas government agencies.

9.43 The Committee accepts the OVPC's concerns relating to large overseas organisations that hold large amounts of personal information, particularly social networking sites. The Committee recommends that the OPC actively engage with overseas regulators to ensure that these organisations are aware of, and adhere to, Australian privacy laws where appropriate. Where this is not the case, the Committee encourages the OPC to use the full extent of its powers to ensure adherence, including by making, and seeking enforcement of, determinations on complaints against overseas organisations.

Recommendation 28

That the Office of the Privacy Commissioner use the full extent of its powers to ensure that overseas organisations that handle the personal information of Australian citizens and residents are aware of, and adhere to, their obligations under the *Privacy Act 1988* (Cth).

9.44 It is the view of the Committee that individuals should be notified if their personal information is compromised by a data breach. The Committee appreciates the desire of organisations to protect their reputation, however individuals must be empowered to protect themselves from identity theft and fraud. The Committee supports the ALRC's recommendation for mandatory data breach reporting, and encourages the Government to accept the recommendation. The Committee notes that mandatory data breach reporting would also permit more accurate data collection on such incidents.

9.45 Risks of cyber crime would also be reduced by the approval of a code of practice that governs privacy in the Australian Internet industry, including small operators, such as small ISPs. The Committee recognises that the removal of the small business exemption would go some way to extending the provisions of the *Privacy Act* to many currently unregulated members of the industry. However an industry specific code would ensure that the protection of personal information is given an appropriately high priority by the Australian Internet industry, an

industry that handles vast amounts of personal information. The Committee commends the IIA in drafting such a code, and encourages both the IIA and OPC to expedite the adoption of robust and accountable principles. However the effectiveness of such a code in enhancing e-security would depend on the breadth of subscription by members of the Australian Internet industry. Thus adherence to any adopted code by all members is to be encouraged.

Recommendation 29

That the Office of the Privacy Commissioner expedite the adoption of an approved privacy code of practice for members of the Australian Internet industry, including smaller Internet Service Providers.

9.46 Finally, the Committee recommends that private organisations and government agencies should be encouraged to conduct regular audits of existing processes and policies, as well as of new projects, to identify and avoid risks of unauthorised access to personal information. This is particularly important in light of the recent moves by the Government to digitise health records. The Committee recognises the OPC's efforts to encourage the use of PIAs by agencies, and praises the Government's acceptance of the ALRC's recommendations to further encourage the use of PIAs by agencies and organisations. However, the Committee also accepts the concerns of the OVPC that PIAs generally only apply to new projects and laws. Private organisations and government agencies should be required to conduct regular privacy audits of existing data systems, processes and policies, as well as of new projects. This is particularly important in light of a trend toward greater online delivery of commercial and public services. For example, to retain public confidence and minimise e-security risks, any new e-health framework will need strong privacy safeguards, including provision for regular audits of the mechanisms for handling sensitive personal health information.

Recommendation 30

That the Office of the Privacy Commissioner encourage government agencies and commercial organisations to undertake regular audits to identify risks to personal information in both new and existing projects and policies particularly projects that involve the digitisation of large amounts of sensitive information such as the new national e-Health records system.

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.

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

Supplementary Remarks — The Hon Tony Smith MP

Having only joined the Committee in February of this year, I was a participating Member for only the final public hearing in March, and consequently was not part of the extensive deliberations with over 50 witnesses at 10 days of public hearings in 2009, when the vast bulk of the evidence was taken.

As such the report's recommendations are very much a product of the considered views of Members formed during those months of hearings and deliberations of which I was not part.

Nonetheless, from my limited involvement on the Inquiry, I believe that, overall, the report is an important contribution to the debate with many sensible and practical recommendations for consideration. I do, however, have a different view on some aspects of the report, which I have outlined below.

In this short period of time, it has become very clear to me that participating Members, led by the Chair and Deputy Chair, worked very hard over many months distilling and weighing the issues. They have been ably assisted by Jerome Brown, Committee Secretary, Jane Hearn, Inquiry Secretary, and the other staff from the Committee Secretariat.

