Australian Government

Department of Broadband,
Communications and the Digital Economy

icode Review

Report

Review of the Internet Service Providers voluntary code of practice for industry self-regulation in the area of cybersecurity

April 2013

Contents

Executive Summary

The purpose of this report is to provide outcomes of the first review by the Australian Government of the icode - the *Internet Service Providers (ISP) Voluntary Code of Practice for Industry Self-Regulation in the Area of Cyber Security*. The icode, which came into effect in December 2010, was developed by the Internet Industry Association (IIA) in partnership with the Australian Government to provide Australian ISPs with a consistent approach to help educate, inform and assist users with cyber security issues.

The review consulted extensively with ISPs, consumer groups and other relevant stakeholders. It was informed by surveys of ISPs and their customers commissioned by the Department of Broadband, Communications and the Digital Economy (the Department), an omnibus survey and the results from surveys previously commissioned by the Department. In addition, the review drew upon studies by the Organisation for Economic Cooperation and Development (OECD) and by the Australian Communications and Media Authority (ACMA) among others, and the preliminary findings of the IIA's own examination of the icode.

Overall, the review finds that the icode is operating largely as intended. That said, the review considers there is room for improvement and has made nine recommendations to strengthen the code. The following is a summary of recommendations, which are discussed in detail later in the report.

Recommendation 1

That:

i) *clear objectives be established for each of the headings listed under **Section 6** "recommended actions for ISPs"*
ii) ***Section 6** be revised to clearly articulate that for ISPs to be compliant they must choose actions from the "recommended actions for ISPs"*
iii) ***Section 9** be revised to include clear reporting requirements and defined timeframes.*

Recommendation 2

*Revise **Section 9** to require ISPs to provide quantitative data to better gauge the effectiveness of the icode and its impact on the overall cyber security environment in Australia.*

Recommendation 3

That:

i) *a working group be established to oversee implementation of the review recommendations, and to provide an avenue for improved communication between*

ISPs, government, consumer groups and other industry stakeholders. The working group would comprise representatives from industry, consumer groups and government, and will be co-chaired by the IIA and the Department of Broadband, Communications and the Digital Economy

ii) *the icode be reviewed on a regular basis (for example every 18 months). This review would be conducted by the working group*

Recommendation 4

That the voluntary nature of the icode be retained for now and that this be reassessed by the working group at the next review of the icode, or through its ongoing monitoring.

Recommendation 5

That measures be taken to:

i) *revise the icode to provide better guidance to ISPs so they enhance efforts to educate their customers. Such guidance could include information on the content of messages to customers, how messages are provided, and when messages are provided (for example: at account creation, periodically or driven by events)*

ii) *as far as possible, ensure consistency of cyber security messages between government and ISPs*

iii) *revise and update the cyber security educational and awareness raising material to be distributed to consumers under **Schedule 1** of the icode*

iv) *in addition to providing educational material to customers, encourage ISPs to refer customers to free government online resources such as the Stay Smart Online website and Stay Smart Online Alert Service for more detailed and up to date information on cyber security issues including software vulnerabilities and scams, and how they can be addressed*.

Recommendation 6

That measures be taken to:

i) *work with application platform providers to develop appropriate mechanisms to communicate to users about application vulnerabilities and how they can be addressed*

ii) *ensure that providers' education and awareness raising activities focus on making users aware of the potential risks associated with the use of mobile devices and other internet connected devices, in particular home devices. This should include providing users with information on measures they could take to protect these devices from online threats, noting that some measures may be more specific to certain types of devices*

iii) *broaden the icode to remain technology neutral so it can be flexible enough to cover current and future changes – including updating the icode to refer to 'compromised devices' rather than 'compromised computers'.*

Recommendation 7

That the icode be revised to specify:

i) *clear triggers for when ISPs should contact their customers once a compromised device is identified*
ii) *a reasonable time within which ISPs are required to take action in response to the detection of a compromised device on a network*
iii) *that ISPs are to establish a system to identity and provide more directed assistance to those customers who remain compromised or are repeatedly compromised*
iv) *the continuation of a flexible approach in how ISPs contact and assist customers so that it meets their operational and resource requirements, noting that such an approach must be effective in assisting customers*
v) *appropriate strategies for follow-up by ISPs of customers with compromised devices.*

Recommendation 8

That:

i) *CERT Australia work with industry to introduce mechanisms, such as an incident matrix, to assist ISPs identify what constitutes a 'significant cyber security incident' for reporting purposes*
ii) *government work with ISPs to facilitate information flow when cyber security incidents are reported.*

Recommendation 9

That:

i) *the term 'internet service provider' be clarified to include mobile internet service providers*
ii) *strategies be developed to promote the icode with ISPs, with a view to increasing the number of signatories*
iii) *strategies be developed to promote the icode Trustmark to raise consumer awareness about the icode.*

Background

The icode

The icode was a key outcome of the Australian Government's 2008 E-security Review into its cyber security policies, programs and capabilities. One of the findings of the review was the need for greater engagement by ISPs on cyber security. The review recognised that ISPs are in a unique position to assist in educating, informing, influencing and protecting Australian online users. It found that, as the owners and operators of networks, ISPs are well placed to understand and act on cyber security threats. The review recommended that the government work with ISPs to develop a code of practice, setting out minimum expectations of ISPs to contribute to cyber security for all users.

The icode was developed through a partnership between the IIA and the Australian Government. A range of stakeholders were consulted during its development, including consumer organisations and software providers.

The icode was established as a voluntary scheme to strike a balance between encouraging take-up by industry and helping to improve the cyber security environment for all Australians. During its development, industry argued that self-regulation was less onerous on ISPs and more likely to be responsive to changes in the rapidly changing cyber security environment. It was also recognised that the flexibility provided by a voluntary scheme would be particularly helpful for smaller ISPs that may not have the resources available to comply with a more prescriptive path. The icode came into effect in December 2010. Currently, there are 34 ISP signatories to the icode, representing approximately 90% of Australian home internet users[1].

A key component of the icode is the Australian Internet Security Initiative (AISI), a voluntary initiative managed by the ACMA. The AISI collects data from various sources on computers exhibiting 'bot'[2] behaviour on Australian networks. Using this data, the ACMA provides daily reports to ISPs identifying compromised IP addresses on their networks with a view that the ISPs inform the relevant customers about the compromise and assist them to address the

[1] A list of icode members is at **Appendix 1.**

[2] A 'bot' is an internet connected device which has been compromised by malware. 'Botnets' are a collection of infected computers, which can be controlled remotely by a third party. Botnets are used by criminals to send spam email messages, launch distributed denial of service attacks and steal personal and financial data, among other harmful activities. Aside from the potential damage such activity can cause to individuals, botnets also represent a threat to government and industry networks: for example, denial of service attacks can compromise the delivery of essential services such as communications, energy, finance and transport.

problem. There are 132 members of the AISI, including universities, of which 30 are also icode signatories.

