SUBMISSION NO. 32

symantec.

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

INQUIRY INTO CYBER CRIME AND ITS IMPACT ON AUSTRALIAN CONSUMERS

1. Symantec welcomes the opportunity offered by the House of Representatives Standing Committee to submit our views on the incidence of cyber crime on consumers, with the stated Terms of Reference as follows:

   a. Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and trojans
   b. The implications of these risks on the wider economy, including the growing economic and security impact of botnets
   c. Level of understanding and awareness of e-security risks within the Australian community
   d. Measures currently deployed to mitigate e-security risks faced by Australian consumers
      i. Education initiatives
      ii. Legislative and regulatory initiatives
      iii. Cross-portfolio and inter-jurisdictional coordination
      iv. International co-operation
   e. Future initiatives that will further mitigate the e-security risks to Australian internet users
   f. Emerging technologies to combat these risks

NATURE AND PREVALENCE OF E-SECURITY RISKS INCLUDING FINANCIAL FRAUD AND THEFT OF PERSONAL INFORMATION, INCLUDING THE IMPACT OF MALICIOUS SOFTWARE SUCH AS VIRUSES AND TROJANS

2. E-security is a complex topic and there is a wide variety of risks. These risks could include loss or theft of personal information, targeted attacks using such personal information to further compromise the user, phishing attacks to obtain passwords for financial gain, denial-of-service (DoS) attacks on corporate systems causing loss of productivity and critical data, malicious attacks on industrial control systems, and in some cases distributed denial-of-service (DDoS) attacks targeting the national information infrastructure of an entire nation as we have seen in the case of Estonia or Georgia.

3. More than ever, cyber criminals are presented with a wide range of possibilities to conduct such attacks. Widely-adopted technologies such as Instant Messaging (IM),

VoIP, P2P and Web 2.0 are increasingly attractive platforms for attacks. For example, IM, one of the most successful and widely deployed applications on the Internet, has become a potent means to propagate viruses, worms and other threats. It is also particularly well suited for social engineering tactics being as it is a tool which tends to be inherently trusted by users.

4. The ubiquity of easy-to-exploit Web application security vulnerabilities have also resulted in the prevalence of Web-based threats. Forums, photo-sharing galleries, blogs, and online shopping applications, are attractive targets for attack, and it has been shown that such Web 2.0 sites could lead to exposure of basic user profile information such as gender, political views, religious views, birthday and hometown, to be exposed if vulnerabilities remained unpatched.

5. Symantec has observed **four key trends in the threat landscape that will likely continue in the foreseeable future**:

   a. Malicious activity has increasingly become Web-based
   b. Attackers are targeting end-users instead of computers
   c. The online underground economy has consolidated and matured
   d. Attackers are able to rapidly adapt their attack activities.

6. **Web-based attacks are now the primary vector for malicious activity over the Internet.** Individual computers are increasingly targeted through the World Wide Web as attackers switch to more focused, stealthier tactics instead of trying to penetrate much stronger perimeter defenses around enterprise networks. Moreover, activities taking place on end-users' computers and/or Web sites are less likely to be detected, and the proliferation of PCs/laptops and high-speed Internet access also make these computers attractive targets of attack.

7. Reputable, high-traffic websites are being targeted in these attacks. Most Web-based attacks are launched against users who visit legitimate websites that have been compromised by attackers in order to serve malicious content. Attackers could compromise a website by exploiting vulnerabilities in the Web application or the host operating system, and then modify the pages served to users visiting the site to directly serve malicious content or redirect a user's browser to another Web server under the attacker's control. **In this way, a popular, trusted site with a large number of visitors can yield thousands of compromises from a single attack, thus providing an optimal beachhead for distributing malicious code.**

8. Patching of vulnerabilities affecting Web applications, on the other hand, remains weak. Many enterprises and end users often prioritize the patching of high-severity vulnerabilities over medium- and low-severity vulnerabilities. Computers therefore remain exposed for longer periods to medium- and low-severity vulnerabilities. However, eight of the top 10 vulnerabilities exploited in 2008 were rated as medium

severity. Additionally, in 2008 alone, there were 12,885 site-specific vulnerabilities identified and 63% of vulnerabilities documented by Symantec affected Web applications. Only 394 (3%) of these 12,885 site-specific cross-site scripting vulnerabilities are known by Symantec to have been fixed.

9. **Attackers are also moving away from targeting computers towards compromising end users for financial gain**. **Attacks are motivated less by notoriety than by economic gain using phishing scams and spyware designed to steal confidential information.** In 2008, 78% of confidential information threats exported user data, and 76% used a keystroke-logging component to steal information such as online banking account credentials. Additionally, 76% of phishing lures targeted brands in the financial services sector and this sector also had the most identities exposed due to data breaches. Similarly, 12% of all data breaches that occurred in 2008 exposed credit card information.

