APEC

Asia-Pacific
Economic Cooperation

APEC Guidelines for Creating

Voluntary Cyber Security

ISP Codes of Practice

May 2011

Telecommunications and Information Working Group

March 2012

TEL self-funded project

Prepared by:
Cybersecurity Policy and Asia Pacific Section
Department of Broadband, Communications and the Digital economy
Australia
Email: asia.pacific@dbcde.gov.au

For APEC Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919 600 Fax: (65) 68919 690
Email: info@apec.org Website: www.apec.org

APEC#212-TC-01.2

Table of Contents

1.0 INTRODUCTION 1
1.1 BACKGROUND 1
1.2 PROJECT BACKGROUND 1
1.3 OBJECTIVE OF THE GUIDELINES 2
1.4 BENEFITS TO ISPS OF PROACTIVELY MANAGING CYBERSECURITY ISSUES 2
2.0 ENGAGING WITH INDUSTRY TO ESTABLISH A CODE 3
2.1 ESTABLISHING A RESPONSIBLE AGENCY 3
2.2 STAKEHOLDER ENGAGEMENT STRATEGY 3
2.3 ENCOURAGING THE PARTICIPATION OF ISPS 3
2.4 ESTABLISHING MINIMUM REQUIREMENTS FOR A CODE 4
2.5 PROVIDING INFORMATION ABOUT THE CODE 5
2.6 REGISTRATION OF PARTICIPATING ISPS 5
3.0 RAISING CYBERSECURITY AWARENESS: PREVENTION IS BETTER THAN THE CURE 7
3.1 EDUCATING CONSUMERS 7
3.2 STANDARDISED INFORMATION 7
4.0 RESPONDING TO CYBER SECURITY THREATS 8
4.1 NETWORK MANAGEMENT 8
4.1.1 COLLECTION OF INFORMATION ON COMPROMISED CONNECTIONS 8
4.1.2 USING THIRD PARTY SERVICES 9
4.1.3 COLLECTING INFORMATION FROM OTHER ISPS 9
4.2 METHODS FOR CONTACTING AFFECTED USERS 10
4.2.1 NOTIFYING USERS INDIVIDUALLY 10
4.2.2 NOTIFYING USERS PUBLICLY 11
4.2.3 NOTIFYING USERS BY RESTRICTING THEIR ONLINE ACCESS 11
4.3 PROVIDING REMEDIAL ASSISTANCE TO AFFECTED USERS 11
4.3.1 OTHER CONTACT POINTS FOR USERS 12
4.4 BUILDING ISPS' CUSTOMER SUPPORT CAPABILITIES 12
5.0 IMPLEMENTING A CODE OF PRACTICE 13
5.1 LAUNCHING THE CODE 13
5.2 MANAGING AND REGULATING THE CODE 13
5.3 CODE REVIEW 14
5.4 ESTABLISHING A FRAMEWORK FOR COOPERATION AND COLLABORATION 14
EXAMPLE – STANDARDISED INFORMATION FOR CUSTOMERS 15
CASE STUDY: THE UNITED STATES (FCC ADVISORY COUNCIL) 15
CASE STUDY: NEW ZEALAND (NETSAFE) 15
CASE STUDY: SHADOWSERVER FOUNDATION 15
CASE STUDY: UNITED STATES (COMCAST) 15
CASE STUDY: JAPAN (CYBER CLEAN CENTER PROJECT) 15
CASE STUDY: AUSTRALIA (AUSTRALIAN INTERNET SECURITY INITIATIVE AND THE INTERNET INDUSTRY ASSOCIATION'S ICODE) 15

1.0 INTRODUCTION

1.1 Background

The Internet provides significant benefits to APEC economies by facilitating business, trade and the delivery of government services including health and education, and by enhancing social interaction. However, the Internet is not a risk free environment. While the increasing bandwidth available to home users and small businesses is helping to improve the efficiency and quality of their online activities, the 'always-on' nature of some broadband access technologies amplifies the risks of certain online attacks. Further, as more people access the Internet through a range of technologies the scope and opportunity for malicious and criminal online activity can be expected to broaden.

Internet users are increasingly exposed to various cyber crimes, including illegal access to personal or private information, theft of financial property and fraud. While the cost of any individual case may be relatively small, there is a risk that if too many people are affected then this may result in a loss of confidence in the online environment. Therefore, as home and business users in the Asia-Pacific region become more dependent on the Internet for their daily activities, it will become more important to maintain a safe online environment. This is particularly true for vulnerable individuals such as children and new users.

Compromised home and small business devices also pose a significant risk to critical infrastructure and government networks. For example, an aggregation of such compromised computers, generally referred to as a "botnet" could be used to send malicious spam or launch distributed denial of service attacks on government or business networks. Such actions have the potential to compromise the delivery of essential services such as communications, water, energy, transport, communications and finance. This represents a growing problem for many businesses, including ISPs.

1.2 Project background

At the 7th APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMIN 7), held in Bangkok, Thailand on April 2008, Ministers recognised that there are a number of cybersecurity risks to Internet users in the Asia-Pacific region. As a result, the Bangkok Declaration articulated the importance of developing effective responses against cyber threats, malicious attacks and spam through:

- providing users with the knowledge and skills needed to deal with these threats; and
- encouraging continued information sharing on how to protect electronic information systems.

This direction was recently reinforced by Ministers at the TELMIN 8 meeting, held in Okinawa, Japan in October 2010. At this meeting, Ministers recognised that to effectively respond to cyber security issues, there is need to improve "...collaboration with industry partners, the Internet technical community and all other relevant stakeholders, including ISPs, telecommunications operators as well as regional and other international organisations."

At the 40th Meeting of the APEC Telecommunications and Information Working Group (APEC TEL 40) held in Cancun, Mexico in September 2009, economies approved the *Cyber Security Voluntary ISP Codes of Practice* project. As part of this project, a workshop was held at APEC TEL 41 in May 2010 in Chinese Taipei to assist economies to identify strategies for developing effective codes of practice. Additionally, preceding the workshop, the *Cyber Security in APEC Economies Questionnaire* was distributed on 19 January 2010 to investigate regulatory and ISP initiatives that address cyber security threats, with a particular focus on regulator and ISP collaboration.