The icode's scope is reflected in its four key objectives: Education, Detection, Action and Reporting. This breadth of scope is clearly articulated in **Section 3** of the code, which states that the icode aims to:

a) Instil a culture of cyber security within Australian ISPs and their customers

b) Provide consistent messaging and plain language information to customers that:

   (i) raises awareness and educates them about cyber security risks
   (ii) sets out simple steps that they can take to better protect themselves online
   (iii) assists those customers whose computer has been identified as possibly compromised by providing them with steps they should take to rectify the situation

c) Assist customers who experience repeated compromises to their computers and develop a strategy to minimise the effect of such compromises to other customers on the ISP's network as well as customers on other ISPs' networks.

d) Encourage ISPs to identify compromised computers on their networks by:

   (i) participating in the ACMA's AISI
   (ii) actively managing their networks
   (iii) obtaining information on compromised computers via other trusted third party sources

e) Develop mechanisms for ISPs to share information and collaborate about cyber security compromises and developments affecting other Australian ISPs

f) Encourage ISPs to identify and report any cyber security issue that may affect Australia's critical infrastructure or that may have a national security dimension

g) Implement these measures in a manner that protects the privacy of customers, consistent with relevant legislative obligations.

Review

As a voluntary code of practice the icode provides a set of guidelines for ISPs to help, educate and inform their customers about cyber security issues. It is one of the first attempts, either domestically or internationally, to codify best practice procedures for ISPs in relation to compromised computers on the internet and to encourage a cyber security consciousness amongst ISPs and their customers.

During its development, it was recognised that the icode would need to be improved and adapted over time in response to the constantly changing cyber security environment. This is reflected in the code itself. **Section 4.5** states that 'the cyber security measures listed in this Code are not exhaustive or exclusive [and] it is envisaged that these measures will change over time.' In addition to this, **Section 10** provides for a review of the code to be

carried out by the IIA within 18 months of implementation. **Section 10.2** of the icode stipulates that the review is to be carried out in consultation with government.

The IIA announced its intention to undertake a review on 3 April 2012 with the stated aim of 'ensuring the icode continues as an effective voluntary code, embraced by ISPs and of improving the icode so that it meets current Internet safety challenges.'[3]

In its response to the House of Representatives Standing Committee on Communications report on the inquiry into cyber crime *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* released in April 2010, the Australian Government stated that it would 'closely monitor the ISP Code and [would] review its effectiveness.' [4]

The Government review has been broader than the IIA review considering issues beyond how effective the icode has been in meeting its objectives. These include:

- whether the current voluntary self-regulatory approach is an effective mechanism for encouraging ISPs to assist their customers with cyber security issues
- whether alternatives to the current approach might be more effective
- what the most appropriate roles are for ISPs and their customers in addressing the problem
- whether the icode has effectively contributed to reducing the problem of compromised computers in Australia
- the level of awareness about and influence of the icode among the broader ISP industry and the general community
- the level of assistance provided by ISPs – whether icode signatories or otherwise – to their customers
- the level of information sharing among ISPs – whether icode signatories or otherwise – with relevant authorities such as CERT Australia and the Australian Federal Police (AFP).

The terms of reference for the review are at **Appendix 2.**

The review was led by the Department with support from the following government agencies:

Australian Communications and Media Authority
Attorney-General's Department (CERT Australia)
Department of the Prime Minister and Cabinet
Australian Federal Police
Defence Signals Directorate.

[3] IIA News Release *Online Industry weapon against Cybercrime under review* 3 April 2012
[4] Government response to Cyber Crime Inquiry, http://www.dbcde.gov.au/__data/assets/pdf_file/0005/131468/Government_Response_to_the_House_of_Representatives_Parliamentary_Committee_Report_on_Cyber_Crime.pdf, p. 17

Research

The Department commissioned research and also drew on existing research to inform the review.

Two surveys were commissioned for the review: one of ISPs and the other of their customers. The ISP survey included ISPs that are signatories and non-signatories of the icode. These surveys were conducted by independent consultants Colmar Brunton.

The Department also included questions in an omnibus survey conducted by Ipsos.

ISP and ISP customer surveys - Colmar Brunton

The ISP survey sought to gain a better understanding of a range of issues, including:

- ISP perceptions of the icode (both signatories and non-signatories)
- the measures ISPs take to detect infected computers on their network
- the steps ISPs take when infected computers are detected
- the level of information ISPs provide to customers whose home computers are infected
- whether customers find this information helpful in remedying the infection.

All 34 icode signatories were approached to complete the survey, along with 10 non-signatories. Responses were received from 12 ISPs, including 10 icode signatories and two non-signatories.

Many of the ISPS did not respond to the survey because they felt that they had already provided input into the review process through roundtable and bilateral discussions and the IIA forum held in June 2012. The ISPs who responded to the survey tended to be those which did not participate in the consultations. The information provided through the ISP survey reinforced the messages received from other research conducted by the review and the consultations undertaken with ISPs. Overall, a good response to the review was received from industry. The survey aimed to explore customer issues such as:

- awareness of the icode
- attitudes towards the icode, including the expectations of customers in relation to ISPs notifying them if their computer is infected
- the experiences of customers who have been contacted by their ISPs in relation to a malware infection.

Ipsos Omnibus Survey

The omnibus survey sought to gain an insight into the percentage of Australians who have been contacted by their ISP about a compromised computer, and of those, what percentage were provided with assistance to resolve the problem.

The survey was conducted nationally, comprising 1046 internet users.

Other research

Other research informed the review, including:

- An international literature search of other botnet mitigation initiatives including in Germany, Japan, Korea, the Netherlands, the United Kingdom, the United States, New Zealand, South Africa, Ireland and Singapore.
- OECD research, including: *The role of internet service providers in botnet mitigation: an empirical analysis based on spam data*, 12 November 2010; *Proactive policy measures by internet service providers against botnets*, 12 March 2012; and *Alternatives to traditional regulation*, 2009.
- ACMA research including: *The Australian Internet Security Initiative – provider responses to security-compromised computers*, June 2012; *An overview of international cyber security awareness raising and educational initiatives*, May 2011; and *Optimal conditions for effective self- and co-regulatory arrangements – Occasional Paper*, September 2011.
- Previously commissioned cyber security research by the Department including the cyber security Baseline and Tracking surveys undertaken by Woolcott Research in 2010 and 2011, and *Segmentation Research into Australian Internet Users* by Quantum Market Research, June 2011.