Recommendation 14

Recommendation 14 states:

> **That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to immediately elaborate a detailed e-security code of practice to be registered under the *Telecommunications Act 1997* (Cth).**
>
> **That the code of practice include:**

- **an obligation that the Internet Service Provider provides basic security advice when an account is set up to assist the end user to protect themselves from hacking and malware infections;**
- **a mandatory obligation to inform end users when their IP address has been identified as linked to an infected machine(s);**
- **a clear policy on graduated access restrictions and, if necessary, disconnection until the infected machine is remediated;**
- **the provision of basic advice and referral for technical assistance for remediation; and**
- **a requirement that acceptable use policies include contractual obligations that require a subscriber to:**
  - ⇒ **install anti-virus software and firewalls before the Internet connection is activated;**
  - ⇒ **endeavour to keep e-security software protections up to date; and**
  - ⇒ **take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.**

The substance of the recommendation and the first four stipulated items for inclusion within a proposed Code are worthy.

However, I believe the last suggested inclusion relating to subscriber contractual obligations is problematic.

Every fair minded person agrees that it is critical to take steps to ensure all internet subscribers understand the importance of, and their responsibility to secure and maintain security of, their own computer systems.

It is clear that while many Australians do take steps to ensure the security of their systems by installing and diligently maintaining security software, large numbers do not, many of whom are unaware of the dangers and potential costs to themselves and the wider community.

Continued education and awareness building at a wide range of levels is the first priority to ramping up knowledge, understanding and action.

However, to dramatically and quickly institute a requirement that ISPs contractually require the subscriber to install anti-virus software and firewalls before connecting to the internet, whilst well meaning, opens up a plethora of new liability issues for subscribers.

Such a move could only be considered in the longer term following careful consideration of the implications to subscribers in terms of their liability, and only

after comprehensive communication over a significant period of time about the implications of such a fundamental change.

Because the fundamental intent of Recommendation 14 is to register an e-security code with 'speed' ("*That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to* ***immediately*** *elaborate a detailed e-security code...*"[1]), I do not believe that this aspect of the recommendation could be implemented without creating major uncertainty and dislocation.

Recommendation 26

In my view, the approach with this recommendation is in some conflict with the approach taken in Recommendation 25, which is for the Productivity Commission to carry out a broader in depth investigation to provide more comprehensive analysis to support future policy development in this area.

It makes sense for the Productivity Commission to consider all of the issues in depth, particularly since any changes resulting from Recommendation 26 could have an impact on the broader market, and recommend on the full and appropriate suite of measures that might be considered.

Recommendations 28–30

Recommendations 28–30 are worthy.

However, I note the Committee's view that the current general exemptions to the *Privacy Act* relating to small business should be removed.

Whilst the expressed view does not translate into a recommendation, I point out that the general small business exemption has been in place as an acknowledgment of the costs that would be entailed by small business if they were brought under the Act.

1 Emphasis added.

I believe the focus should be on the adoption of codes of practice in areas where there is a clear necessity, which is precisely what Recommendation 29 envisages with respect to the Australian Internet industry, including smaller ISPs, rather than adopt a blanket approach that would place a burden on all small businesses.

Hon Tony Smith MP

Supplementary Remarks — Coalition members

We note the Majority Committee's view that the Government's planned NBN rollout could be utilised to promote education about cyber safety and the uptake of security measures.

We do not support the Government's ill conceived NBN plans.

The fact that the Government's planned NBN might be able to be utilised for other objectives does not cause us to alter our fundamental view.

Mrs Kay Hull MP

Ms Nola Marino MP

Hon Peter Lindsay MP

Hon Tony Smith MP

A

Appendix A — Submissions

1 May Justice Always Prevail

2 South Australia Police

3 Office of the Privacy Commissioner

4 Standards Australia

5 Macquarie University

6 Mr David Ready

7 Australian Bankers' Association NSW Inc

7.1 Australian Bankers' Association NSW Inc

8 Law Society of Western Australia

9 Mr Paul Myers

10 McAfee Australia

10.1 McAfee Australia

11 Office of the Privacy Commissioner NSW

12 Members Equity Bank

13 Fujitsu Australia Limited

14 Timesavers International Pty Ltd

15 NetChoice Coalition

16 Australian Bureau of Statistics

17 Australian Merchant Payments Forum

18 Yahoo! Group Australia and New Zealand

19 ThreatMetrix Pty Ltd

20 Department of Defence

21 INTERPOL

22 The Australian Information Industry Association

23 EUROPOL

24 Google Australia and New Zealand

25 Australian Federal Police

25.1 Australian Federal Police

26 CSIRO Government and International

27 Australia Post

28 RSA

29 Fortinet - Real Time Network Protection

30 AusCERT

30.1 AusCERT

31 Council of Europe

32 Symantec Asia Pacific Pte Ltd

32.1 Symantec Asia Pacific Pte Ltd

33 Office of the Victorian Privacy Commissioner

34 Department of Broadband, Communications and the Digital Economy

35 Microsoft Australia Pty Ltd

36 Lockstep Consulting Pty Ltd

37 Mr Alastair MacGibbon

38 Australian Computer Society Inc

39 e-Bay Inc.