1.3 Objective of the guidelines

Many online security threats are difficult for Internet users to detect. However, as the conduit for much of the Internet's traffic, ISPs are well placed to provide information, raise awareness of cybersecurity issues and educate Internet users on how to better protect themselves online.

The key objective of these guidelines is to provide information for economies to assist them to develop effective ISP cyber security codes of practice. The aim of providing this information is to supply guidance to APEC economies on how to manage cyber security issues on their networks, including through:

- providing information to raise cyber security awareness;
- monitoring connections on their networks for suspected malicious activity;
- notifying consumers when a compromised connection has been detected;
- providing remedial information to affected consumers; and
- providing remedial support to affected consumers.

1.4 Benefits to ISPs of proactively managing cybersecurity issues

A collaborative approach to addressing cybersecurity threats benefits all sectors of the online environment, including ISPs, consumers, business and governments. In particular, a proactive industry-wide approach to cyber security can benefit the ISPs in a number of possible ways including:

- the provisioning of more secure product offerings to customers;
- reducing help desk and customer service costs;
- increasing network performance due to managing and reducing the incidence of compromised Internet connections; and
- increasing user confidence in ISPs operating in an enhanced security culture, both in and across regional economies.

2.0 ENGAGING WITH INDUSTRY TO ESTABLISH A CODE

2.1 Establishing a responsible agency

Peak industry groups are well placed to initiate dialogue with ISPs, administer industry codes and undertake drafting. Therefore, from the outset, the development of a code should be the responsibility of an appropriate peak industry group or, if this does not exist, a group of leading ISPs. While it is more likely that a code will be successful if its development is driven by industry, in some circumstances, it may be necessary for regulatory authorities to take the lead on drafting and maintaining the voluntary code. Importantly, the agency responsible for the code should take carriage of the code through its development, implementation and ongoing management.

While industry, particularly peak industry groups, would be effective in the administration of the code, the government agencies responsible for cyber security and telecommunications regulation are encouraged to adopt an active assisting role. For example, regulators could assist with drafting the code, in particular by ensuring that the proposed text is consistent with existing regulation.

The government agency responsible for cyber security may also consider partnering with industry by promoting and providing information on the code. Where necessary, government may also provide financial assistance to implement the code. Government would be encouraged to coordinate communications between industry groups and other relevant agencies/ministries. Governments are also well positioned to facilitate international partnerships and information sharing.

2.2 Stakeholder engagement strategy

Due to the complexity of managing cybersecurity threats on the Internet, the development of an ISP code of practice will ideally receive input from a broad range of stakeholders. To develop an effective code, the interests of stakeholders need to be managed and addressed. The development of a stakeholder engagement strategy by the responsible agency is a useful measure for planning wider consultation. Considering how stakeholders will be impacted and their level of influence, the responsible agency can prioritise the consultation process.

From the *Cyber Security in APEC Economies Questionnaire*, all survey respondents indicated that there were several types of stakeholders in their economies responsible for managing cyber security. These stakeholder groups included ISPs, and peak industry groups, government agencies and ministries, and Computer Emergency Response Teams (CERTs). Developing and implementing a voluntary ISP code of practice will not succeed without the commitment of at least the major ISPs. Effective strategies for engaging consumers should also be considered in developing a code.

2.3 Encouraging the participation of ISPs

ISPs would be encouraged to promote compliance with an ISP cyber security code of practice because it would be a strong positive for consumers. Where there is a peak industry group, it would therefore be beneficial to further promote the code through the group’s website.

Participating ISPs should be encouraged to promote themselves as compliant with the code and therefore, as reputable providers of Internet services to consumers.

In drafting the code, the responsible agency should attempt to ensure the simplicity of the code in all steps of its process. The implementation, management and the added responsibilities that participating ISPs must undertake should not be onerous, so as to minimise the compliance costs for ISPs. This would encourage greater participation of industry, particularly in the case of smaller ISPs where compliance to the code could be costly.

2.4 Establishing minimum requirements for a code

In drafting a code of practice it is useful to develop a checklist of requirements to ensure the code effectively responds to cyber security threats. At a minimum, this checklist should include the following sections:

- Registration – while the code would be voluntary, participant ISPs should be registered to commit themselves to the code and to assist with its effective implementation (see **Section 2.6**).
- Awareness raising – the code should not be limited solely to responding to compromised connections detected on a network. Raising cyber security awareness minimizes the level of intervention for an ISP and may prevent Internet users from being impacted by future cyber threats (see **Section 3**).
- Network management – to provide guidance to ISPs on how to efficiently and effectively manage their networks to detect cyber security threats and other irregular activity in an unobtrusive way that has a negligible impact on their customers' online experience and privacy (see **Section 4.1**).
- Responses for ISPs –the responses ISPs should take when they detect a compromised connection on their account is likely to vary from economy to economy. However, at a minimum, the code should outline if and how customers will be contacted to inform them that their computer has been potentially compromised, remedial information on how an affected user may redress the compromise, and who to contact for further information (see **Section 4.2 to 4.4**).
- Reporting –what information and how often ISPs should send to the regulator or agency managing the code to review the security of an economy's networks and the effectiveness of the code (see **Section 5.2**).
- Review – the code should state when and who will review the code (see **Section 5.3**).

There are also other elements that could be considered in the drafting of a code:

- Standardised information for consumers – a set of standard information may be provided by ISPs to all new consumers to raise their awareness of the code and cyber security in general. An example of this information has been provided at **Appendix A**.
- Self regulation – information should be provided to ISPs on how they will self monitor and implement the code (see **Section 5.2**).

- Benchmarks – informal benchmarks may be established to reduce the costs for participating ISPs. For instance, given the significant number of cyber attacks and other compromises on ISP networks, it could be difficult for participating ISPs to respond to all suspected compromised connections. It may therefore be reasonable for the code to establish an informal benchmark on the amount of cases investigated by the ISP, for example, as a broad percentage of the number of total suspected compromised connections detected. However, it may be more appropriate to target connections that exhibit repeated suspicious activity. For example, the ISP might only take action after a compromised connection has been ongoing for more than a specified period (see **Section 5.2**).