Consultation

Consultation with industry and consumer groups was a key component of the review and occurred primarily through two roundtables held in Sydney on 31 May and 25 July 2012. Attendees included a number of major and smaller ISPs, a non-icode signatory ISP, the Australian Communications Consumer Action Network (ACCAN) and the Internet Society of Australia (ISOC-au), academics, IIA icode Review Taskforce members, the ACMA, the Telecommunications Industry Ombudsman (TIO) and members of the review's Steering Group.

Besides consultation through the roundtables, ongoing consultation with the IIA and other relevant stakeholders occurred throughout the review process. Steering Group members participated in the icode review forum hosted by the IIA on 14 June 2012. In addition, the IIA provided the Department with the initial feedback it had received from participating ISPs in April-May 2012.

Review findings

Overall, the review found that the icode appears to have engendered some level of awareness within the ISP community about their role in assisting Australian internet users to address cyber security issues. The review recognised that cyberspace is evolving with the

convergence of devices, and threats which are highly targeted and sophisticated. The ability to precisely measure the extent to which the icode has been successful in meeting its objectives is somewhat limited due to the absence of established metrics. However, broad consultations with ISPs, surveys conducted and other research undertaken during the course of the review indicate that ISPs generally value the icode and have implemented a number of measures to be 'icode compliant'. Our research also indicates that customers rely on the advice of their ISPs for cyber security matters and expect their ISP to inform them in a timely manner when there is a problem and to help the internet user address the problem.

There is a strong interest from ISPs and other stakeholders to strengthen the icode both in terms of what it can do and also how it is enforced by the IIA. As noted above when the icode was established it was considered a first step in the right direction and it was recognised that more could be done. The review has provided this opportunity to better meet the expectations of ISPs, their customers and other stakeholders.

Below are the key findings of the review and its recommendations.

Compliance

The decision to become an icode signatory is a voluntary one. In choosing to sign up to the icode ISPs agree to undertake certain actions in order to demonstrate ongoing compliance. These actions are detailed in **Section 6** and are divided into four broad headings: Education, Detection, Action and Reporting. To be considered icode compliant, ISPs are required to undertake at least one of the items listed under each of these headings.

The reporting provisions under **Section 9.2** are intended to allow the IIA to monitor this compliance. ISPs are required to periodically submit to the IIA, or publish on their own website, details of the actions they have taken to demonstrate their compliance with the icode. During the roundtables, ISPs told the review that this is not occurring, which suggests a lack of enforcement of compliance by the IIA. The absence of such reporting makes it difficult for the review to gauge the extent with which ISPs are compliant with the code. In saying this, our research indicates that most ISPs are in fact taking some steps to comply with icode requirements.

According to the Colmar Brunton survey, 'detection' appears to have the highest level of compliance[5]. All ISPs surveyed indicated that they perform at least one of the actions required to be compliant under 'detection', with most performing multiple actions. This is not unexpected, as ISPs will want to be aware of compromises on their networks. An ISP need only subscribe to the free AISI reports provided by the ACMA to be considered compliant under this heading. All survey respondents subscribe to the AISI reports, which

[5] Colmar Brunton, *icode review - ISP Stakeholders Survey*, p 28

were considered 'very useful' by most ISPs. Third party resources were also widely used, as were in-house network detection methods.

Most ISPs who participated in the survey also appear to be taking action when they become aware of a compromised computer on their network. The most common action taken is to contact the customer by email, telephone or SMS to make them aware of the compromise. All but one of the ISPs who responded to the survey reported contacting customers, with the most common means of doing so by email (66%) or telephone (10%). About half of responding ISPs reported using both means to contact customers. This is significant in that a key risk identified regarding notifications was the need for users to be able to readily verify that the contact is legitimate (as opposed to another potential source of malware infection).

As for education, almost all responding ISPs reported that they provide new and existing customers with information on how they can protect themselves from cyber security risks. Information is predominantly provided via email, newsletter and/or on the ISP's website. This reflects the importance that ISPs place on the provision of educational material: the large majority of ISPs surveyed think it is 'moderately' or 'very important' to educate their customers on how to better protect themselves from cyber security risks. The ISPs who rated education as 'neither important nor unimportant' believed customers should ultimately be responsible for their own online security, with ISPs providing support.

Specifically, the review recommends that the IIA introduce clear reporting requirements with set timeframes that state when ISPs are required to report. Further, the review recommends that the language under **Section 6** be strengthened to better reflect that ISPs must choose an action or set of actions from the list of 'recommended actions for ISPs' in this section to be considered compliant.

In order to ensure compliance, the review considers that it would be beneficial if each broad heading – education, detection, action and reporting – also contained the overarching objective that is to be achieved under that heading. This may assist ISPs in choosing which actions to take. For example, the overarching objective for Education could be to 'provide Australian internet users with the confidence and knowledge they need to protect their personal and financial information online.'

Recommendation 1

That:

i) *clear objectives be established for each of the headings listed under **Section 6** "recommended actions for ISPs"*
ii) ***Section 6** be revised to clearly articulate that for ISPs to be compliant they must choose actions from the "recommended actions for ISPs"*
iii) ***Section 9** be revised to include clear reporting requirements and defined timeframes.*

Metrics

Section 9.2 of the icode seeks information on the actions that ISPs take to comply with it. However, it does not require ISPs to provide quantitative data such as the number of compromises identified on an ISP network, the number of customers contacted, the response rate of customers to ISP notifications or the time taken to resolve a compromised computer.

One of the challenges faced by the review was obtaining quantitative data from ISPs which is critical to determining the extent of the icode's success. While the results of surveys commissioned by the review and other anecdotal evidence suggest that the icode is, to a degree, fulfilling its objectives, there is little hard data available from ISPs to confirm this view.

The only clear quantitative data available to the review is the number of ISPs that have signed up to the code. Currently 34 ISPs have signed up, covering around 90% of Australian internet users. This coverage rate compares favourably with analogous international initiatives. The Netherlands has seen a similar result with its private-sector led scheme, which represents over 90% of the local internet market. Meanwhile, when it was announced in March 2012, the US Anti-Bot Code of Conduct was expected to cover 51% of US households with broadband connections.[6]

Some ISPs have argued that the significant international interest in the icode is a sign of its success.[7] In 2010, former deputy director and chief information officer of the US National Security Agency, Dr Prescott Winter, praised the icode and saw its implementation as a sign that Australia was in a position to lead cyber security collaboration on combating malware globally.[8] As already noted, in March 2012 the United State ISPs announced a voluntary Anti-Bot Code of Conduct for ISPs, known as the ABCs for ISPs. A number of other countries including the United Kingdom, Singapore, South Africa, India and New Zealand have either adopted or are considering adopting similar approaches to the icode.

