Supplementary Submission No. 32.1

symantec.

SYMANTEC'S SUBMISSION TO THE HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON COMMUNICATIONS, AUSTRALIA

ADDITIONAL QUESTIONS FOR INQUIRY INTO CYBERCRIME

1. Symantec welcomes the opportunity offered by the House of Representatives Standing Committee to submit our response to the question on notice taken at the public hearing and the two additional questions seeking further elaboration on the points raised in our submission.

CYBERCRIME LEGISLATION – GAPS & RECOMMENDATIONS

Question taken on notice:
Can you identify some of the gaps in the Australian legislation to protect against cybercrime?

2. In our first submission, we had elaborated on the threat landscape particularly how cybercriminals are shifting their tactics towards web-based stealthier attacks; how the underground economy has become a sophisticated market for stolen digital goods and malicious toolkits; and how many computers are being used as botnets through which such cyber attacks and digital thefts are committed.

3. Moreover, cybercrime is a global phenomenon whereby attacks can easily be orchestrated by blackhats based overseas through computers and bots not located within a single geographical boundary. Malicious programs are distributed globally via the Internet through multiple channels like spam emails, malicious or compromised websites, IM, etc. A professionalised underground economy also means that stolen goods and malicious toolkits are distributed and sold across national boundaries.

4. It is therefore critical that the international community acts collaboratively to apprehend and bring to justice cybercriminals. This can only be effective if there is greater harmonisation in cybercrime laws across the various jurisdictions, be it federal, state or local legislation. As a collective effort, all countries should strengthen their national cyber laws and bring them to internationally acceptable standards such as the Council of Europe Convention of Cybercrime (Cybercrime Convention) in order to sufficiently deter and punish cybercriminals. In the same way, federal governments should recognise the importance of having harmonised legislation within the country, in order for minimum standards of cybercrime enforcement to be uniformly applied across the nation.

5. In this context, Australia has gone a long way in establishing and refining its cyber laws. Computer offenses are addressed in Part 10.7 of Australia's Federal Criminal

Code Act of 1995 broadly in line with the provisions found in the Cybercrime Convention, while the various state and territorial laws are similar to their federal counterpart. Data privacy is also protected under Australia's Federal Privacy Act, which is undergoing review, and the various state and territorial laws regarding personal information protection. Other pieces of legislation like the Spam Act further protect citizens from the spam and other cyber-related ill-effects.

6. Nevertheless, given the rapid developments in the threat landscape, Australia's legislation could be further amended, while incorporating adequate safeguards, in several respects to increase its effectiveness in fighting computer crimes.

a. **Need to strengthen criminal procedural elements of the Criminal Code Act in order to facilitate investigation and enforcement of computer offences subject to adequate safeguards**. For instance, while the Criminal Code Act contains some procedural measures of law enforcement like remote search and seizure of digital evidence, it does not appear to empower authorities to order or obtain the expeditious preservation of specified computer data or traffic data for a period of time, as contained in the Cybercrime Convention. The ability to collect, analyse and present to the courts accurate, reliable and sufficient data is critical for cyber forensics purposes.

b. **Need to clarify the relevant provisions of the Criminal Code Act to criminalise the intentional and illegal possession, usage, or distribution of devices, including malicious programs, designed or adapted primarily with the intention of committing cyber offences**. The Criminal Code Act makes illegal the possession, control, production, distribution or obtention of data with intent to commit a computer offence. However, it could be further clarified that "data" would include malicious devices and tools/toolkits. In addition, there is a need to ensure that the suppliers of legitimate software are not inadvertently committing offences by such provisions when using tools/devices for legitimate business purposes, e.g. conducting research, penetration testing, and/or supplying patches for vulnerabilities. Factors to consider include whether the device has been developed primarily, deliberately and for the sole purpose of committing an offence; whether the device is available on a wide scale commercial basis and sold through legitimate channels; whether the device is widely used for legitimate purposes with a substantial installation base; and the context in which the device was used to commit the offence compared with its original intended purpose.