2.5 Providing information about the code

Information about the code should be made readily available to all ISPs and consumers. The industry or other body responsible for the code should make it available from its website, or consider developing a standalone website focussed on providing content about the code. Responsible government agencies should be encouraged to develop additional resources to complement this website, for example through publicising Frequently Asked Questions and fact sheets on their own website.

Additionally, as the website may be the first exposure ISPs have to the code, it should display contact details for interested ISPs and other stakeholders to use if they have further queries. For the convenience of ISPs, a variety of contact methods should be made available, including phone, email and fax.

Additionally, promotion of the code is important in the initial stages of its implementation. To attract significant publicity, government agencies and industry should be encouraged to approach the Minister with appropriate portfolio responsibility covering cyber security to launch the code; participation of the Minister is likely to attract interest from the broader telecommunications industry and the media.

2.6 Registration of participating ISPs

While complying with an ISP cyber security code of practice would be voluntary, provisions should be made to ensure the code is implemented effectively and efficiently. A formal registration process is an effective means for obtaining commitment from participating ISPs to implement the provisions. Further, registration is key to accurately reporting the level of cyber security threats and the effectiveness of the code in an economy.

Registration of participating ISPs should be incorporated as part of the consultative process. It should be a simple process and accessible through different media channels such as via the Internet, phone, email or fax. A webform on the code's website would be the most direct means for an ISP to register. Details collected in the registration process should focus on identifying a contact within the ISP, information about their networks and their network security regime. Importantly, this information can provide a snapshot of an economy's networks and cybersecurity initiatives.

Registered ISPs that achieve the requirements set out in the code may also display a Trustmark to indicate their compliance with the code of practice on their website and in emails to their customers. The Trustmark could provide an online link to information about the code of practice to further increase consumer awareness of the provisions of the code.

For example, the Australian Internet Industry Association has provided the following example Trustmark in its *Internet Industry Code of Practice* or *icode*:

icode
compliant

Further information on compliance of ISPs to the code is covered in **Section 5.2**.

A case study on engaging with industry from the United States has been provided at **Appendix B**.

3.0 RAISING CYBERSECURITY AWARENESS: PREVENTION IS BETTER THAN THE CURE

Raising cyber security awareness of Internet users is critical for responding to cyber security threats and therefore should be an important aspect of an ISP cyber security code.

3.1 Educating consumers

ISPs who have agreed to comply with a cyber security code should be encouraged to raise the cyber security awareness of their customers. ISPs are best placed to distribute this information as they have a direct relationship with their customers and are in regular contact through network updates and billing.

The code should require or at least encourage ISPs to provide existing and new customers with information on how to better protect themselves online. Channels for conveying this information could be emailing customers directly, features on the ISP's website, or on customer bills/statements. Additionally, as governments in many economies have their own websites for raising cyber security awareness, ISPs should be encouraged to direct customers to these websites for further detailed information.

3.2 Standardised information

As stated in **Section 2.4**, in the drafting of the code the responsible agency may consider including standardised information to be provided to consumers once the code is implemented. This information would be provided by ISPs to their customers to introduce the code and, importantly, to raise awareness.

Consumer awareness information should be clear, consistent and easily understood. The format may be a checklist of easy to implement steps Internet users may take that may help protect them online. A checklist of tips for consumers to improve the security of their connection may include:

- Turn on automatic operating system updates and install them when they are released
- Install anti-virus and other security software and keep it updated*
- Install a personal firewall or use a hardware router*
- Use a stronger password and change it regularly
- Take caution when clicking on links or attachments in emails
- Take caution when sharing personal information online
- Take action immediately if you suspect that your computer has been compromised.

* ISPs may use this opportunity to develop and market their own security software or act as a channel partner for software vendors.

An example of standardised information which includes cyber security awareness raising tips from the Australian icode has been provided at **Appendix A**.

A case study on cyber security awareness raising strategies from New Zealand has been provided at **Appendix C**.

4.0 RESPONDING TO CYBER SECURITY THREATS

When a compromised connection exists on an ISP's network, it is of benefit to the ISP to provide assistance to affected users and therefore restore the integrity of its networks. For a cyber security code of practice to function efficiently, ISPs need to be sufficiently engaged in managing their networks, notifying affected users and assisting in their recovery.

4.1 Network Management

Analysing network activity for suspicious online behaviour can be an effective means to expedite the identification of and responses to cyber security threats. Suspicious online activity could be the unwarranted and often significant transmission of data, such as from a 'botnet' infected computer, or the sending of numerous emails within a short timeframe, as in the case of a computer compromised by a 'spambot'.

Collecting information from compromised connections assists in their recovery and helps protect customers and network infrastructure from future cyber attacks. ISPs may consider the use of 'honeypots' to assist them in the detection of suspicious activity on their networks. Alternatively, an ISP may use third party sources of information to inform them of suspicious activity on their networks. These are described in **Sections 4.1.1 and 4.1.2** below.

4.1.1 Collection of information on compromised connections

Collecting information from a compromised connection can assist affected consumers to remedy their situation. For example, the honeypot system detects unauthorized activities on compromised connections, collects information on malicious activity on the network, such as botnet activity, and the sources of the attack. Used as part of network security management, honeypots are an effective means for collecting information on compromised connections.

A honeypot may be a computer or a network that appears to be part of a network but is isolated and should not have any network traffic. Any information captured as Internet traffic is likely to be malicious or unauthorized. Honeypots may be set up at a variety of locations on the network, including inside or outside of the internal network, or within the firewall.