The review considers that to enhance compliance, ISPs should be required to provide metrics, such as those outlined above. This will help to determine the extent to which the steps taken by ISPs and consumers are contributing to alleviating the problem of compromised computers, and also help to establish an overall picture of the cyber security environment. While not prescribing specific actions to be taken, the review considers that a combination of different measures would be appropriate.

---

[6] OTA, *US anti-botnet code of conduct for ISPs unveiled,* 29 March 2012, http://www.otalliance.org/news/releases/ABCsISPs.html

[7] For more discussion on similar and related international initiatives refer to **Appendix 3** of this report

[8] James Hutchinson, *ComputerWorld*, 6 October 2010

Recommendation 2

*Revise **Section 9** to require ISPs to provide quantitative data to better gauge the effectiveness of the icode and its impact on the overall cyber security environment in Australia.*

Implementing change

In order for the icode to continue to help Australian internet users be better protected online, it needs to keep pace with the changes that occur in the cyber security environment. As an industry code, responsibility for its management – including updates, membership, compliance and review – lies with the peak industry body, the IIA.

Section 10 of the code provides for a one-off review by the IIA within 18 months of implementation. The present review does not, however, consider this sufficient to ensure the currency and effectiveness of the code into the future. The cyber security environment is dynamic, with both the technology used and the threats that are present in an ongoing state of flux. For instance, the use of converged devices such as smartphones is increasing, bringing new challenges for internet users and new opportunities for criminals to exploit the online environment. Online attacks, too, are becoming increasingly targeted and sophisticated.

This is likely to remain true in the coming years as different risks and technologies emerge. The review therefore recommends that the icode be appraised on a periodic basis to ensure that it remains effective. Such a review should be carried out collaboratively by the Department, the ACMA and other government agencies as appropriate, and be conducted, as a guide, every 18 months.

The review also considers that there is a need for a body to monitor the ongoing operation of the icode and provide oversight as required. The review therefore recommends that, at the conclusion of this review, an icode working group be established. The initial task of the working group would be to oversee implementation of recommendations from the IIA and government reviews, with an ongoing role to monitor and suggest improvements to the code as required.

The working group should comprise representatives from the IIA, member and non-IIA member ISPs, consumer groups and government to ensure that it takes into account the views and needs of stakeholders. It is recommended that the group be co-chaired by the Department and the IIA, with secretariat support provided by the Department. It is anticipated that the group would, initially, meet regularly to oversee the implementation of review recommendations. This frequency would be expected to reduce over time.

As well as providing oversight, the proposed working group would also help to address a number of other issues identified during the review, including the need for improved communications, both between ISPs and between ISPs and government, and the adoption

of a coordinated approach to cyber security awareness messaging. **Section 7** of the icode recommends that ISPs actively share cyber security information with each other, with CERT Australia facilitating this information exchange process. This does not appear to be taking place to the extent envisaged when the icode was drafted.

ISPs have expressed an interest in better communication with other ISPs and government on cyber security issues. When asked how to improve the icode, one ISP suggested better options for providing feedback. Another suggested that regular discussions between government and ISPs on issues of relevance would be beneficial. Government, too, sees value in having a formal avenue for regular communication with industry participants. A related issue raised during the review consultations was how icode participants can better communicate with relevant industry sectors that have a stake or interest in cyber security, such as hardware vendors, app developers and internet based companies.

The proposed working group would provide a platform for ongoing communication between the government, ISPs and other relevant stakeholders.

Recommendation 3

That:

i) a working group be established to oversee implementation of the review recommendations, and to provide an avenue for improved communication between ISPs, government, consumer groups and other industry stakeholders. The working group would comprise representatives from industry, consumer groups and government, and will be co-chaired by the IIA and the Department of Broadband, Communications and the Digital Economy

ii) the icode be reviewed on a regular basis (for example every 18 months). This review would be conducted by the working group

Voluntary or Mandatory

One of the key issues considered by the review was the icode's self-regulatory nature. Consideration of whether a voluntary or mandatory approach is more appropriate has been an issue since the icode was first conceived. In its June 2010 report of the Inquiry into Cyber Crime, the House of Representatives Standing Committee on Communications expressed its preference for a mandatory code, arguing that a registered code would be 'consistent with existing law and policy and ensure a greater consistency across the industry.' The Committee also noted that registration by the ACMA would give it the authority to 'make an order if it was necessary to do so as a measure of last resort,' thereby improving compliance with the code.

An opposing view put forward by the IIA was that a voluntary code is preferable due to its flexibility, ease of compliance and the lack of burden it places on ISPs. A key consideration at the time the icode was developed was the resource burden a mandatory code might place

particularly on smaller ISPs. A voluntary approach was therefore considered more likely to garner industry support.

The costs for ISPs associated with implementing the icode are an important consideration due to the potential resourcing disparities between small and large ISPs. The principles of the code listed under **Section 5** state that it should be 'fair to all concerned' and 'should not adversely affect the commercial viability of the parties and the services they make available'.

ISPs have indicated that from their perspective the strength of the icode is that it is not overly prescriptive and allows ISPs the flexibility to respond to compromises in a way that suits both their business needs and the nature of the compromise.[9] In the survey commissioned by the Department, ISPs that rated the icode as operating 'very well' said it provided good flexibility by setting a baseline standard for the sector that was adaptable to both large and small providers.[10]

This flexibility is highlighted, for example, by the different approaches taken by ISPs to address compromised computers. According to the Colmar Brunton survey, ISPs choose to contact customers by telephone, through email, or via SMS, depending on their operational requirements or the circumstances of the compromise. ISPs may also apply restrictions to outbound mail (in the case of spam), temporarily quarantine the customer's service, regenerate the customer's password to prompt the customer to contact the service desk or throttle the customer's internet speed.

ISPs have indicated that a mandated approach would make it challenging for many smaller ISPs to comply.[11] As noted above, resource implications and a lack of flexibility to respond to the changing cyber security environment are two arguments put forward by ISPs against a mandated approach. That said, ACMA research suggests some smaller ISPs have been responding more actively to notifications than some large ISPs.[12]

Although it is not surprising that industry has strong views about the icode remaining a voluntary scheme, internationally there are few, if any, examples of strict, top-down government regulatory schemes covering ISP responses to consumer-level cyber security issues. As outlined in **Appendix 3** the regulatory forms that exist are generally codes of practice, best practice guidelines or self-regulatory agreements. These are predominantly developed by industry, usually with support from relevant government agencies. The international trend appears to be towards the development of voluntary codes of practice similar to Australia's icode. As noted above, the United States has implemented its 'ABCs for ISPs', which is a voluntary code.