40 The Internet Corporation for Assigned Names and Numbers

41 Australian Institute of Criminology

42 Australian Council of State School Organisations

43 Telstra

43.1 Telstra

44 Attorney-General's Department

44.1 Attorney-General's Department

45 Internet Society of Australia

46 Australian Competition and Consumer Commission

47 Australian Security Intelligence Organisation

48 Government of Western Australia Department of Commerce

49 NSW Government

50 Australian Payments Clearing Association

51 Tasmanian Government

52 Australian Securities and Investment Commission

53 Northern Territory Government

54 Internet Industry Association

54.1 Internet Industry Association

55 Abacus - Australian Mutuals

56 Australian Communications and Media Authority

56.1 Australian Communications and Media Authority

56.2 CONFIDENTIAL

57 Australian Communications Consumers Action Network

57.1 Australian Communications Consumers Action Network

58 CONFIDENTIAL

59 Australian Taxation Office

59.1 Australian Taxation Office

60 PayPal

61 Dr Peiyuan Zhu

62 Cyberspace Law and Policy Centre

62.1 Cyberspace Law and Policy Centre

63 Australian Seniors Computer Clubs Association

63.1 Australian Seniors Computer Clubs Association

64 ROAR Film Pty Ltd

65 CONFIDENTIAL

66 Sophos Pty Ltd

67 Queensland Government

68 Web Management InterActive Technologies Pty Ltd

68.1 Web Management InterActive Technologies Pty Ltd

68.2 Web Management InterActive Technologies Pty Ltd

68.3 Web Management InterActive Technologies Pty Ltd

68.4 Web Management InterActive Technologies Pty Ltd

B

Appendix B — Exhibits

1 The Australian Information Industry Association
Convention on Cybercrime (Related to Submission No. 22)

2 RSA
RSA Special Online Fraud Report: What to Expect in 2009 and Beyond (Related to Submission No. 28)

3 RSA
RSA Online Fraud Report (Related to Submission No. 28)

4 Council of Europe
Convention on Cybercrime (Related to Submission No. 31)

5 Australian Institute of Criminology
Inquiry into Cyber Crime 2009 (Related to Submission No. 41)

6 Internet Safety Institute
The drivers for online crime (Related to Submission No. 37)

7 Microsoft Australia
Establishing End to End Trust (Related to Submission No. 35)

8 ROAR Film Pty Ltd
ROAR - Cyber Risk Education (Related to Submission No. 64)

9 Australian Communications Consumers Action Network
Informed Consent (Related to Submission No. 57)

10 Australian Communications Consumers Action Network
Customer Service (Related to Submission No. 57)

11 Australian Communications Consumers Action Network
Future Consumer (Related to Submission No. 57)

12 AusCERT
The Need for Customer-Centric Signalling in the Software Market
(Related to Submission No. 30)

13 AusCERT
Internet Industry Code of Practice (Related to Submission No. 30)

14 McAfee Australia
Cloud Computing: Risks and Rewards (Related to Submission No. 10)

15 Internet Industry Association
An Important Security Notice from the Internet Industry Association (IIA)
(Related to Submission No. 54)

16 Australian Competition and Consumer Commission
The little black book of scams (Related to Submission No. 46)

17 Australian Competition and Consumer Commission
SCAM watch (Related to Submission No. 46)

18 Australian Competition and Consumer Commission
Money transfer scams (Related to Submission No. 46)

19 Australian Competition and Consumer Commission
Sports 'investment' scams (Related to Submission No. 46)

20 Australian Competition and Consumer Commission
Phishing scams (Related to Submission No. 46)

21 Australian Competition and Consumer Commission
Lotteries, sweepstakes and competition scams (Related to Submission No. 46)