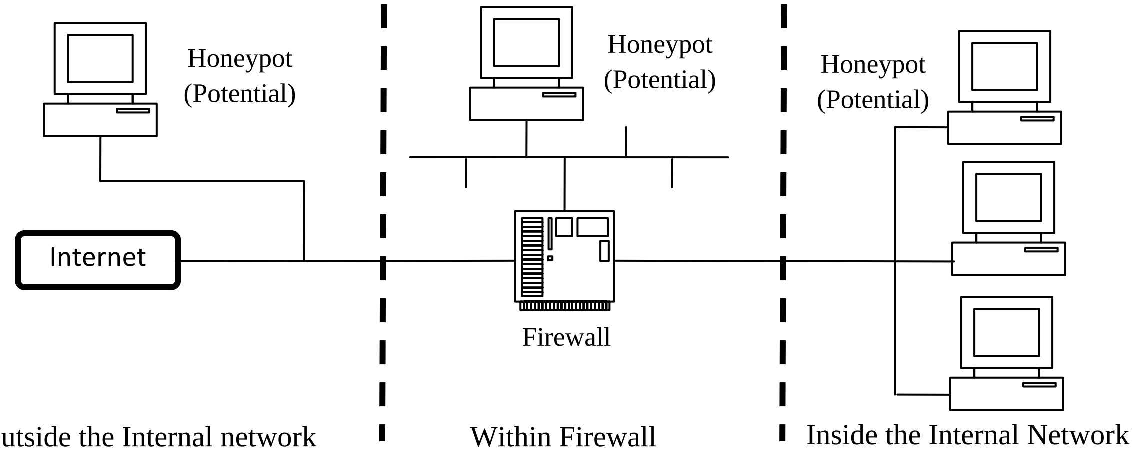


Figure 4.1 Example of a honeypot system. Adapted from 'Honey Pot System Explained' by Loras R. Even available at SANS (SysAdmin, Audit, Network, Security) Institute available at www.sans.org/security-resources/idfaq/honeypot3.php

In the event that a connection is infected by a bot, it launches attacks on neighboring IP addresses. Honeypots on the network collect the bots along with the attacker's IP address and timestamps the event. This information may then be used to alert affected users or help ISPs provide remedial assistance.

Tips for using honeypots:

Combine different honeypots on the network:
There are several types of honeypot:

- Low-interaction – A honeypot of this type emulates vulnerabilities of a certain operating system and collects information on attacks it is subjected to.
- High-interaction – This type of honeypot emulates a real operating system that can interact with other infected computers and thereby collects bot programs and may be used to observe the follow-on cyber attacks launched from that computer.

Using high-interaction honeypots may be more accurate given that the computers are actually infected, which assists ISPs avoid false-positive detections. However, in order to collect data on a wide range of attacks, combining both types of honeypots on the network is more effective.

Network allocation of honeypots
If clustered together, compromised high-interaction honeypots may degrade network performance. To prevent this, ISPs should consider placing each honeypot in a different segment of the network and limit the communication between the honeypots using firewalls.

4.1.2 Using third party services

ISPs may utilise the services of third parties to assist with detecting and identifying compromised connections on their networks. Relevant third party services include:

- databases of known malware;
- databases of known domain and IP blocklists; and
- screening of suspicious files.

Importantly, there are also third party organisations that more directly assist in the management of network security; for example, providing ISPs with data to help them identify compromised connections on their networks. Therefore, depending on the size of the ISP and its networks, it may be more practical to use the services provided by a third party to assist with network security.

A short case study on the Shadowserver Foundation, a third party organisation, has been provided at **Appendix D**.

4.1.3 Collecting information from other ISPs

As most cyber security threats quickly spread regionally or internationally, ISPs will encounter a volume of cyber attacks originating from other ISP networks. Therefore, to protect their networks from compromises, ISPs should be encouraged to collect information on malicious activities and to share this with other ISPs. Further, ISPs should be encouraged to proactively collaborate with other relevant stakeholders on the exchange and sharing of information on cyber attacks.

However, it should be noted that ISPs should be encouraged to consider regulations and legislation pertaining to privacy for each economy. These should be taken into account when collecting and distributing information from networks.

Tips on collecting information:

Using a combination of information sources
ISPs should consider using multiple data sources to inform them of suspicious activity on their networks. For example, rather than depending only on a honeypot system, it would be more effective for ISPs to combine data from a honeypot with data provided by a third party. This would allow the ISP to cross-check information in addition to identifying other possible compromises on their networks.

Privacy protection
ISPs should avoid disclosing the personal information of users when sharing cyber attack information with other ISPs or organizations. ISPs should consider anonymization measures such as using anonymous identities when sharing and exchanging information on compromised computers.

Recording timestamps of infections and attacks
Recording a timestamp of infections and attacks along with other information may assist in identification of affected users even if their IP address is dynamically assigned.

4.2 Methods for contacting affected users

If a compromised connection is detected, ISPs are encouraged to further investigate to verify the accuracy of any information recorded. Once satisfied that an affected user has been correctly identified, ISPs should notify the user. ISPs may consider notifying users by contacting them individually, as part of a group or by blocking or limiting their online access.

In notifying users individually, ISPs may contact affected users by email, phone or mail. The approach should be selected taking into account the cost and effectiveness of each method. Further, contacting users through more than one channel may improve the effectiveness of ISPs' notification strategies.

4.2.1 Notifying users individually

Email is a cost effective method for notifying users as the information conveyed may be reused for numerous affected users. Alternatively, each time the user connects to the Internet, the ISP may alert the user through their web browser; for instance, by redirecting them to an alert message. This method is used in the private cyber security initiative of Comcast which is outlined in **Appendix E**.

In the first instance of notification, other methods, such as a phone call or mail, may be considered too labour intensive and should instead be used later in the remedial process to complement specific support provided to affected users.

4.2.2 Notifying users publicly

An efficient method for notification would be to contact numerous affected users simultaneously through methods such as:

- online announcements, for example, through the ISP's website or newsletter, weblog or podcast; and
- a blind-copied email list.

While an effective method for both informing affected users and raising awareness, ISPs need to consider the privacy of users' data. Online announcements should use a reliable domain name or URL to ensure that consumers trust the authenticity of this information.

4.2.3 Notifying users by restricting their online access

While primarily a remedial approach, ISPs may also consider using blocking an affected user's access to the Internet to notify an individual. ISP blocking methods, such as a 'walled garden' may be used to prevent the user's connection from continued unauthorised access. These methods are discussed in **Section 4.3**.

4.3 Providing remedial assistance to affected users

Once a compromised connection is detected and the affected user(s) are notified, ISPs are encouraged to provide remedial assistance. There is a range of remedial tools and services ISPs may deploy to assist affected users including:

- clear instructions on how to repair compromised computers manually;
- directing affected users to an anti-virus and/or security software vendor website;
- providing software specifically developed to assist with repairing compromised computers, often referred to as 'first-aid kits'; and
- onsite support.