c. **Need to strengthen the relevant provisions of the Criminal Code Act to address the computer-related identity thefts in particular the growing underground economy dealing with such stolen identities**. The current legislation criminalises the possession, control, production, distribution or obtention of data with intent to commit a computer offence, and contains related provisions on obtaining properties through fraud, forgery and deception as well as proceeds of crime. While these provisions would address identity-targeting tactics like phishing and spyware, it is not clear if these provisions also address the purchasing, selling or offering for sale of data, be it stolen identities or identities obtained otherwise. We note that new legal provisions via the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008[1] are being proposed to plug existing holes in the law relating to identity fraud, i.e. assuming or stealing another person's identity. Symantec supports these initiatives, which will go a long way in combating identity crimes.

d. **Need to explore new provisions supporting stronger cooperation between the relevant authorities and ISPs.** Internet hosting services are a critical piece of the underground economy's IT infrastructure. Cybercriminals use them to host command and control servers of botnets, as well as phishing sites. Better cooperation between authorities and ISPs is critical, which could be achieved through better information-sharing on possible bot/phishing sites, clearer procedures by which positively identified sites would be taken down, higher security standards of ISPs, 'safe harbor' provisions absolving ISPs from liabilities in taking actions against suspected/confirmed bot or phishing activities, and penalties if they were knowingly facilitating the hosting of botnets or phishing sites.

e. **Need to include data breach notification in legislative framework**. Recent data breaches have been shown to compromise large amounts of personal data, and such data could be easily used for criminal purposes, for example targeted phishing attacks, credit card fraud, fraudulent impersonation, etc. Timely notification of data breaches with potential risk of significant harm, would give affected individuals more time to take mitigating actions to protect their assets. Having a mandatory notification mechanism in place would also lead to greater awareness amongst individuals and businesses on the importance of protecting confidential information.

7. Even with strong legislation, it is extremely difficult to prevent or mitigate the various types of cyber attacks or cyber crimes. Countering botnets is a challenging task given the new ways in which cyber criminals configure their command-and-

[1] On 23 February 2009 the House of Representatives passed the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008. Now with the Senate, the Bill inserts three new identity crime offences into new Part 9.5 of the Criminal Code criminalising the dealing (i.e. making, supplying, using) of identification information; the possession of identification information, and the possession of equipment used to make identification documentation, if the intention is to impersonate another person to commit or facilitate the commission of an offence.

control systems to evade detection and shutdowns[2]. As the underground economy continues to grow, legislation coupled with enforcement efforts will deter but not completely prevent malwares, toolkits and stolen information from being transacted and sold across borders. It is therefore critical that each individual and organisation adopts the appropriate administrative, procedural and technological measures to protect their information, systems and networks from cyber criminals.

EARLY WARNING SYSTEMS

Question on Early Warning Systems:
Symantec's submission identifies the need for an early warning intelligence collection and security response capability.

a. *Do you see a role for a combined public/private centre that has the capacity to aggregate intelligence data; develop anti-malware or other technical responses; and support strategic prosecutions?*
b. *What types of actors should be involved in a national centre of this type?*
c. *Are you aware of the Japanese Clean Computers Centre and program?*
d. *If so, do you have comment to make on the efficacy of the Japanese model?*

8. Developing strong national early warning and incident response capabilities is critical to any national cyber security strategy. Many countries have already developed certain capabilities in providing advice and technical assistance on computer security incidents, to various communities like government agencies, defence agencies, general public, as well as sectors designated as critical as part of their national critical infrastructure protection strategies. Some more advanced countries are also undertaking important initiatives to strengthen coordination and better leverage resources between different agencies leading these capabilities, for instance the new National Cybersecurity and Communications Integration Center (NCCIC) [3] in the U.S., and the Cyber Security Operations Centre (CSOC) under the first Cyber Security Strategy of the U.K. government.