22 Australian Competition and Consumer Commission
SCAM watch (Related to Submission No. 46)

23 AusCERT
German ISPs team up with Government agency to clean up malware (Related to Submission No. 30)

C

Appendix C — Witnesses

Wednesday, 19 August 2009 - Canberra

Australian Institute of Criminology

Dr Judy Putt, General Manager, Research

Dr Russell Smith, Principal Criminologist

Wednesday, 9 September 2009 - Canberra

Australian Federal Police

Dr Jenny Cartwright, Coordinator Crime Prevention

Commander Neil Gaughan, National Manager, High Tech Crime Operations

Friday, 11 September 2009 - Canberra

AusCERT

Mr Graham Ingram, General Manager

Australian Payments Clearing Association Ltd

Mr Chris Hamilton, Chief Executive Officer

Ms Caroline Pearce, Head of Fraud, Risk and Compliance

Fujitsu Australia Limited

Mr Michael Sinkowitsch, Business Development Manager

Internet Industry Association

Mr Peter Coroneos, Chief Executive

Internet Safety Institute

Mr Alastair MacGibbon

Telstra

Mr Glenn Chisholm, General Manager, Network Security

Mr Darren Kane, Director, Corporate Security and investigations

Mr James Shaw, Director, Government Relations

The Australian Information Industry Association

Ms Loretta Johnson, General Manager, Policy and Government Relations

Wednesday, 16 September 2009 - Canberra

Australian Taxation Office

Mr Michael Cranston, Deputy Commissioner, Serious Non-Compliance

Mr Bill Gibson, Chief Information Officer

Ms Bettina Konti, Acting First Assistant Commissioner, Business Solutions, Enterprise Solutions and Technology

Thursday, 8 October 2009 - Sydney

Australian Bankers' Association NSW Inc

Mr Tony Burke, Director

Australian Communications Consumers Action Network

Mr Allan Asher, Chief Executive Officer

Commonwealth Bank of Australia

Mr John Geurts, Executive General Manager Group Security

Cyberspace Law & Policy Centre (CLPC)

Ms Alana Maurushat, Deputy Director, Cyberspace Law and Policy Centre, UNSW

Department of Justice and Attorney General NSW

Ms Penelope Musgrave, Director, Criminal Law Review

Office of the Victorian Privacy Commissioner

Dr Anthony Bendall, Deputy Privacy Commissioner

ROAR Film Pty Ltd

Mr Terry Hilsberg, Executive Director, Strategy

State Crime Command, NSW Police Force

Mr William van der Graaf, Detective Inspector - Co-Ordinator, Computer Crime Team, Fraud Squad

The Internet Corporation for Assigned Names and Numbers (ICANN)

Mr Paul Twomey, Senior President

Westpac Banking Corporation

Mr Richard Johnson, Chief Information Security Officer

Friday, 9 October 2009 - Sydney

Australian Computer Society

Mr Alastair MacGibbon, Member, Filtering & eSecurity Taskforce

Prof. Vijay Varadharajan, Chair of National E-Security Taskforce

Internet Society of Australia (ISOC-AU)

Dr Paul Brooks, Director

Ms Holly Raiche, Executive Director

Lockstep Consulting Pty Ltd

Mr Stephen Wilson, Managing Director

McAfee Australia

Mr Andrew Littleproud, Regional Director Australia and New Zealand

Mr Sean Duca, Technical Solutions Manager, Australia and New Zealand

Microsoft Australia Pty Ltd

Mr John Galligan, Director of Corporate Affairs

Mr Stuart Strathdee, Security Program Manager

Mr Peter Watson, Manager of Platform Strategy

Symantec Corporation

Mr Craig Scroggie, Vice President Asia Pacific

Wednesday, 21 October 2009 - Canberra

Australian Communications and Media Authority VIC

Mr Bruce Matthews, Acting Executive Manager, Strategy and Coordination Branch

Mr David Zielezna, Senior IT Technical Officer, E-security and DCNR Section

Wednesday, 28 October 2009 - Canberra

Australian Seniors Computer Clubs Association

Mrs Nan Bosler, President

Wednesday, 18 November 2009 - Canberra

Australian Competition and Consumer Commission

Mr Scott Gregson, Group General Manager, Enforcement Operations

Mr Nigel Ridgway, Group General Manager, Compliance, Research, Outreach and Product Safety

Wednesday, 25 November 2009 - Canberra

Attorney-General's Department

Mr Sarah Chidgey, Assistant Secretary, Criminal Law and Law Enforcement Branch

Ms Sheridan Evans, Assistant Secretary, Identity Security Branch

Ms Marcella Hawkes, Acting Assistant Secretary, E-Security Policy and Coordination, National Security Resilience Policy Division

Ms Susan Mihalic, Principal Legal Officer, Telecommunications and Surveillance Law Branch