[9] icode Review Stakeholder Roundtable, 31 May 2012
[10] Colmar Brunton *DBCDE icode review: ISP stakeholder report*, p. 9
[11] Drawn from ISP quotes to the IIA on the icode in April/May 2012
[12] Email, ACMA to the department, 29 November 2012

The Australian Government encourages the use of self- and co-regulatory mechanisms as part of its best practice regulation agenda. Traditionally, self-regulation is where industry voluntarily develops, administers and enforces its own solution to address a particular issue, and where no formal oversight by the regulator is mandated.[13] In reality, however, pure self-regulation without any form of government or statutory involvement is rare.[14] This is true for the icode where government and industry cooperated on its development, the government is working with industry for the code's ongoing improvement as evidenced by the review and through the AISI that provides an ongoing resource to assist industry meet the objectives of the icode.

In the telecommunications sector, government policy has supported regulation that 'promotes the greatest practicable use of industry self-regulation'.[15] A key policy intent of the *Broadcasting Services Act 1992* is for the broadcasting and internet sectors to be regulated in a way that 'does not impose unnecessary financial and administrative burdens' on industry.[16]

OECD research suggests that, when used in the right circumstances, self-regulation and co-regulation can offer a number of advantages over command and control regulation, including:

- greater flexibility and adaptability
- potentially lower compliance and administrative costs
- an ability to harness industry knowledge and expertise to address industry-specific and consumer issues directly
- quick and low-cost complaints-handling and dispute resolution mechanisms. [17]

The review acknowledges that there are significant benefits to a voluntary scheme, and that this is generally the preferred option of industry. However, in making a recommendation the review must also take into account the overall cyber security environment and whether the icode is contributing to this in a positive way.

As previously discussed, given the lack of reliable metrics currently available it is difficult for the review to draw conclusions as to the extent to which the icode is helping to address the problem of compromised computers and whether a mandatory code would facilitate a better outcome. As such, the review considers it would be premature to recommend a more stringent approach until a better overall picture can be drawn.

---

[13] ACMA, Occasional paper *Optimal conditions for effective self- and co-regulatory arrangements,* September 2011, p.7

[14] Ibid, p.4

[15] *Telecommunications Act 1997,* Section 4

[16] ACMA, Occasional paper *Optimal conditions for effective self- and co-regulatory arrangements,* September 2011, p.8

[17] OECD, *Alternatives to Traditional Regulation*, 2009, p.6

Consequently, given ISPs are voluntarily signing up to the icode and are taking some steps to address cyber security risks for their customers, the review supports the icode remaining a self-regulatory scheme at this stage. The review recommends that, at a later date, this position be reassessed by the government against the ongoing performance of the icode following the implementation of a system of metrics.

Recommendation 4

That the voluntary nature of the icode be retained for now and that this be reassessed by the working group at the next review of the icode, or through its ongoing monitoring.

Awareness Raising and Education

Educating Australian internet users about cyber security risks is a key objective of the icode. Users' awareness of online risk, and having the knowledge and tools to deal with such risks, goes a long way towards protecting users from online threats. Educating customers about safe and secure online practices is an essential part of ensuring that Australians are confident online and are able to take full advantage of the benefits of the digital economy.

According to the Colmar Brunton survey, 42% of ISP customers who responded to the survey named their ISP as their primary source of information about cyber security, either through the ISP website or via ISP newsletters. This highlights the importance of awareness raising and education carried out by ISPs. The importance of the ISP's role here is reinforced by research into cyber security commissioned by the Department in 2010 and 2011 that suggested that home and small business users rely on trusted sources for cyber security information.[18]

While most ISPs have strategies in place to educate and raise consumer awareness on cyber security issues, there is a general view held by the review stakeholders that more could be done in this area.

The Colmar Brunton ISP customer survey also found that a high proportion of ISP customers undertake some key behaviours to keep their devices safe from malicious software. For example, many customers are aware that they should not click on suspicious emails (92%), need to regularly update anti-virus software (91%), and should not provide personal details in response to suspicious emails (92%). The survey also showed that other activities that are important for ensuring users' online security, such as regularly changing passwords, were undertaken by a significantly lower proportion of customers. These findings are consistent with the findings from the 2010 and 2011 surveys undertaken by the Department on cyber security awareness. These surveys suggested there is a high reliance on security software to limit exposure to online risks. Only a very small proportion of respondents appeared to recognise the value of employing other mitigation measures such as regularly changing

[18] Woolcott Research, *Cyber security Baseline Survey*, 2010, p.46

passwords.[19] This demonstrates that users do not recognise that they need to adopt a range of measures rather than rely on one or two to protect themselves online.

Survey respondents suggested that many customers are not sufficiently aware of cyber security threats and often take no steps to protect themselves until 'it's too late'. The ISP survey appeared to show that few ISPs actively educate their customers about cyber security at the point of customer acquisition. Less than one in five respondents to the customer survey reported remembering having received information about steps they could take to better protect themselves online when signing up with an ISP.

During the review consultation ISPs suggested that the icode should provide ISPs with more guidance, particularly around awareness raising. The need for more consistent messaging between government agencies and industry was also indentified. ISPs recognised that customers receive cyber security information and messages from a number of sources such as through their ISP, government agencies and also software vendors. ISPs said that it is important that such information and messages are consistent to avoid confusion amongst users. The review recommends that ISPs and government work together to develop consistent cyber security messages for the Australian community. The working group would provide an ideal mechanism for such government and ISP engagement.

Given the reliance customers place on their ISPs for cyber security information, it is important that the icode provides appropriate guidance to allow ISPs to increase their efforts in this area. In particular, ISPs need to encourage customers to take a range of practical steps to better protect themselves online.

The review also noted that the information for distribution to customers, provided under **Schedule 1,** has become dated. Again the working group would be an appropriate forum to update this information to ensure its currency, relevance and effectiveness.

As noted above, the surveys suggested that customers identified their ISP's website as their most common source of information in relation to cyber security issues[20]. During the roundtable discussions stakeholders felt that ISPs should also be encouraged to refer their customers to government cyber security resources, such as **staysmartonline.gov.au** and its associated alert service, that are available for free for more detailed information and for additional help on cyber security matters. This will also help bring about a level of consistency of messaging between ISPs and the government. In addition it will assist the smaller ISPs that may have limited capacity to develop their own resources. Government resources such as the Stay Smart Online Alert Service will also help users receive timely information about the latest cyber security threats, including scams and software vulnerabilities and how they can be addressed.