10. Once attackers have obtained financial information or other personal details—such as names, addresses, and government identification numbers—they frequently sell that data on the underground economy. The most popular item for sale on underground economy servers in 2008 was credit card information, accounting for 32% of the total. This is likely due to the fact that there are numerous ways for credit card information to be stolen, and that stolen card data can be easily cashed out.

11. **The underground economy has become more professionalized and commercialized**. The underground economy is geographically diverse and able to generate millions of dollars in revenue for (often) well-organized groups. It is increasingly becoming a self-sustaining system where tools are specifically developed to facilitate fraud and theft are freely bought and sold. These tools are then used for information theft that may then be converted into profit to fund the development of additional tools.

12. In fact, the coordination of specialized and, in some cases, competitive groups for the production and distribution of items such as customized malicious code and phishing kits has led to a dramatic increase in the general proliferation of malicious code. **In 2008, Symantec detected 1,656,227 malicious code threats. This represents over 60% of the approximately 2.6 million malicious code threats that Symantec has detected in total over time.** Malicious codes can be propagated through means like sharing of executables, transfer of email attachments, peer-to-peer (P2P) file-sharing, and transfer of files through HTTP, Internet relay chat (IRC) or instant messaging (IM).

13. **Malicious code developers are increasingly able to adapt their attack activity in response to security measures being implemented, and evade detection**. In some cases, this adaptability takes the form of geographic mobility, particularly in the case of attackers who may relocate their operations to seek digital safe havens or

places where security practices, cyber security legislation and/or well-secured infrastructure are inadequate. Methods of attack also change to maximize the returns for the attackers - in fact, we expect that overt attack activities will either be abandoned or pushed further underground where stealthier tactics can reap greater returns.

14. **Social engineering methods are also becoming commonplace.** Unlike the past, modern Internet users are heavily engaged in social networking sites, online music downloads, file-sharing, online gaming, etc. These are popular means to spread malicious codes, and hence malwares and attacks are designed to utilise these platforms. For instance, malicious codes like the Brisv Trojan, specifically targets multimedia files on computers and injects a malicious URL into them. Other worms like a variant of the W32.Ackanatta worm use an email purporting to be an eCard or a solicitation of a job offer to entice users, which is effective in the current downturn. Phishing attacks target an increasing pool of users using online banking services.

15. Symantec has identified a number of trends in specific areas like threat activity, vulnerabilities, malicious codes and phishing/spam attacks as listed below:

Threat Activity Trends

- The education sector accounted for 27% of data breaches that could lead to identity theft during this period, more than any other sector and a slight increase from 26% in 2007.
- The financial sector was the top sector for identities exposed in 2008, accounting for 29% of the total, an increase from 10% in 2007.
- In 2008, the theft or loss of a computer or other data-storage devices accounted for 48% of data breaches that could lead to identity theft and for 66% of the identities exposed.
- Symantec observed an average of 75,158 active bot-infected computers per day in 2008, an increase of 31% from the previous period.
- In 2008, Symantec identified 15,197 distinct new bot command-and-control servers; of these, 43% operated through Internet Relay Chat (IRC) channels and 57% used HTTP .

Vulnerability Trends

- Symantec documented 5,491 vulnerabilities in 2008; this is a 19% increase over the 4,625 vulnerabilities documented in 2007.
- Two% of vulnerabilities in 2008 were classified as high severity, 67% as medium severity, and 30% as low severity. In 2007, 4% of vulnerabilities were classified as high severity, 61% as medium severity, and 35% as low severity.
- Eighty% of documented vulnerabilities were classified as easily exploitable in 2008; this is an increase from 2007, when 74% of documented vulnerabilities were classified as easily exploitable.

- During 2008, there were 12,885 site-specific cross-site scripting vulnerabilities identified, compared to 17,697 in 2007; of the vulnerabilities identified in 2008, only 3% (394 vulnerabilities) had been fixed at the time of writing.
- In 2008, Symantec documented nine zero-day vulnerabilities, compared to 15 in 2007.
- In 2008, 95% of attacked vulnerabilities were client-side vulnerabilities and 5% were server-side vulnerabilities, compared to 93% and 7%, respectively, in 2007.

Malicious Code Trends

- In 2008, the number of new malicious code signatures increased by 265% over 2007; over 60% of all currently detected malicious code threats were detected in 2008.
- Of the top 10 new malicious code families detected in 2008, three were Trojans, three were Trojans with a back door component, two were worms, one was a worm with a back door component, and one was a worm with back door and virus components.
- In 2008, 78% of threats to confidential information exported user data and 76% had a keystroke-logging component; these are increases from 74% and 72%, respectively, in 2007.
- Propagation through executable file sharing continued to increase in 2008, accounting for 66% of malicious code that propagates—up from 44% in 2007.
- Malicious code that targets online games accounted for 10% of the volume of the top 50 potential malicious code infections, up from 7% in 2007.