There are a variety of channels for providing remedial assistance to users; for instance, ISPs may contact affected users by email, phone or mail. However, the contact method selected will depend on the cost and effectiveness of each method for informing users of the most effective remedial tools and services.

Websites represent a cost effective and efficient method. Websites can be used to guide numerous affected users on how to resolve a range of cyber security issues. Websites can also be used to simultaneously raise consumer awareness because they are publicly available.

ISPs may also choose to quarantine the affected user's connection by restricting Internet access through a walled garden. A walled garden limits an affected user's Internet access and online services to:

- prevent any infection spreading to other users; and
- direct the affected user to specific content which could assist in resolving the compromised connection. This may include links to anti-virus software vendors' websites, links to relevant material on the ISP's own website, or access to an instant messaging service with technical support staff.

Tips for remedial tools and services:

Accessibility for users
In their first contact with the affected user, ISPs should list the actions a user may take. This may include directing them to a website with suggested steps to restore their connection, which can somewhat reduce the burden on ISPs' customer support.

Usability
The consumer tools and services recommended or provided by ISPs should be easy for users with various levels of computer skills to use. Providing software that does not need an installation process would be preferable for novice users. By simplifying the remedial process, ISPs may reduce unnecessary complaints or inquiries from affected users.

Complementary role to anti-virus software
If ISPs provide proprietary software tools as a "first-aid kit" for customers, it should complement anti-virus software. The first-aid kits may focus on newly found malware.

Tracking user behaviours
If remedial procedures require user action, ISPs may track the user's behaviour; this is possible if ISPs provide remedial software as part of the process. ISPs can collect feedback from software to see if the user has finished the remedial procedure.

4.3.1 Other contact points for users

Affected users may also be provided with alternative contact points for assistance to resolve their compromised connection. This could include government offices, CERT/CSIRT bodies or law enforcement agencies (if criminal activity is suspected). Users may be informed of these contact points by ISPs or the agency responsible for the code.

4.4 Building ISPs' customer support capabilities

ISP customer support staff are often the first contact points for users and therefore, could be the first to notice unusual events or incidents. However, if they do not have enough knowledge or experience on cyber security issues or incidents and they lack effective means to collect information in real time then ISPs may miss the early signs that would otherwise be available from their own customers. This could lead to the avoidable spread of malware within an ISP's network.

Therefore, the education and training of customer support staff is an important issue for ISPs. Moreover, larger ISPs have experience and expertise on information security issues and should be encouraged to assist small and medium sized ISPs to build their cyber security capabilities. This partnership should be encouraged through the code and would strengthen the capabilities of the industry as a whole and reduce the number of attacks to be remedied.

Relevant initiatives in the United States, Japan and Australia to counter cyber threats have been attached at **Appendix E, F and G** respectively.

5.0 IMPLEMENTING A CODE OF PRACTICE

5.1 Launching the Code

The launch of the code should also be planned carefully to ensure that it achieves maximum exposure and commitment. Depending on the domestic ISP market structure, it is advisable to wait until a substantial number of ISPs or most of the major ISPs have registered for the code and have satisfactorily prepared for its implementation before launching the code. Once satisfied that the code can be successfully implemented and that there is firm industry support, the timing for when the code will come into effect should be established in the text of the code itself.

To increase industry and public interest in the code of practice, a media strategy should be developed by the responsible agency. The involvement of the relevant Minister in the launch the code is reliable method of attracting media attention, and so it is advisable to consult the relevant regulatory authority or Ministry prior to the launch. Other domestic cybersecurity activities, including events such as an annual cybersecurity awareness day/week, should be considered as platforms for announcing the commencement of a code of practice.

5.2 Managing and regulating the Code

Following the launch of a code of practice, supporting mechanisms should be established. For example, the responsible agency could consider setting benchmarks for ISPs participating in the code. The benchmark should relate to how well the ISP implements the various aspects of the code. For example:

- the average time for ISPs to identify and respond to possible cyber threats on its networks;
- the quality of remedial assistance an ISP provides; and
- how soon compromised computers are removed and returned to the network.

Scope for making future changes to the code should be incorporated into the text of the code itself. Building in this flexibility to the code will enable ISPs to either increase or decrease commitments according to whether benchmarks are being met. It also enables ISPs to respond to cyber threats that may require more specific actions and monitoring

ISPs participating in the code should be encouraged to make data available to demonstrate what actions they have taken to comply with the code. For example, detailed reports outlining the level of compromised connections identified and remedial assistance provided could be reported regularly (for example, quarterly) by participant ISPs to the appropriate industry regulator. If ISPs agree then it may be useful to make this information publicly available.

Establishing a benchmark leads to the development of a compliance register. As noted previously in **Section 2.6**, participating ISPs that comply may be able to display a Trustmark on their website and in their emails to customers. As stated in **Section 2.3**, the display of a Trustmark promotes the code, cyber security in general, and significantly for ISPs, their compliance with the code. Compliance, and therefore display of the Trustmark would be an incentive for ISPs by effectively advertising the cyber security of their networks.

5.3 Code Review

As the scope for the code of practice will change over time, either the responsible agency or the regulatory authority should review the code periodically. The review should determine whether the code is having a positive impact and whether benchmarks should be established or further refined. Depending on the level of government involvement, industry may be encouraged to invite regulators and government agencies/ministries to participate in this review and advise on new compliance measures.

The responsible agency should establish the expected timeframe for the review in the code. This timing should be set from when the code is first implemented. Beginning a review between 12 and 24 months from the code's implementation may provide a sufficient window to monitor the performance of the code.

Additionally, the review may involve ISPs reporting activity on their networks including the level of cyber threats and effectiveness of cyber security initiatives. This information then provides a useful foundation for governments to develop effective and efficient strategies for addressing cyber security issues.

5.4 Establishing a framework for cooperation and collaboration

The Internet is borderless in nature and therefore, if an ISP in one economy were to implement cyber security initiatives to address compromises on their network, the threat may persist unless further cyber security measures are implemented by other ISPs, both domestically and internationally.