[19] Ibid, p.40
[20] Colmar Brunton, *icode review – ISP Customer Report*, p.8

Recommendation 5

That measures be taken to:

i) revise the icode to provide better guidance to ISPs so they enhance efforts to educate their customers. Such guidance could include information on the content of messages to customers, how messages are provided, and when messages are provided (for example: at account creation, periodically or driven by events)

ii) as far as possible, ensure consistency of cyber security messages between government and ISPs

*iii) revise and update the cyber security educational and awareness raising material to be distributed to consumers under **Schedule 1** of the icode*

iv) in addition to providing educational material to customers, encourage ISPs to refer customers to free government online resources such as the Stay Smart Online website and Stay Smart Online Alert Service for more detailed and up to date information on cyber security issues including software vulnerabilities and scams, and how they can be addressed.

New technologies

Since the icode came into effect, new technologies such as smartphones and tablet computers have increased in popularity to the extent that they are now challenging home computers as the device of choice for connecting to the internet.

Australian Bureau of Statistics data indicates that, at 30 June 2012, there were 16.2 million mobile handset subscribers in Australia using those devices to access the internet, an increase of 7% from December 2011. The Australian Interactive Media Industry Association (AIMIA) reports that ownership of smart devices has accelerated, with 76% of Australians adopting smartphones and 38% owning tablets in 2012.[21]

During consultations with stakeholders two areas of concern with the increased use of mobile devices were highlighted. Firstly the general view was that users do not recognise that these devices can be vulnerable to cyber security threats. The current icode is limited in addressing this issue. For example, while it is clear that there has been a high take-up of smartphones, tablets and other mobile devices in Australia, these technologies are not explicitly referenced in the icode. ISPs indicated that this is of particular concern as some of the measures, including anti-virus software, available for traditional devices, such as PCs and laptops, are not well developed for mobile devices such as smartphones. The review therefore recommended that the icode should take account of the increasing reliance on mobile devices and provide appropriate guidance to ISPs on how they could effectively educate customers about online protection measures when using these devices.

[21] Adam Bender, *Smartphone, tablet adoption accelerates: AIMIA survey*, ComputerWorld, 27 September 2012

The second area of vulnerability relates to mobile applications. Consultation with stakeholders during the review indicated that users are increasingly exposed to threats from smartphone and tablet applications. Stakeholders were concerned that users download applications on their mobile devices from a range of sources many of which may not be reliable and may have embedded malware. It is therefore important that users are made aware of such vulnerabilities and of the steps they can take to ensure applications are downloaded from reliable sources. Stakeholders felt that ISPs, who in many cases are also mobile providers, should work with application platform providers (such as Google and Apple) to develop appropriate mechanisms to communicate to users about application vulnerabilities and how users could protect themselves from such vulnerabilities being exploited.[22]

In addition, there is an increasing number of devices connected to home networks. This means that multiple devices (such as desktops, laptops, gaming machines, televisions, photo frames and fridges) are working from one home internet connection. Once connected to the internet all these devices have the potential to be compromised with malware. ISPs are of the view that users generally do not understand that traditional home devices such as a television can be subject to online threats once connected to the internet, and therefore, take no precautions to protect these devices from cyber security threats.

Throughout the review process, ISPs highlighted the need to educate customers about the cyber security threats that may be encountered when using internet enabled devices. ISPs also agree that it is critical to change customers' thinking to acknowledge that they need to consider these threats regardless of the device.

When the icode was developed, it was intended to be technology neutral and the review recommends that it should remain so. However, some of the language used in the icode refers largely to more traditional forms of computing, such as desktops or laptops. With this in mind, the review recommends that the 'actions for ISPs' listed under **Sections 6** to **6.4** refer to 'compromised devices' rather than 'compromised computers'.

Recommendation 6

That measures be taken to:

i) work with application platform providers to develop appropriate mechanisms to communicate to users about application vulnerabilities and how they can be addressed

ii) ensure that providers' education and awareness raising activities focus on making users aware of the potential risks associated with the use of mobile devices and other internet connected devices, in particular home devices. This should include providing users with information on measures they could take to protect these devices from

[22] Icode Review Industry Roundtables, 31 May and 25 July 2012.

online threats, noting that some measures may be more specific to certain types of devices

iii) *broaden the icode to remain technology neutral so it can be flexible enough to cover current and future changes – including updating the icode to refer to 'compromised devices' rather than 'compromised computers'.*

Detection and Assistance to Customers

The ACMA provides two reports to ISPs participating in the AISI which have compromised computers on their networks – a daily report and a repeated sightings report. The daily report identifies the number of compromised computers detected for each participant, a list of compromised IP addresses and the corresponding name of the compromise. The list contains information reported to the ACMA in the previous 24 hours. The weekly repeated sightings list records those IP addresses which have appeared in the daily AISI reports at least 10 times in the previous fortnight.

The purpose of the repeated sightings report is to identify long-term, persistent compromises. Where an ISP relies on the repeated sightings reports, a compromise will have existed for at least two weeks before action is taken to inform the customer. This can be problematic because many customers are assigned dynamic IP addresses by their ISP. With dynamic IP addressing, a customer's IP address changes on a regular basis. This leads to a situation where a compromised computer may not appear on the repeated sightings list at all because its primary identifier, the IP address, has changed before it could appear at least 10 times in a particular fortnight. It may be that a substantial number of compromises are never addressed. The ACMA estimates that the repeated sightings report lists fewer than 5% of the unique compromises covered in the daily reports.[23]

The icode does not specify a trigger for ISPs to take action in response to compromised computers on their network. According to ACMA research, around a third of ISPs interviewed only take action in response to the AISI repeated sightings report.[24] Therefore, relying on these reports to address all compromises is not ideal.

Colmar Brunton noted from their customer survey results that, of those customers that had been notified by their ISP that their computer had become infected by malicious software, almost two thirds (61%) said they were not aware of the issue prior to notification. Colmar Brunton observed that this figure highlights why it is important for ISPs to contact customers in a timely manner when their systems detect a compromise. The customer survey also identified that, of those customers who had never had a compromised

[23] Ibid, p.8

[24] ACMA, *The Australian Internet Security Initiative - provider responses to security-compromised computers: Interview with industry participants,* September 2012, p.2

computer, most expected their ISP to inform them either immediately (60%) or within 24 hours (31%) of when their computer was infected by malware.