Phishing and Spam Trends

- The majority of brands used in phishing attacks in 2008 were in the financial services sector, accounting for 79%, down slightly from 83% identified in 2007.
- The financial services sector accounted for the highest volume of phishing lures during this period, with 76% of the total; this is considerably higher than 2007, when the volume for financial services was 52%.
- In 2008, Symantec detected 55,389 phishing website hosts, an increase of 66% over 2007, when 33,428 phishing hosts were detected.
- Phishing website toolkits have made phishing attacks much easier and more time efficient. One prevalent phishing kit was responsible for an average of 14% of all phishing attacks during 2008, with spikes up to 26%.
- Credit card information was the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 32% of all goods and services; this is an increase from 2007 when credit card information accounted for 21% of the total.
- The most common type of spam detected in 2008 was related to Internet- or computer-related goods and services, which made up 24% of all detected spam; this was the second most common type of spam in 2007, accounting for 19% of the total.

- Symantec observed a 192% increase in spam detected across the Internet, from 119.6 billion messages in 2007 to 349.6 billion in 2008.
- In 2008, bot networks were responsible for the distribution of approximately 90% of all spam email.

16. **Australia's rankings amongst countries in the Asia Pacific & Japan region according to Symantec's Internet Security Threat Report (ISTR)** are as follows (c.f. Annex I for detailed explanation on the metrics used):

- Ranked 6th in terms of malicious activity by country/region.
- Ranked 7th in terms of bot-infected computers by country/region.
- Ranked 7th in terms of bot command-and-control servers by country/region.
- Ranked 6th in terms of top countries/regions of origin for Web-based attacks.
- Ranked 5th in terms of top countries/regions hosting phishing websites and top targeted sectors.
- Ranked 8th in terms of top countries/regions of spam origin.

THE IMPLICATIONS OF THESE RISKS ON THE WIDER ECONOMY, INCLUDING THE GROWING ECONOMIC AND SECURITY IMPACT OF BOTNETS

17. Bots and bot networks are clearly a huge problem with significant impact to the wider economy. Bots are programs that are covertly installed on a targeted system, allowing an unauthorized user to remotely control the computer for a wide variety of purposes. Attackers often coordinate large groups of bot-controlled systems, or bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks by launching coordinated attacks.

18. Symantec has seen a large increase in the number of remotely controlled bots. Symantec observed an average of 75,158 active bot-infected computers per day in 2008, an increase of 31 percent from the previous period. Symantec also identified 15,197 distinct new bot C&C servers, which are what botnet owners use to relay commands to bot-infected computers on their networks. Bot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly, which could potentially allow attackers to outpace an organization's security efforts to patch vulnerable systems.

19. **More than just a nuisance, attackers can use bots to perform a variety of tasks, such as setting up denial-of-service (DoS) attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information** from compromised computers that may be used in identity theft, all of which can have serious financial and legal consequences. **Botnets have been known to bring down an entire nation's information infrastructure**, as in the case of Estonia and Georgia.

20. Beyond networks and systems, Symantec has observed that **information itself is increasingly at risk**. Information is the lifeblood of a modern highly-informatised economy like Australia. However, personal and confidential information of individuals and businesses are now being targeted by attackers adopting stealthier tactics and newer vectors of attack especially Web-based attacks which are designed to circumvent traditional protective defenses. **Over 60% of Symantec's malicious code signatures were created in 2008, and over 90% of threats discovered in 2008 are threats to confidential information,** which allow remote access, export user data, export email addresses, log keystrokes, or export system data.

21. The economic impact of data breaches is significant. **In 2008 the average cost per incident of a data breach in the United States was $6.7 million—which is an increase of 5% from 2007—and lost business amounted to an average of $4.6 million**. This does not even include the intrinsic value of the data itself that has been lost, the financial losses incurred by the affected individuals arising from misuse of the data, or indirect costs such as undermining of confidence and damage to an organization's reputation.

22. Beyond invasion of privacy, the risk of financial losses to data subjects may be grossly underestimated. For instance, targeted attacks can easily be conducted using personal data of employees stolen from an organization. Attackers can impersonate the organization and ask these victims for sensitive information, send them email attachments containing malicious code, or redirect them to phishing sites to steal confidential information like bank accounts, usernames and passwords.

23. Organizations that store and manage large amounts of personal information are particularly susceptible. **Educational, government and health care organizations store large amounts of information that could be used for identity theft**. In 2008, the education sector represented the highest number of known data breaches that could lead to identity theft, accounting for 27% of the total. The government and healthcare sectors were ranked second and third, accounting for 20% and 15% of the total number of such breaches respectively.