9. In this respect, Australia has gone a long way toward developing early warning and incident response capabilities. Currently, these capabilities are being delivered through organisations like AusCERT, the Australian Government Computer Emergency Response Team, and the Defence Signal Directorate (DSD). The Australian government has also recently announced plans to create, in collaboration

[2] http://four.cs.uni-bonn.de/fileadmin/user_upload/werner/papers/proactive-botnet-countermeasures.pdf

[3] The NCCIC consolidates the US' cyber and communications operations centers and provides an integrated incident response facility to mitigate risks that could disrupt or degrade critical information technology functions and services, while allowing for flexibility in handling traditional voice and more modern data networks.
http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm
http://gcn.com/Articles/2009/10/30/DHS-new-national-cybersecurity-operations-center.aspx?p=1

with AusCERT, a new national Computer Emergency Response Team (CERT)[4] operational in early 2010 to complement the work of the new Cyber Security Operations Centre (CSOC) to be established within the DSD[5].

10. The private sector has an important role to play in these initiatives. First and foremost, the private sector information security experts and companies are an important source of expertise and knowledge in terms of cyber security policies, methodologies, operations and technologies. Global information security companies like Symantec also possess a rich repository of real-time cyber threat intelligence data. For example, Symantec possesses a Global Intelligence Network consisting of more than 240,000 sensors deployed in over 200 countries monitoring attack activities; gathers malicious code intelligence from more than 130 million client, server, and gateway systems; captures spam and phishing data from more than 2.5 million decoy accounts in the Symantec Probe Network; and processes over 8 billion email messages and over 1 billion Web requests per day across 16 major data centers. Such expertise and knowledge would be extremely difficult for the government alone to replicate or develop.

11. The private sector also controls many critical resources, particularly owners and operators of critical information infrastructure. The telecommunications and Internet service providers are especially important players, as they control the national Internet infrastructure through which cyber attacks like DDoS attacks can take place and on which whole bot-armies are hosted. The majority of a nation's critical infrastructure - utilities, finance, transport, healthcare, etc – owned or operated by private hands are also becoming reliant on IT and the Internet, and many are being exposed to the same vulnerabilities as corporate systems. A government needs to pro-actively develop a trusted long-term relationship with these private sector players and encourage them to participate in the national efforts to secure the Internet.

12. Organisations like the new national CERT and the new CSOC are therefore welcome developments toward achieving better early warning and incident response capabilities. While such centres need not be co-owned by the public and private sector, the participation of the information security industry and owners/operators of critical infrastructure is paramount. They could work with the information security industry to:

[4] The new CERT aims to provide citizens with access to information on cyber threats, vulnerabilities in their systems, and information on how to better protect their information technology environment.

[5] The establishment of CSOC under the DSD was announced in the Defence White Paper 2009, and will comprise staffed from agencies including the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO), and the Attorney-General's Department.

a. Obtain accurate and real-time global intelligence on vulnerabilities, malwares and other cyber threats. These could include attack, vulnerability and malicious code intelligence; phishing, spam, data leakage, spyware, adware and virus intelligence; underground cyber economies and honeypot network intelligence; and other related analysis and reports;

b. Develop accurate and real-time local intelligence through information-sharing or deploying sensors in the IT infrastructure taking into account the specific operating environments within critical sectors or within the companies of these sectors;

c. Enhance deep cyber threat analysis capabilities to identify and detect critical security events based on deep analysis and automated correlation of the millions of log data collected, that the affected community should act upon; and

d. Develop counter-attack or mitigating measures to manage actual cyber security incidents, which may include developing anti-virus signatures or even anti-virus toolkits, providing expert advice to affected organisations on how to contain the attacks, or working with telecommunications and/or Internet service providers to mitigate DDoS attacks.