While the review recognises that it may not be possible to match notification times to this timeframe, these figures suggest that there is a strong customer expectation that ISPs will alert them in a timely way about a compromised device. The review considers that it is important for the icode to specify clear triggers and reasonable timeframes for ISPs to act in response to the detection or notification of a compromised device.

It is also important that ISPs are able to identify those customers who remain compromised. Possible reasons for persistent compromises include a lack of timely advice about the compromise from the ISP, the customer not taking action when informed about the compromise, or the customer becoming the victim of repeated compromises. These customers will require more specific direction so that they can effectively address the problem. As noted above, given the dynamic nature of IP addresses, solely relying on the ACMA repeat sighting list may lead to an ISP missing some compromises. However, ISPs generally hold information about which IP address matches a particular customer at a given point in time for various reasons such as network management. This information is typically held for a limited period, such as a few weeks or months, and varies across ISPs. Given this, ISPs should be in a position to identity the customers who remain, or are repeatedly, compromised, and therefore offer assistance.

The resource implications of assisting customers is a key area of concern for ISPs. Some large and medium sized ISPs surveyed by the ACMA indicated that an inability to allocate sufficient organisational resources was the main barrier preventing them from dealing with computer compromises more effectively. Around a third of surveyed ISPs who indicated that they act on AISI reports identified resourcing issues as limiting their capacity to make system improvements or provide better assistance to their customers to help them deal with these compromises. The Colmar Brunton survey indicated that very few (10%) internet users reported having been contacted by their ISP about a specific security problem.[25] The ACMA's research noted that AISI participants advised that their residential customers and small to medium sized businesses experienced the most computer compromises, and had the most need for assistance from ISPs.

The OECD noted in 2012 that there are good reasons for ISPs to want to alert customers about compromises.[26] For example, a proactive approach to cyber security can allow ISPs to provide more secure services to customers, giving those ISPs a competitive advantage over other ISPs. ISPs can also use this approach to reduce the costs associated with technical support and customer service, improve network performance through the management and reduction of compromised devices, and strengthen user confidence.

[25] Colmar Brunton, *icode Review – ISP Customer Report*, 2012, p. 14
[26] OECD, *Proactive Policy Measures By Internet Service Providers Against Botnets*, 7 May 2012, p.7

Once the ISP has identified or been informed about an infected device, the icode provides that the ISP should, through various avenues, communicate this to the customer and provide assistance. For example, the icode suggests that ISPs can send an email, call the customer, reset a customer's password to oblige them to contact the ISP, temporarily quarantine an infected device or restrict outbound e-mail messages. This range of measures provides ISPs with the flexibility to adopt the most resource efficient approach consistent with their operational requirements.

According to Colmar Brunton survey results, around 94% of customers provided with guidance or assistance by their ISP to resolve a security problem found the help either useful or very useful.[27] However, the same research also showed that ISP follow-up was undertaken in around only one in five cases, despite customers feeling such follow-up contact was important. The review believes that follow-up by ISPs would not only help to ensure that the compromise is addressed by the customer, it would also provide ISPs with an opportunity to further assist customers so that they can avoid becoming victims of a repeat compromise.

Recommendation 7

That the icode be revised to specify:

i) *clear triggers for when ISPs should contact their customers once a compromised device is identified*
ii) *a reasonable time within which ISPs are required to take action in response to the detection of a compromised device on a network*
iii) *that ISPs are to establish a system to identity and provide more directed assistance to those customers who remain compromised or are repeatedly compromised*
iv) *the continuation of a flexible approach in how ISPs contact and assist customers so that it meets their operational and resource requirements, noting that such an approach must be effective in assisting customers*
v) *appropriate strategies for follow-up by ISPs of customers with compromised devices.*

Reporting to government agencies

One of the actions ISPs are required to take under **PART B – Recommended Action for ISPs** is to report malicious activity to the relevant government authority where the ISP believes the nature or extent of the activity represents a significant 'cyber security incident'.

Signatories were asked about the usefulness of the guidance provided in the icode on reporting of such activity. The majority of ISPs respondents to the Colmar Brunton survey reported that the icode was moderately or very useful in this respect. The contact details for

[27] IPSOS Omnibus Survey, *Cyber security Awareness Post Wave Report*, 23 July 2012, p.7

agencies who can act on reports, listed under **Schedule 3**, were considered particularly beneficial.

Approximately half of ISPs respondents of the survey reported having notified the AFP, CERT Australia and State/Territory law enforcement agencies in relation to cyber security incidents involving their customers. Amongst those who had contacted the AFP and CERT Australia, satisfaction was generally high. Conversely, satisfaction with the response of State/Territory law enforcement was low. One ISP perceived local police authorities to be disinterested unless a direct threat had been made on an individual, while another provider argued that the police react to outbreaks only, rather than to individual threats. In another case, State and Territory law enforcement agencies acted as an intermediary, passing on the report to the AFP's High Tech Crime Centre. These bodies appear to have limited direct impact on the actions undertaken upon receipt of a cyber security incident report.

Three of the ISPs who responded to the survey reported that there were cyber security incidents that they had considered reporting but ultimately did not. Other ISPs said there were no incidents, or they could not recall any incidents, that had not been reported. The reason given by the three ISPs that did not report incidents were that they did not think it was serious enough, did not know which agency to contact or did not think it was worth the time and effort to report.

CERT Australia told the review that it has received few 'significant cyber security incident' reports from ISPs. The review considers that the notification provisions under **Section 6.4** could be improved to provide a mechanism for ISPs to better evaluate the significance of cyber security incidents and judge whether a particular incident should be reported. Several ISPs suggested that case studies or some guidance or tips would be helpful. The review recommends the working group revise and clarify the notification provisions to take this into account.

The review also notes that while ISPs are generally satisfied with the response from government agencies when reporting to them, there is occasionally a lack of follow-up from the agency concerned.

Recommendation 8

That:

i) *CERT Australia work with industry to introduce mechanisms, such as an incident matrix, to assist ISPs identify what constitutes a 'significant cyber security incident' for reporting purposes*

ii) *government work with ISPs to facilitate information flow when cyber security incidents are reported.*

Coverage of the icode

The 34 signatories to the icode represent approximately 90% of Australian home internet users. While this can be considered a good initial result, there remain a considerable number of ISPs which are not signatories. As a guide, the AISI has a membership of 132, many of which are ISPs providing internet services to Australian consumers.

Through the Colmar Brunton survey non-icode signatories were asked why they had not signed up to the code. One mobile telecommunications provider responded that there had been considerable internal discussion about whether they considered themselves an ISP or not. This is an interesting response as it highlights how the provision of internet services has evolved with mobile computing. The term 'internet service provider' is still largely associated with those companies offering fixed line broadband connections. While this remains a valid categorisation it ignores the role played by mobile telecommunications companies in providing wireless broadband internet.