24. It is important to note that most of these data breaches are not due to malicious hacking from the outside. Symantec observed that **in 2008, more than half of data breach or identity theft incidents was due to the theft or loss of computer or other medium on which data is stored or transmitted**[1]. The compact size and larger storage capability of laptops and other storage devices has drastically increased the opportunity for theft, loss, or misplacement, as well as the potential amount of

[1] In 2008, the top three causes of data breaches that could facilitate identity theft were the theft or loss of computer or other medium on which data is stored or transmitted (48%), insecure policy (21%) and hacking (17%) while the top three causes of identities exposed were theft or loss (66%), hacking (22%) and insecure policy (8%).

information breached; a single DVD disk can contain personal information on millions of people.

25. **These security concerns can also influence consumer behavior in a significant way, affecting the take-up of various Internet services like e-commerce and e-government services**. According to Gartner[2], the fact that large numbers of U.S. citizens have lost money through financial frauds in 2008, in large part because of data breaches, had an adverse effect on consumer victims' financial transaction behavior. In percentage terms, the behaviors most influenced by security concerns included online shopping and payments. Online banking also took a big hit, with 20 percent of worried consumers in the survey saying that their online banking behavior had been affected.

LEVEL OF UNDERSTANDING AND AWARENESS OF E-SECURITY RISKS WITHIN THE AUSTRALIAN COMMUNITY

26. Globally, there is a lack of awareness generally about the current level of information security threats. The level of sophistication, economic capacity and risk profile of an organization or user will generally be an indicator of level of understanding of the issue and likelihood of taking preventative action. The average consumer or Small and Medium Businesses (SMBs) are frequently the groups with the least knowledge around this issue which makes them most vulnerable, heightened to a large extent by the proliferation of "always on" broadband connectivity.

27. **A significant gap often exists between perception and reality in terms of how users protect themselves from cyber threats**. A National Cyber Security Awareness Study jointly conducted by Symantec and the National Cyber Security Alliance (NCSA) in the United States in Oct 2008[3] clearly demonstrated this:
    a. 58% of respondents lacked combination of antivirus, anti-spyware and firewall solutions, yet 83% said they felt safe or somewhat safe from hackers.
    b. 80% of respondents claimed to have a firewall, yet only 42% indeed had firewall protection.
    c. 84% of respondents were aware of phishing, yet half of the computers assessed lacked any anti-phishing or anti-spyware solutions installed.

28. Other results of the Symantec-NCSA study showed that Internet users faced a clear risk of harm in the cyber space:
    a. 26% of respondents felt that their computer was "very safe" from viruses, and only 21% said their computer was "very safe" from hacker attacks
    b. 54% of respondents have had their computer infected by a virus

[2] https://www.gartner.com/it/page.jsp?id=906312
[3] http://www.symantec.com/about/government/policyblogs/detail.jsp?prid=20081009_01

c. Almost 50% of respondents do not know how to determine if a Web site is safe before visiting it
d. 51% of respondents said they have been a victim of a phishing attempt, with 65% saying the attempt looked like a legitimate email.

29. **In Australia, a similar perception-reality gap and inadequacy in the level of security exist**, as revealed in AusCERT's Home Users Security Survey 2008[4]:
a. 37% of respondents reported that either they never automatically updated their operating system, or only sometimes updated it 'automatically'.
b. While 68% of respondents were either 'confident' or 'very confident' in managing their computer's security, 58% of them did not use any type of anti-phishing tool and almost half held an incorrect understanding of the capability of certain security technologies.
c. 23% had confirmed malware infections and of these, 14% took no action to fix the problem.
d. 20% of respondents said that they would be 'very comfortable' and 40% 'comfortable' providing personal information online.
e. 17% of respondents would not be prepared to pay anything if their computer was compromised with malware that stole personal information.

30. Symantec's global survey of 1,425 SMBs worldwide in Feb 2009 also revealed that **while SMBs were acutely aware of today's security risks, a large number had yet to take even the basic steps needed to protect themselves**. The lack of a dedicated IT staff and tight budgets were the main reasons for the lack of action. Respondents also cited a lack of employee skills as a top barrier to security. Key findings are:
a. 58% of SMBs in Australia and New Zealand experience security breaches[5]
b. 43% of respondents do not have no endpoint protection[6]
c. 43% do not have any antispam solution
d. 45% do not back up their desktop PCs
e. 39% lack basic antivirus protection
f. 43% do not have dedicated IT staff, with no one managing their computers or using staff doing other jobs
g. Lack of employee skills (40%), lack of time (38%) and budget restrictions (37%) cited as leading barriers to security
h. Lack of awareness of current threats (31%) cited as another factor

31. Symantec works closely with governments worldwide to drive national online / cyber safety campaigns, for example through online safety weeks, informational websites, publications, and other initiatives like the recent launch of the Symantec Family

[4] http://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_2008.pdf
[5] Incidents where nformation has been subject to unauthorised access, often where the data is lost, stolen, or hacked.
[6] Software that combines antivirus with advanced threat protection technologies such as desktop firewall and intrusion prevention for laptops, desktops, and servers

Safety Initiative to protect children on social networking sites. Symantec has also supported Australia's national initiatives like the National E-Security Week 2009 and Privacy Awareness Week 2009. More details can be found in Annex II.