13. On the specific topic of the Japan Cyber Clean Center (CCC)[6], Symantec is one of the security vendors, together with other major security vendors, participating in the program. Set up in 2006, the CCC initiative analyses bot characteristics, provides information on bot-infestation, promotes bot cleaning and prevention amongst Internet users in Japan. A cooperative effort between the Japan government with ISPs and security vendors, it functions along a five-step process whereby bot-malware samples are collected; 'cleaners' (or anti-malware tools) are developed; infected users are identified and instructed to 'clean' their computers; 'cleaners' are downloaded by users; and the bot-malware samples are sent to participating security vendors for creation of malware signatures.

14. According to Japan's CCC FY2008 report[7], the project has been described to have accomplished "concrete results" and gained "wide acceptance", although the number of bot infections still remained large and further effort was needed to clean up infected computers. A clearer understanding of the nature of bot infections within the local environment also seems to have been developed. An initiative like the CCC could lead to better situational awareness of the local bot landscape, more proactive remediation of end-users' bot-infected computers and increased public

[6] https://www.ccc.go.jp/en_ccc/index.html

[7] https://www.ccc.go.jp/en_report/h20ccc_en_report.pdf

awareness. However it is important for individual governments to carefully examine and address all relevant aspects including potential concerns over privacy and expected support from ISPs, before implementing such a regime in their respective environments.

15. It is also important to note that Japan's CCC FY2008 report concluded that although no measures can provide full immunity from bot infection, individuals could minimise the risk by adopting minimal countermeasures like keeping computer software up-to-date, installing antivirus software, using personal firewalls, using broadband routers for connection to the Internet, not previewing emails in HTML format, paying careful attention to emails with attached files, and using strong IDs and passwords. As mentioned in paragraph 7, efforts to clean up botnets and criminalise cybercrimes can only go so far, hence putting in place such minimal preventative measures is an important step in stopping cybercriminals in their tracks.

PUBLIC PRIVATE COOPERATION

<u>Question on Public Private Cooperation</u>:
Symantec's submission suggests that the Australian Government should improve cooperation and get better leverage from existing public-private partnerships:

a. Can you tell the committee what barriers currently exist that prevent optimum cooperation between the public and private sectors?
b. Are there specific examples of partnerships that could be strengthened through better cooperation?
c. Is Symantec part of the Trusted Security Information Network?
d. If so, do you have any comments on the operation of the Network or suggestions on how the Network might be strengthened?

16. Trust, time and resources are examples of barriers between the public and private sector. For instance, information-sharing between the government and owners/operators of critical information infrastructures is a core, yet extremely difficult, component of a national cyber security strategy.

17. In Australia, Symantec has been involved in the earlier work of the Trusted Information Sharing Network (TISN) as part of the IT Security Expert Advisory Group providing strategic advice on IT elements of Australia's critical infrastructure. We continue to seek further engagement in the TISN's work going forward.

18. Having early knowledge and actual incidents of cyber strikes occurring within each sector, would help the sector to better understand any impending threats and defend against cyber attacks. However, private sector members may not be sure how information, if shared, might be used against them by the government or by

competitors. Members may also see limited value in investing time and effort in participating in such initiatives without getting commensurate benefits. Several major questions need to be addressed:

a. To what extent will the authorities be involved in monitoring privately owned and operated infrastructures? What is the role and intention of the authorities in requesting that information be shared? What does the authority intend to do to/with the members upon examining the data?

b. If information is to be shared, who should it be shared with – should it be the authority responsible for national security or the sectoral regulator? While the former may not have sufficient operational and technical expertise within that sector to be able to effectively use that information, the regulatory agency may also not be willing to undertake the responsibility and be ultimately held accountable for security within the sector.

c. What are the legal issues - including privacy and liability – that would impede information sharing between the government and private sector members? Would information shared expose them to liability, punishment, or other negative consequences, for example if the regulator decides on taking enforcement actions on the sharing party or if the information is somehow misused by other sector members?

d. Given the sensitivity of the data shared, where would the information be housed and will it be adequately safeguarded?

e. What is the value of providing information to the authority and other sector members? Why should a member offer potentially sensitive information if it is not receiving relevant and actionable intelligence or even exclusive intelligence not obtainable from other sources in return?

f. As requirements of the members may differ within the sector and across sectors, would any alerts and advisories be customised to their specific needs or the needs of their sector?

g. Would there be equally strong long-term commitment from other sectoral members to share information? If there is no corresponding advantage in being proactive in sharing, why should one be actively sharing information for the benefit of others?