Mr Mike Rothery, First Assistant Secretary, National Security Resilience Policy Division

Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Department of Broadband, Communications and the Digital Economy

Mr Simon Cordina, Assistant Secretary, Cyber-Safety and Trade Branch

Ms Sabeena Oberoi, Assistant Secretary, E-security and APEC Branch

Mr Keith Besgrove, First Assistant Secretary, Telecommunications, Networks Regulation and Australia Post, Digital Economy Services Division

Wednesday, 17 March 2010 - Canberra

Queensland Police Service

Mr Brian Hay, Detective Superintendent, Fraud and Corporate Crime Group, State Crime Operations Command

D

Appendix D — Commonwealth Computer Offences

The following offences are contained in the Commonwealth Criminal Code.

Hacking, malware and denial of service attacks with intent to commit a serious offence - Subsections 477.1(1) and (4)

Knowingly causing unauthorised access to or modification of data held in a computer or unauthorised impairment of an electronic communication to or from a computer with *intent to commit a serious offence*.[1]

The offence applies where the primary offence, for example of fraud or terrorism, carries a penalty of five years or more or life imprisonment.[2]

The penalty cannot exceed the penalty applicable to the primary offence.

Malware infections - Section 477.2

Knowingly causing an unauthorised modification of data with reckless disregard as to whether the modification impairs or will impair access to, or the reliability, security or operation of other data.

The offence applies to, for example, the use of the Internet to infect a computer with malware (e.g. key loggers, Trojans, viruses, worms).

Penalty: 10 years imprisonment.

---

1 The offence set out in subsection 477.1 (1) applies where conduct is caused by means of a carriage service and involves an intention to commit or facilitate a serious offence under Commonwealth, State or Territory law. Subsection 477.1(4) does not require the use of the Internet and is limited to the intention to commit or facilitate a crime under Commonwealth law.

2 Subsection 477.2(9) of the Criminal Code.

Denial of Service Attacks - Section 477.3

Knowingly causing unauthorised impairment of electronic communication to or from a computer involving either (i) the use of a carriage service; or (ii) a Commonwealth computer.

This offence covers cyber attacks, such as denial of service attacks, where a server is inundated with a large volume of emails.

Penalty: 10 years imprisonment.

Hacking password protected data - Section 478.1

Knowingly and intentionally causes unauthorised access to or modification of restricted data. This offence applies where the restricted data is held in a Commonwealth computer or held on behalf of the Commonwealth. It also applies where the conduct is carried out by the means of a carriage service.

This is intended to cover conduct such as hacking into password protected data held by or for the Commonwealth.

Penalty: maximum two years imprisonment.

Damaging data held on a mobile device owned or leased by the Commonwealth - Section 478.2

Knowingly and intentionally causing any unauthorised impairment of the reliability, security or operation of data held on a computer disk, or credit card or other device used to store data by electronic means that is owned or leased by a Commonwealth entity.

This offence includes, for example, damaging a computer disc or credit card by passing a magnet over a credit card.

Penalty: maximum two years imprisonment.

Possession or control of data – Section 478.3

The possession or control of data with intent to commit a computer offence.

This offence is intended to cover the possession of a program or a root-kit that enables a person to hack into another person's computer system, impair data via a malware infection or impair electronic communications via a DDOS attack.

Penalty: maximum three years imprisonment.

Production and supply of data – Section 478.4

Producing, supplying or obtaining data with intent to commit a computer offence.

This offence is intended to cover the production and/or supply of data to be used in a computer offence.[3]

Penalty: maximum three years imprisonment.

3 AGD, *Submission* 44, p.19.

E

Appendix E — Proposed Commonwealth Identity Fraud Offences

The following proposed offences will be inserted into Commonwealth Criminal Code.[1]

Dealing with identification information - Proposed new subsection 372.1

It is an offence to deal (make, supply or use) identification information with the intention that any person will use that information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of committing or facilitating the commission of an indictable offence.

Penalty: maximum five years imprisonment.

Possession of identification information - Proposed new subsection 372.2

It is an offence to possess identification information with the intention that any person will deal (make, supply or use) in the information to commit an indictable offence.

Penalty: maximum 3 years imprisonment.

Possession of equipment used to make identification documentation - Proposed new subsection 372.3

It is an offence to possess equipment with the intention that any person will use the equipment to make identification documentation to engage in conduct prohibited by subsection 372.1.

Penalty: maximum 3 years imprisonment.

---

1 AGD, *Supplementary Submission 44.1*, p.3.