MEASURES CURRENTLY DEPLOYED TO MITIGATE E-SECURITY RISKS FACED BY AUSTRALIAN CONSUMERS &
FUTURE INITIATIVES THAT WILL FURTHER MITIGATE THE E-SECURITY RISKS TO AUSTRALIAN INTERNET USERS

32. There is no silver bullet to mitigate all these risks. The threat landscape has evolved so much that it is no longer a simple matter of installing a firewall or anti-virus in computers, or erecting perimeter defenses around the network. There are now so many ways by which users and systems can be compromised – via external or internal attacks, through the endpoints or the network, through emails, websites, IM, VOIP, P2P, social networks, etc.

33. First of all, **user education and raising public awareness are paramount**. As shown in the various surveys, individuals and SMBs lack awareness of basic information security practices, and there is a significant perception-reality gap in how well they are protected. User education is all the more important because users are now the new targets of malicious attacks. Hence SMBs and the general should be educated and regularly reminded on best practices (c.f. Annex III) to secure their computers and networks, as well as social engineering techniques that attackers are using.

34. Initiatives such as the recently concluded E-Security Awareness Week 2009 and the provision of public information and alert services on latest security threats through means like the Stay Smart Online website are very valuable to helping educate Australian consumers and businesses about information security risks. **Education is an ongoing issue** as more consumers are using a broader mix of online services and applications and with the forthcoming rollout of Australia's next generation broadband infrastructure, this will likely further increase Internet usage.

35. **More therefore needs to be done to protect SMBs and individuals who are low-hanging fruit for would-be attackers.**
    a. Efforts should be stepped up to increase visibility of user education / public awareness events and information channels like Stay Smart Online vis-à-vis the Australian community.
    b. SMBs and individuals should be incentivized to adopt not just ICT, but specifically security technologies. Given SMBs' lack of dedicated IT staff and their tight budgets, government could develop more co-funding programs or grant schemes to help SMBs and individuals beef up implementation and understanding of information security technologies and best practices.

c. Affordable software/service packages targeted at SMBs could be developed in partnership with industry. These packages could be subsidized by the government to reduce the cost of ownership, and actively promoted and delivered to the public through select industry partners. As security is seen more as a cost and less as a business enabler, such SMB software/service packages should include security as a component.

d. 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.

36. Secondly, **organizations and individuals should also be encouraged to adopt the latest and more comprehensive suite of protective technologies in order to keep pace with evolutions in the threat landscape and have the ability to tackle a whole range of threats:**

a. For individuals, this means adopting solutions integrating components like firewall, anti-virus, anti-spam, anti-spyware, anti-phishing, etc in order to counter the different kinds of threats.

b. For small and medium businesses, this could mean implementing more comprehensive protection suites including endpoint protection, mail security, and backup and recovery technologies.

c. For larger enterprises, in addition to endpoint management and protection technologies, data loss prevention (DLP) technologies will minimize the risk of data loss of personal and business confidential information.

37. A strong legislative/regulatory framework is a critical driver in placing information security high on the agenda of the government and businesses. Australia has done well in implementing cyber security laws at the federal and/or state level, relating to various aspects like privacy, spam, cybercrime, online child safety. Other examples include sectoral regulations like HIPPA, SOX, Basel II. These laws/regulations are necessary to maintain adequate levels of protection against different types of cyber threats.

38. **Mandatory notification of data breaches has an important role in making the public aware of the real dangers posed to their personal information.** In this respect, we welcome the Australian government's consideration to mandate breach notification, which Symantec agrees is important to provide complete protection throughout the information lifecycle. Nevertheless, data breach notification is an emergency measure and hence a balanced risk-based approach must be adopted to ensure that organizations and individuals do not find the framework overly burdensome. The inclusion of a "safe harbor" principle will help address this, i.e. organizations demonstrating that the data has been secured to an adequate level of security, need not undertake any notification.