19. Other factors like costs, impact on operations, and privacy are also issues that need to be tackled. Private sector members may be concerned about government imposing unnecessary costs and hampering operational efficiencies in rolling out their initiatives. Telecommunications providers and ISPs, who own the Internet and mobile infrastructure, may be concerned about bandwidth being slowed down. The public, whom these members ultimately serve as their customers, may be concerned that their personal information is being monitored.

20. Information sharing within and across critical infrastructure sectors is a good example of a public-private partnership that can be enhanced through better cooperation. Several methods could be employed to build trust and provide a sufficient value proposition for private sector members to want to participate:

a. Enact legislation and regulations to assure the private sector that confidential, proprietary, and business-sensitive information submitted will remain secure and only be used for national protection efforts. Subject to prescribed requirements, the information will be protected from public disclosure and/or even regulatory action, and uniform procedures will be established for the receipt, care, and storage of information submitted. A similar structure exists in the United States via the Critical Infrastructure Information Act of 2002, and the Protected Critical Infrastructure Information (PCII) Program created under the authority of this act.

b. In the absence of or as a complement to legislative protection, formalised and enforceable data sharing or non-disclosure agreements can be developed to ensure that information provided is protected from abuse by sector members and may not be used for any other purposes. However, such agreements may still likely entail the possibility of regulatory or legal action.

c. Establish standardised structure for the exchange of information. This could include the description, categorisation, prioritisation and escalation channels of security incidents. Parts or all of the information submitted could be classified with the desired levels of confidentiality, and the corresponding levels of protection implemented accordingly. There exists several messaging standards developed for information-sharing purposes, for instance Messaging Standard for Sharing Security Information (MS3i) developed under EU funding and the National Information Exchange Model (NIEM) in the United States.

d. Establish appropriate house rules of participation in sector meetings. For instance, minimum levels of seniority could be established to generate trust and to involve decision-makers. This would allow personalised and mutual trust to be established between participants of the sector discussions. Example of such a concept is the Warning, Advice and Reporting Point (WARP) in the UK.

e. Offer to participants exclusive cyber threat intelligence information – be it sector specific threats or more generic threats - that they cannot obtain elsewhere. This may mean developing government's capabilities to analyse and anticipate cyber threats, and providing more in-depth intelligence leveraging resources within the government.

21. Another area where the government could tap on the expertise of the private sector is in the area of early warning and incident response. This aspect has been addressed in detailed in the second segment of this submission.

22. In other areas like raising public awareness, there is already quite a strong private-public partnership in place. An example is the National E-Security Week where many private sector members including Symantec have worked closely with the Australian government to develop activities and materials to raise awareness of information security issues. Such cooperation could continue to be enhanced.

23. The government could also work with the private sector in rolling out new initiatives to target specific audiences. For instance, government and security vendors could work together to offer small-and-medium businesses affordable software/service packages subsidised by the government to reduce the cost of ownership, and the government could actively promote these packages to the public. In a similar way, affordable information security training courses could be developed in partnership with industry, and made available to the public with subsidies from the government.

20th November 2009

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.
For further information, please contact either of the following:

Craig Scroggie, Vice President & Managing Director, Pacific Region, Symantec Corporation, Symantec House, Level 14, 207 Kent Street, Sydney NSW 2000 – tel. +61 2 8220 7050 / +61 423 060 136 craig_scroggie@symantec.com

Wei Ming Tan, Senior Manager of Government Relations, Asia Pacific & Japan, Symantec Asia Pacific Pte. Ltd., 6 Temasek Boulevard #11-01, Suntec Tower 4, Singapore 038986 – tel. +65 6413 4307 / +65 9623 6998 weiming_tan@symantec.com