Despite the highly competitive ISP environment that exists in most APEC economies, from a business perspective there is significant benefit to implementing ISP cyber security initiatives simultaneously across the sector. Therefore, the existence of a separate coordinating body is likely to be very useful in the effective implementation of a code.

A coordinating body would be responsible for encouraging, initiating and managing industry-wide collaboration on cyber security. While the coordinating body may be the same as the responsible agency, it would be advantageous to have a separate entity which may be filled by regulators, Ministries, industry bodies or an independent ombudsman. Having members from the broader telecommunications sector would allow the coordinating body to serve as a valuable distribution point which may be used to deliver network information ensuring that the privacy of users is protected, and to provide updates on other cyber security strategies deployed overseas and new remedial services and tools for ISPs.

In addition, international coordination is also encouraged. International collaboration is essential for countering cyber threats and in monitoring future trends. In November 2005, Senior Officials endorsed the *APEC Strategy to ensure Trusted, Secure and Sustainable Online Environment* which expands APEC's work on promoting information and network security, harmonizing frameworks for securing transactions and communications, and combating cybercrime. This strategy strongly encourages close collaboration with the private sector and with other international organizations. Therefore, economies should take advantage of opportunities to enhance international coordination through international forums such as the APEC TEL or through bilateral engagement.

Example – Standardised Information for Customers

The information below is to be included in information provided by the ISP or on the resource created by the Australian Internet Industry Association (that ISPs can link to)

1. Internet security is an ongoing challenge – but it is a challenge that must be met if you are to enjoy a safer and more secure online experience. As Internet users, we are all required to play our part in promoting and practising a "culture of cyber security".
2. The Internet Industry Association recommends that the following top tips be taken to help ensure that your computer stays adequately protected for a safer and more secure online experience:
    - Take action immediately if you suspect your computer has been compromised. Report unauthorised access to the police. Change your passwords immediately and contact your bank if you suspect personal financial information has been stolen.
    - Keep your anti-virus and other security software updated.
    - Install a firewall to prevent unauthorised access to your computer.
    - Turn on automatic updates so that all your software receives the latest fixes.
    - Get a stronger password and change it regularly.
    - Stop and think before you click on links or attachments. Don't open suspicious emails or attachments from unknown sources. Don't click on links in emails requesting your personal details.
    - Check your "sent items" file or "outgoing" email. If you find unknown messages in your out box, it is a sign that your computer may be infected with spyware, and may be part of a botnet. This isn't foolproof: many spammers have learned to hide their unauthorised access.
    - Stop and think before you share any personal or financial information about yourself, your friends or family online.
    - Configure your wireless network securely. If you are using a wireless router/modem, enable the security features with a strong password. Use WPA or WPA2 encryption on your Wi-Fi equipment (WEP is an older standard and is less secure). Refer to your router/modem manual or contact your ISP for further details.
    - Know what your children are doing online. Make sure they know how to stay safe and encourage them to report anything suspicious. For further information about online safety go to the Australian Government's Cybersafety website: www.cybersmart.gov.au

3. More Information and tools for ongoing security

3.1 Learn more about securing your computer at www.esec.iia.net.au. This site offers practical tips from the Internet industry to help guard against Internet fraud, computer security, and the protection of personal information. This site also provides information about recommended products and services to help ensure ongoing protection.

3.2 In addition, the Australian Government undertakes a range of awareness raising initiatives including:

- The Australian Government's cyber security website www.staysmartonline.gov.au
- The Stay Smart Online email alert service.
- An annual National Cyber-security Awareness Week.
- The Budd:e cyber security education package for Australian schools. The Package consists of two self-learning, interactive modules, one for year 3 and one for year 9 students. The modules are available online or on CD ROM and can be ordered online.

Visit www.staysmartonline.gov.au for more details about these initiatives.

3.3 The Australian Communications and Media Authority is a statutory body responsible for the regulation of broadcasting, the Internet, radiocommunications and telecommunications.

The ACMA operates a range of cybersafety and cyber security education and awareness programs designed for children, parents and teachers. To learn more about these programs visit www.cybersmart.gov.au.

Case Study: The United States

FCC Advisory Council

In March, 2009, the FCC chartered a Communications Security, Reliability and Interoperability Council (CSRIC).[1] The CSRIC is one of several Advisory Committees which provide expert advice to the FCC on complex communications issues.[2] Members of the CSRIC were selected from among public safety agencies, consumer or community organizations or other non-profit entities, and the private sector. The CSRIC's mission was to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. In December 2010, the CSRIC issued its final report to the FCC[3]. That report included Internet Service Provider (ISP) Network Protection Practices, with a focus on bots and botnets. According to the report:

- The Working Group examined potentially relevant existing Best Practices (BPs), and in consultation with industry and other experts in the field, identified additional Best Practices to address this growing problem.

- The Working Group identified 24 Best Practices to address protection for end-users as well as the network. The Best Practices, set out in the report, are organized into the logical steps required to address botnets. The first step is Prevention (12 BPs), followed by Detection (5 BPs), Notification (2 BPs), and then Mitigation (3 BPs). In addition, 2 BPs on Privacy Considerations were identified to address the handling of customer information in botnet response. The BPs identified are primarily for use by ISPs that provide service to consumer end-users on residential broadband networks but may apply to other end-users and networks as well.

- Industry participants are encouraged to have their respective subject matter experts review these Best Practices for applicability. It is critical to note that Best Practices in general are not applicable in every situation because of multiple factors, and such a caveat applies to the work product of the Working Group. Therefore, the Best Practices set out are intended to be voluntary in nature for ISPs, and may not apply in all contexts (and thus for a host of reasons should not be made mandatory). With this understanding, the Working Group recommended that the Best Practices be implemented by ISPs, where applicable, in order to address the growing botnet problem in consumer end-user devices and ISP networks.

[1] www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf

[2] The CSRIC was established pursuant to the Federal Advisory Committee Act (FACA). The Federal Advisory Committee Act was enacted in 1972 to ensure that advice by the various advisory committees formed over the years is objective and accessible to the public.

[3] www.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf

Case Study: New Zealand

NetSafe

NetSafe serves as an instructive model for collaboration between industry, government and civil society. NetSafe is an organisation that promotes a confident, safe and responsible use of cyberspace. NetSafe is a multi-stakeholder partnership which represents a range of perspectives from New Zealand's cybersafety community. This partnership includes members from the information technology and telecommunications industry and works with a range of other sectors and groups including government, education, legal, community groups and law enforcement.