39. **Securing the Australian community also requires developing effective early warning, intelligence collection, and security response capabilities**. Tracking security events on a global basis can enable early warning of upcoming active attacks, allowing users to be alerted and prepared against a potential attack. Gaining responsive insight into incidents within the organization's network and potentially within information infrastructure across critical sectors (e.g. telco, utility, transport, etc), is also important to enable quick response to any attacks. Protection of critical infrastructure has become more important as industrial systems controlling these infrastructures, erstwhile thought to be isolated and thus protected, are nowadays being exposed to similar vulnerabilities to that usually found in corporate IT systems.

40. **Strong cooperation between public and private sector should be pursued** and the Australian government could examine how existing public-private partnerships with leading industry security players like Symantec can be better leveraged. Assessments should be made how trusted information-sharing between the government and private sector owners of critical infrastructure can be better forged through existing programs like the Trusted Information Sharing Network (TISN), how better sector-specific threat-sharing and early warning systems can be developed with the national computer emergency response teams, and how private security vendors can be better tapped on for expertise in best practices and for cooperation in developing sector-specific understanding of the Australian threat landscape.

41. **As a national policy, the establishment of a competitive market for the security software industry should be upheld as a guarantee for security**. Diversity coupled with interoperability helps break the growth and spread of security exploits such as malware and viruses that can take advantage of common vulnerabilities across ubiquitous platforms. Security is greatly enhanced by fostering a heterogeneous security environment and a dominated market could threaten consumer choice and competitiveness. More importantly, it could potentially threaten the security of our entire information infrastructure since it risks facilitating the growth and spread of common vulnerabilities.

42. A healthy competitive market also spurs innovation in security solutions. It is essential that innovation keep pace with the fast evolution of the threat landscape. As the rewards get more attractive, attackers continue to improve their methods. Attacks have become increasingly stealthier and silent therefore more complex to identify. Traditional perimeter defense is no longer sufficient. With the rise of client side attacks and web application attacks, attackers are constantly on the lookout for new inroads into the network. As a result, the volume and severity of attacks continues to rise. The market's dynamics and flexibility place it in the best position to provide the necessary pace of innovation to respond to evolving attacks.

EMERGING TECHNOLOGIES TO COMBAT THESE RISKS

43. There are a number of technologies available to detect and record security breaches and attacks, which are employed in different ways by different users. Some of these solutions are mentioned in paragraph 36 above. Specifically, Symantec offers solutions like Norton Internet Security 2009 (without backup) and Norton 360 (includes backup) which protect consumers comprehensively against a wide variety of threats. Symantec also offers Symantec Protection Suite Small Business Edition for small businesses, which includes endpoint protection, mail security and backup solutions. For larger businesses and enterprises, Symantec offers solutions like Symantec Endpoint Protection and Data Loss Prevention as well as a whole suite of other technologies for security, infrastructure operations, information risk & compliance, storage and business continuity.

44. In particular, Data Loss Prevention (DLP) is an emerging technology that will help companies prevent personal or business confidential data from flowing out inadvertently or with malicious intent. Symantec's DLP technology basically helps the organisation answer three fundamental questions – where confidential data resides, how it is being used, and how data loss can be prevented. Discovering where data is located - be it at file servers, databases, email repositories, endpoints, etc - is the first important step to take. Next, monitoring of how data is used is important to know whether confidential data is channeled out of the organization through corporate emails, web mails, USB sticks, etc. Finally, data can be protected from being leaked out for example by quarantining, copying or removing it from stored location, or simply blocking files from being downloaded to drives or removable media. To ensure compliance, policies can be set, monitored and enforced.

45. Software-as-a-Service (SaaS) is an emerging technology by which services are rendered to an organization as a Web service, rather than by installing software. Security services like email security, Web & IM security, email archival, etc can similarly be delivered via the SaaS model. This gives CIOs the option of using a fully third-party managed service requiring no hardware or software to protect their systems.

46. Other specialized technologies include sensor technologies employed by the Symantec early warning system (DeepSight) which is designed to record attacking activity and provide early warning information and intelligence on attacks. Another technology is employed by Symantec Managed Security Services which monitor using sensors real-time customer systems and alert the system administrator for attacks on its system or can even take precautionary measures to prevent a system compromise.

47. In the area of child online safety, traditional forms of parental control solutions tend to drive children underground. New technologies like OnlineFamily.Norton[7] have emerged that allow parents and kids to jointly set simple, clear rules that support active, safe use of the online world. Parents stay informed about what their children are doing right now, and can check their children's online activity anytime, from anywhere where they can connect to the web. Children know exactly what their parents are monitoring and can ask permission to access new sites or to communicate with new people. Such solutions foster greater trust and healthy dialogue between parent and child, and allow increasingly mobile parents to have greater visibility and active control over the multitude of online threats to their children in a timely manner.

48. OnlineFamily.Norton also help protect a child's personal information by preventing the child from sharing such information - phone number, email address, social security number, or any other information to be specified - over the Internet. A parents can specify the child's personal information that they want protected, and any attempt by the child (be it accidental or on purpose) to send such information over the Internet will be blocked. Parents can also be automatically notified when such incidents happen.