The review considers that organisations providing internet services to the community on a commercial basis should be considered an internet service provider for the purposes of the icode. This is of particular importance given the increased popularity of internet connected mobile devices. As such, the review recommends that the IIA clarify the definition of internet service provider to include the provision of wireless internet services, with a view to encouraging mobile telecommunications providers to become icode signatories.

The review also considered that raising the profile of the icode amongst consumers would help to increase its membership. The Colmar Brunton customer survey found that only 3% of all customers had heard of the icode. This figure was marginally higher (10%) for those who had experienced a compromised computer and had been contacted by their ISP.

The survey also showed that cyber security is an 'important' or 'very important' consideration for consumers when selecting an ISP. However for some ISPs, the obligation imposed on them by the icode to educate customers about cyber security threats – which does not apply to their non-signatory competitors – is currently seen to be of limited value

in terms of potential commercial return. This view is likely to change if the icode and its purpose are better known amongst consumers.

The mechanism currently in place to help consumers identify icode compliant signatories is the consumer Trustmark provided for under **Section 9**. The Trustmark is intended to both promote the icode and act as a commercial incentive by showing customers which ISPs achieve minimum standards on cyber security (that other, non-compliant ISPs may not). This may influence a customer's decision when selecting an ISP. Only icode compliant ISPs are permitted to display the Trustmark on their websites or distribute it as part of the promotional material provided to their customers.

Considering the low level of consumer recognition of the icode, the review recommends that the Trustmark is more widely promoted by the IIA and the icode signatories. This is consistent with other trust marks such as the Heart Foundation Tick.

Recommendation 9

That:

i) *the term 'internet service provider' be clarified to include mobile internet service providers*
ii) *strategies be developed to promote the icode with ISPs, with a view to increasing the number of signatories*
iii) *strategies be developed to promote the icode Trustmark to raise consumer awareness about the icode.*

Appendix 1

icode members

AAPT
Activ8me
Albury Local Internet
APEX Internet
BarNet
BKB Internet
China Telecom (Aust.)
Comcen
DCS Internet
Dreamtilt
Earthwave
ECN
Edith Cowan University
Enterprise IT
Isage Internet
Internode
iiNet
ISP One
Minopher
Montimedia
Netspeed Internet
Nextep Broadband
Optus Internet
PPS Internet
Primus Telecommunications
SkyMesh Pty Ltd
SpinTel
Studentnet
Telstra Bigpond
The Galaxy Gateway Computer System
Unwired
Vividwireless
Velocity Internet
Zettanet

Appendix 2

icode Review Terms of Reference

1. The review will examine the operation of the icode since its implementation in 2010 and evaluate its effectiveness at achieving its stated objectives, including:
    (i) educating customers and raising awareness of cyber security risks
    (ii) detecting compromised computers and other malicious activity on their networks
    (iii) taking action when compromised computers are detected
    (iv) reporting significant cyber security events to relevant government agencies

    The review will also explore whether these stated objectives remain current and relevant.

2. In undertaking the above, the review will examine:

    a. the level of take up and awareness of the icode by Australian ISPs
    b. the level that ISPs participate in related initiatives, specifically the AISI
    c. how, and to what extent, ISP adherence with the icode is measured and managed
    d. the response rate and actions undertaken by ISPs when receiving notifications from the AISI
    e. the response rate and actions undertaken by ISPs when receiving notifications from third party resources
    f. the level and type of assistance provided by ISPs to customers when a compromised computer is identified
    g. the measures ISPs take when customers do not respond to notifications that their computers are compromised
    h. how awareness raising and education is provided by ISPs to customers
    i. customer feedback on the effectiveness of the notification and support provided by ISPs
    j. the level of reporting by ISPs to the appropriate Government agencies on significant cyber security events
    k. comparisons with relevant international models
    l. potential methodologies and metrics to provide measures of the effectiveness of the icode in managing cyber security risks in future
    m. how, and to what extent, ISPs otherwise manage cyber security on their networks
    n. other sources of assistance customers may use to remediate a compromised connection

3. The review will also seek to assess how successful self-regulation has been, and if necessary, consider measures to strengthen compliance with the icode and enhance obligations on ISPs.

In developing recommendations, the review will take into account whole-of-government priorities, including the outcomes of the Cyber White Paper process.

Appendix 3

International anti-malware initiatives

A good picture of international efforts in this area is provided by the OECD. In a 2011 analysis of international initiatives aimed at mitigating botnets at the ISP level, the OECD examined the icode, as well as initiatives in Germany, Japan, Korea, the Netherlands, the United Kingdom and the United States. Because these schemes are relatively new, the study focused primarily on the attributes of the various schemes and attempts to identify the characteristics of successful initiatives. The study does not rate their effectiveness. It is worth noting that in the relatively short space of time since the study was completed, a number of countries have introduced or refined their own anti-botnet strategies. This gives a good indication of the fluidity of efforts in this space.

The OECD report notes that none of the countries analysed has yet mandated ISP participation in anti-botnet initiatives (and this continues to be the case with the new initiatives established). In most cases self-regulatory measures have been adopted. Current botnet mitigation initiatives at the international level are either primarily private sector-led schemes or public-private partnerships.

As an example, the report notes that with the encouragement of the Dutch Telecom Regulatory Authority (OPTA), ISPs in the Netherlands have created a formal, private sector-managed alliance to address the country's botnet threat. Germany's anti-botnet effort is also led by the private sector, but with financial and technical support provided by the federal government.

The approaches taken by Japan and Korea are similar to the public-private approach adopted in Australia, with government agencies working closely with ISPs to identify and mitigate botnets. Each of these countries also has a dedicated department within the relevant government agency that co-ordinates efforts across the ISP industry, as is the case in Australia.

In the United Kingdom, ISPs have previously responded to botnets on an *ad hoc* basis. However, as noted in the Government's Cyber Security Strategy, published in November 2011, UK government departments, law enforcement and ISPs have laid the groundwork to form a public-private partnership in order to identify and mitigate botnet attacks, as well as identify the kinds of support that might be offered to internet users.

In the United States, the current policy guidance exists in the form of a voluntary 'best practice' document produced by the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC).

In Germany, similarly to Australia, ISPs can choose to sign a code of conduct pledging to participate in an anti-botnet initiative on a voluntary basis. In the Netherlands, ISPs may choose to sign a commitment to notify customers of compromised machines, isolate infected computers and share information with other providers, but no compliance mechanisms are in place.