NetSafe is not affiliated with any organisation or company and offers free, unbiased education and advice. NetSafe has education program targeting individuals, organisations, and industry on a range of cybersafety issues.

NetSafe's ongoing work is primarily made possible by financial support from the Ministry of Education and InternetNZ with support from a range of partners on a project by project basis.

The main cybersecurity resources produced by NetSafe are the multi-award winning and Webby nominated *NetBasics*, *Whatsit*, *the Scam Machine*, and the *ORB*.

NetBasics (www.netbasics.org.nz) is a series of short animated stories supported by character information and computer security advice. It was launched in April 2008 and targeted home personal computer users but is also used in secondary education. The site is structured around the following seven point security strategy:

1. Keep all software up to date
2. Use security (anti-virus and anti-spyware) software
3. Maintain a firewall
4. Backup your data
5. Be careful what you download
6. Be on the lookout for online trickery
7. Use and protect a strong password

The stories deliberately intermingle different aspects of the security equation in an attempt to more accurately reflect the complexity of managing and maintaining computer security. The fun style of the animations was chosen to appeal to a broad audience who may not otherwise proactively consider computer security.

Whatsit (www.thewhatsit.org.nz) is an online Policy builder for Small Businesses supported by a series of educative videos. Whatsit was created in response to concerns from Small Business owners that they did feel in control of their ICT assets. This presented a barrier to further investment in ICT and the potential productivity gains that may be delivered.

The Whatsit supports Small Business owners and managers through the production of a 17 point ICT use policy without requiring any existing ICT expertise. There are 17 videos outlining the rationale of each facet of the policy which help explain the reasons for restrictions and controls. The system can provide feedback to managers as to which staff have watched the videos.

The Scam Machine (www.scammachine.org.nz) was created to give people an opportunity to experience scams without actually being scammed. Users of the site can upload names and pictures of their friends that the system embeds into a mock news story about a scam. The stories are humorous but present a range of scam scenarios that are consistent with current common scams.

The person producing the scam story is also exposed to some covert education as they make decisions about what sort of scam the story will include and what its “hook” will be.

The ORB, or online reporting button (www.theorb.org.nz), is an initiative developed in collaboration between New Zealand’s online crime and offence enforcement agencies. The ORB provides a single place for New Zealanders wishing to report cyber crimes and offences. Reports are diverted to the relevant agencies where possible, by the system’s decision-making algorithm and if not, by members of the NetSafe staff.

These resources are further supported by:

- The www.hectorsworld.com animations that provide early school aged (5-7 year old) children introductions to base level cybersafety and cybersecurity concepts.
- The www.inmyday.org.nz website for parents of digital children that compares young people’s digital lives and challenges to similar pre-digital activities and challenges.

Case Study: Shadowserver Foundation

The Shadowserver Foundation is an all volunteer watchdog group of security professionals that gather, track, and report on malware, botnet activity, and electronic fraud. It is the mission of the Shadowserver Foundation to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware.

The Shadowserver Foundation is responsible for:

- capturing and receiving malicious software, or information related to compromised devices;
- disassembling, sandboxing, and analysing viruses and Trojans;
- monitoring and reporting on malicious attackers;
- tracking and reporting on botnet activities;
- disseminating cyber threat information; and
- coordinating incident response.

The Shadowserver Foundation works alongside other security agencies to develop strategies against the threats and to form action plans to help mitigate the threats as they develop.

Shadowserver volunteers do not receive any compensation from the Shadowserver Foundation for their work or efforts. Shadowserver is an independent organisation managed and operated solely by its members under the direction of an executive team. All initiatives and execution of its process is initiated and carried out by the Shadowserver members.

Further information about the organisation is available at www.shadowserver.org

Case Study: United States

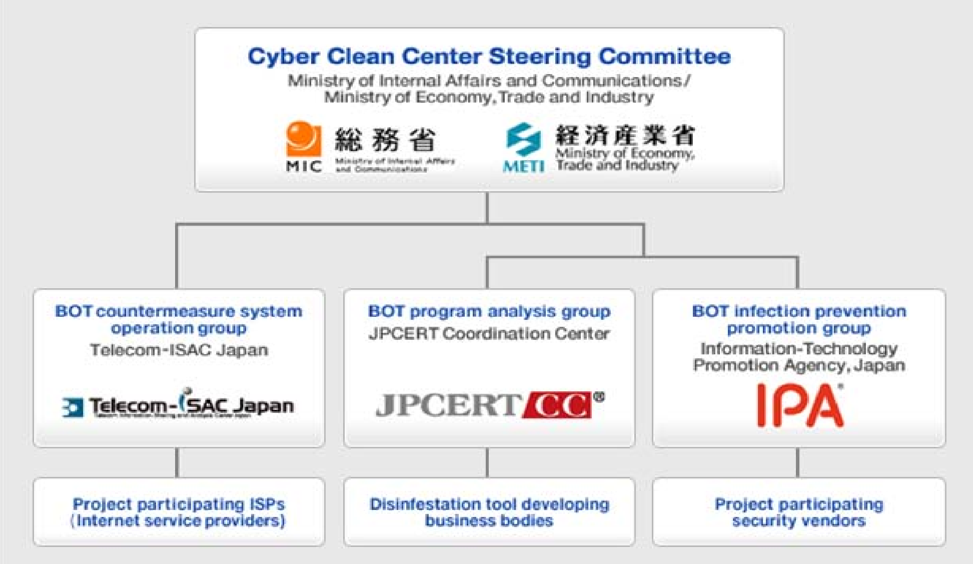
Comcast

In October 8, 2009 a commercial Internet service provider, Comcast, announced a security program designed to help protect its customers from bots, viruses and other online threats. Called “Constant Guard,” the program saw the creation of a security web portal of consumer resources to protect customers from increasingly sophisticated online security threats. The service was rolled out to all its US customers by September 2009. Comcast can detect traffic between its customer’s computers and known botnet control servers. They initially email customers with potentially infected machines, and then direct them to the company's Constant Guard Web site via an in-browser alert, where they can get instructions on how to clean up their computer, including the option of downloading Norton Security Suite for free.