3rd July 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

[7] https://onlinefamily.norton.com

ANNEX I

Description of metrics used in ISTR rankings:

1. **Malicious activity by country/region.** This metric will assess the countries or regions in which the most malicious activity takes place or originates in the APJ region. To determine this, Symantec has compiled geographical data on numerous malicious activities, including: bot-infected computers, phishing website hosts, malicious code reports, spam zombies, and attack origin. The rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each country.

2. **Bot-infected computers by country/region.** Recognizing the ongoing threat posed by botnets, Symantec tracks the distribution of bot-infected computers both worldwide and regionally. For regions, Symantec calculates the number of computers worldwide that are known to be infected with bots, and assesses which countries within the region are home to high percentages of these computers. A high percentage of infected machines could mean a greater potential for bot-related attacks, and indicate the level of patching and security awareness in the region.

3. **Bot command-and-control servers by country/region**. In locating bot C&C servers, bot controllers look for hosting services with stable Internet connections, high bandwidth, and whose security measures may not be fully developed or rigidly enforced. A high proportion of bot C&C servers may indicate inadequacy of end-user education and weak implementation of security practices. However, bot C&C servers might not be located in the same place as the person controlling the botnet. Additionally, “normal” bot-infected computers can often become bot C&C servers through the use of fast-flux domain name service scheme where the control of a botnet is decentralized using a number of bot-infected computers throughout the network.

4. **Top countries/regions of origin for Web-based attacks**. This metric will assess the top countries of origin for Web-based attacks against users in APJ by determining the location of computers from which the attack occurred. Note that the server hosting the exploit may not necessarily be the same server that the user has visited due to redirection. A user could visit a website that redirects his or her browser to a malicious server in another country. Once an attacker has compromised a legitimate website, users who visit the website may be attacked by several additional means. One way is through a drive-by download, which can include installation of malicious code without the user’s knowledge, or which will mislead the user to indirectly authorize a malicious download via a fake client-side application authorization request. Another way is to redirect the

user to another website that is used to host malicious code. Sites and servers hosting a variety of malicious exploits can be found worldwide. Multiple domains can be associated with one compromised site, which is used to exploit one or more security vulnerabilities in affected client browsers.

5. **Top countries/regions hosting phishing websites and top targeted sectors**. This metric will assess the APJ countries and regions in which the most phishing websites were hosted. This data is a snapshot in time, and does not offer insight into changes in the locations of certain phishing sites over the course of the reporting period. It should also be noted that the fact that a phishing website is hosted in a certain country does not necessarily mean that the attacker is located in that country.

6. **Top countries/regions of spam origin**. This section will discuss the top 10 countries/regions of spam origin in APJ. Data is gathered by customer installations of Symantec Brightmail AntiSpam, and includes the originating server's IP address, against which frequency statistics are compared. Each IP address is mapped to a specific country and charted over time. The nature of spam and its distribution on the Internet presents challenges in identifying the location of people who are sending it because many spammers try to redirect attention away from their actual geographic location. In an attempt to bypass DNS block lists, they use Trojans that relay email, which allow them to send spam from sites distinct from their physical location. In doing so, they tend to focus on compromised computers in those regions with the largest bandwidth capabilities. As such, the region in which the spam originates may not correspond to the region in which the spammers are located.

ANNEX II

SYMANTEC'S WORK ON CYBERSECURITY AWARENESS

Symantec works with governments worldwide – US, UK, France, Germany, Belgium, Ireland, Singapore, Malaysia, Australia and many others - to drive **national online / cyber safety campaigns**, for example through online safety weeks, **informational websites**, **publications**, and other initiatives like the recent launch of the Symantec Family Safety Initiative to protect children on social networking sites.
http://www.symantec.com/about/profile/responsibility/cyberawareness.jsp

Symantec has developed free educational tools and guides for parents and the public on various topics - examples include Symantec's Cybercrime Website[8] providing tips and resources for avoiding and responding to online fraud; Symantec's Family Resource Website[9] educating parents on risks to children's online safety, Symantec's blogs[10] on how to protect oneself in the cyber world. Symantec's Family Online Safety Guide won the 2008 iParenting Media Award in the Best Book category. iParenting Media Awards Program is the only consumer awards program certified by ISO 9001:2000 , the internationally recognized standard of quality assurance.

Symantec also works with non-profit organizations and government agencies on joint initiatives such as getsafeonline.org, staysafeonline.org, ikeepsafe.org, i-SAFE.org, Web Wise Kids Project Safe Childhood program, One Economy's online information portal The Beehive. Symantec is a top-level member of the Family Online Safety Institute (FOSI) and Marian Merritt, Symantec's Internet Safety Advocate is our representative on the board.

Examples of other partnerships that Symantec has formed with industry associations and government authorities to enhance public awareness of various issues like cybercrime, include:

- In Singapore, Symantec is part of the **Cyber Security Awareness Alliance** set up by the Infocomm Development Authority of Singapore (IDA) to build a positive culture of cyber security in Singapore, and promote and enhance awareness and adoption of essential cyber security practices. This initiative is part of the Infocomm Security Masterplan 2.0 launched in year 2008. We are also member of the **Internet & Media Advisory Committee (INMAC)**, an advisory and consultative council formed on 1 May 2007 that looks into media literacy, Cyber Wellness and related policies, issues and programmes in Singapore.

- Created in Feb 2008, the Internet Safety Technical Task Force (ISTTF), of which Symantec was a sponsor, was established through an agreement between My Space and 49 of the 50 state attorneys general to consider those technologies that industry and end users - including parents - can use to help keep minors safer on the Internet. The task force released its final report, Enhancing Child Safety and Online Technologies, in January.

[8] http://www.symantec.com/norton/cybercrime/index.jsp
[9] http://www.symantec.com/norton/familyresources/index.jsp
[10] http://community.norton.com/norton/blog?blog.id=npb1 ;
http://community.norton.com/norton/blog?blog.id=askmarian

- Symantec was an active participant in Australia's National E-security Week 2009 to help Australians understand e-security risks and how they can protect themselves online.

- Symantec partners National Cyber Security Alliance (NCSA) and a global nonprofit organization One Economy Corporation, in San Jose to provide Internet users with cyber safety tips, educational presentations on the dangers of lax computer security and give away free copies of Norton 360, Symantec's all-in-one security solution as part of the national campaign, National Cyber Security Awareness Month, to educate the American public, businesses, schools and government agencies about ways to secure their part of cyber space, computers and our nation's critical infrastructure.

- Symantec is one of three partners forming the European High Tech Crime Response Network, a consortium tasked with a cybercrime awareness-raising project funded by the EU Commission. Symantec will take the lead role in shaping the message of the project[11]. Other partners of the consortium include Business Software Alliance, Europe, and the Estonian national police.

[11] Symantec's role will be to raise citizens', governments' and corporations' awareness of the existing and emerging threats posed by cybercrime. The partnership was set up under the EU's AGIS program, which helps police, the courts, and professionals from EU member states cooperate in crimefighting matters. AGIS is part of a larger EU umbrella fund that supports public/private partnerships to address matters related to justice, police and judicial cooperation, such as terrorism, money laundering, narcotics and others.

symantec.™

ANNEX III

ONLINE SECURITY BEST PRACTICES

1. Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.

2. Ensure that security patches are up-to-date and that they are applied to all vulnerable applications in a timely manner.

3. Ensure that passwords are a mix of letters and numbers. Do not use dictionary words. Change passwords often.

4. Never view, open or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.

5. Keep virus definitions updated regularly. By deploying the latest virus definitions, private users can protect their computers against the latest viruses known to be spreading "in the wild."

6. Private users should routinely check to see if their PC or Macintosh system is vulnerable to threats by using Symantec Security Check at www.symantec.com/securitycheck.

7. All computer users need to know how to recognize computer hoaxes and phishing scams. Hoaxes typically include a bogus email warning to "send this to everyone you know" and/or improper technical jargon that is intended to frighten or mislead users. Phishing scams are much more sophisticated. Often arriving in email, phishing scams appear to come from a legitimate organization and entice users to enter credit card or other confidential information into forms on a Web site designed to look like that of the legitimate organization. Computer users also need to consider who is sending the information and determine if the sender is a trustworthy, reliable source. The best course of action is to simply delete these types of emails.

8. Private users can get involved in fighting cybercrime by tracking and reporting intruders. With Symantec Security Check's tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker's Internet service provider or local police.

9. Be aware of the differences between adware and spyware. Adware is often used to gather data for marketing purposes and generally has a valid, benign purpose. Spyware, on the other hand, may be used for malicious purposes, such as identity theft.

10. Both spyware and adware can be automatically installed on a computer along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links and/or attachments in e-mail messages, or via instant messaging clients. Therefore, users should be informed and selective about what they install on their computer.

11. Don’t just click those “Yes, I accept” buttons on end-user licensing agreements (EULAs). Some spyware and adware applications can be installed after an end user has accept the EULA, or as a consequence of that acceptance. Read EULAs carefully to examine what they mean in terms of privacy. The agreement should clearly explain what the product is doing and provide an uninstaller.

12. Beware of programs that flash ads in the user interface. Many spyware programs track how users respond to these ads, and their presence is a red flag. When users see ads in a program’s user interface, they may be looking at a piece of spyware.