Case Study: Japan

Cyber Clean Center project

The CCC project was established as part of a joint project by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) in fiscal year 2006 with the intention of reducing the number of botnet-infected computers to as close to zero as possible. The CCC project engages in anti-botnet activity by warning users in collaboration with ISPs. Participants include the Japanese Telecom Information Sharing and Analysis Center (Telecom-ISAC), the Japanese CERT and the Information technology Promotion Agency (IPA). These participants work under different branches of the CCC and dedicated to specific actions: the Bot Countermeasure System Operations Group; the Bot Program Analysis Group; and the Bot Infection Prevention Promotion Group.


Cyber Clean Center Steering Committee
Ministry of Internal Affairs and Communications/
Ministry of Economy, Trade and Industry
総務省
MIC
経済産業省
Ministry of Economy, Trade and Industry
METI
BOT countermeasure system operation group
Telecom-ISAC Japan
Telecom-ISAC Japan
BOT program analysis group
JPCERT Coordination Center
JPCERT CC
BOT infection prevention promotion group
Information-Technology Promotion Agency, Japan
IPA
Project participating ISPs (Internet service providers)
Disinfestation tool developing business bodies
Project participating security vendors

Bot Countermeasure System Operations Group – operates the main systems of the project, including the honeypot and warning system, to collect and analyse bots and notify users of bot-infected computers through the ISPs participating in the CCC project. This group collaborates with security vendors to stay updated on current malware trends.

Bot Program Analysis Group – analyses the characteristics and technology of the bot samples. This analysis group works with disinfection tool developers to provide the CCC Cleaner to affected users. The group also studies effective analysis methods and cooperates with security vendors to develop countermeasure technologies.

Bot Infection Prevention Promotion Group – maintains bot samples and provides these to security vendors for their updates. This allows affected users to remove new bots before they spread.

You can find a variety of useful ideas and tips based on the experiences of the CCC project in the following report:

www.ccc.go.jp/en_report/Report_on_the_activities_of_the_Cyber_Clean_Center.pdf

Case Study: Australia

The Australian Internet Security Initiative and the Internet Industry Association's iCode

In June 2010, the Internet Industry Association of Australia (IIA) launched a voluntary ISP code of practice, the 'icode', aimed to promote a security culture among the Internet industry by reducing the number of compromised computers in Australia. The icode is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks.

The icode encourages all Australian ISPs to participate in the AISI and to take steps to respond to data contained in the AISI reports. It can be accessed at: iia.net.au/images/resources/pdf/icode-v1.pdf, and the icode website is located at www.icode.net.au

The **icode builds upon the** Australian Internet Security Initiative (AISI) which commenced as a pilot in 2005 and received Government funding in 2007 for further expansion and development.

Six Australian ISPs participated in the 2005 pilot— the AISI has since expanded and is estimated to now cover over 90 per cent of the Australian IP address space, with 95 Australian ISPs currently participating. The AISI is a voluntary program.

The AISI software was developed in-house by Australian Communications and Media Authority (ACMA) staff utilising open source applications and components. The source code for the AISI is continually updated to accommodate evolving data sources and botnet developments.

General information on the AISI

The ACMA developed the AISI to help address the problem of compromised computers (sometimes referred to as 'zombies', 'bots' or 'drones')—computers that have become compromised through the surreptitious installation of malicious software (malware) that enables them to be controlled remotely for illegal and harmful activities.

While most anti-bot initiatives focus on combating 'botnets' (aggregations of compromised computers) by disabling their command and control centres, the AISI is focused on home and small business Internet users whose computers are surreptitiously hijacked to send spam or steal personal information and login credentials. Most of these users are connected to the Internet via broadband services.

Through the AISI, the ACMA collects data from various sources about computers that are exhibiting 'bot' behaviour on the Australian Internet. Using this data, the ACMA provides daily reports to ISPs identifying IP addresses on their networks that have been reported in the previous 24-hour period. The currency of the data is an important part of the initiative as it is based on evidence of a recent infection that is highly likely to be still occurring when the ISP contacts the customer.

The reports are provided in a plain text format that is easily parseable, including information on the IP address, timestamp and type of compromise identified. The IP address and timestamp enables ISPs to identify the customer associated with the compromise at a given point in time.

When an AISI report is received, ISPs are expected to contact their customers to advise them that their computer appears to be compromised, and to provide them with information to assist them in addressing the problem. ISPs currently participating in the AISI have informed the ACMA that when contacted, their customers are generally unaware their computer has been compromised and are grateful that their ISP has informed them of their malware infection.

Benefits of participation in the AISI

Participating in the AISI allows ISPs to assist their customers through providing them with advice that their computer appears to be compromised, thereby giving them the opportunity to remove the malware infection. Participation also contributes to the overall security of the Internet through disinfecting Australian computers that damage this security. The problems associated with compromised computers and botnets are many and varied; including:

- **identity theft**: the malware installed on the customer's computer potentially may extract personal information, such as Internet banking passwords and login information, for criminal usage;
- **distributed denial of service (DDoS)** attacks on websites, which may render the website inoperable during the attack;
- **dissemination of spam:** approximately 90 per cent of spam is sent from compromised computers;
- **dissemination of malware,** which is either embedded in the spam sent from botnets, or through directing spam email recipients to websites where malware is downloaded onto their computer; and
- **hosting of illegal content** on a compromised computer**,** such as child pornography.

Through participating in the AISI, ISPs contribute to the overall reduction of spam and e-security compromises, thereby reducing costs for all ISPs and Internet users.

Recommended information for ISPs to provide to their customers about a compromise

It is recommended that when ISPs contact their customers they advise them:

- that their computer appears to be compromised, with information on how such compromises can occur and the potential consequences of not addressing the compromise;
- that to protect others and to avoid network disturbance they need to rectify the problem as soon as possible;
- of the steps they may take to fix their current problem; and
- of the steps they may take to help secure their computer for the future (e.g. firewall, anti-virus software, regular security patches).

General information on how to prevent and respond to malware infections is provided at www.staysmartonline.gov.au