Symantec's Comments on the Workplace Surveillance Act 2005

This paper sets out Symantec's views on the *Workplace Surveillance Act 2005* review being carried out by the NSW Department of Justice and Attorney General.

The importance and relevance of information security in a connected world

1. As defined by the Act, computer surveillance is defined as "surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites)". Based on this definition, this could include a number of security technologies such as end-point security software which work by monitoring traffic for malicious activity, as well as Hosted of Managed services such as Cloud-based scanning of malicious email.

2. Symantec's Global Internet Security Threat Report 2009[1] highlighted the emergence of targeted threats against enterprises through Advanced Persistent Threats (APTs), such as the Hydraq Trojan. Unlike the previous generation of malware which had broadcasted their existence by making noticeable changes to the infected computer (such as displaying a message on the computer or rendering it inoperable), APTs are designed to remain undetected and used to siphon as much information as possible from the enterprise network. This would include security credentials (that can be used to further penetrate the enterprise system) as well as commercially sensitive information.

3. Attacks on enterprises are also increasing in reach and number. Symantec's State of Enterprise Security Report 2010[2] found that 75% of all respondents (which included Small and Medium Enterprises) had experienced cyber attacks of one form or another in 2009. In all cases, the respondents had reported monetary losses, most commonly due to downtime of environment, theft of customer information (including credit card information) and intellectual property.

4. Thus, the threat landscape requires that enterprises take proactive steps to properly secure their systems, which would generally require the use of security technologies. As with all security technologies there is a level of information disclosure that is necessary in order to be able to determine what needs to be protected and to do that effectively. Information security technologies however have reached an adequate level of maturity to be able to do that in the least privacy invasive manner.

---

[1] Symantec's Global Internet Security Threat Report is published annually by Symantec, collating information gathered by Symantec's Global Intelligence Network, of more than 240,000 sensors in over 200 countries. It aims to provide an informed commentary on the internet threat landscape. The latest edition (published in April 2010) can be found at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

[2] Symantec's State of Enterprise Security Report 2010 is based on information collected from 2100 enterprises from around the world as a measure of top of mind concerns and considerations of Enterprise IT security. The 2010 edition can be found at http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sesreport2010

5. For example security software monitors files to determine if malicious code has been embedded, it does not necessarily monitor the content. This is with certain exceptions such as software designed to prevent data loss or data leakage or anti-spam filters. In cases such as data loss prevention, the software is designed to conduct the monitoring in the least invasive manner possible, and with the goal of protecting employees and enterprises from accidental data breaches and data loss, by effectively blocking content that is designated as confidential from being exported to unauthorized locations. This threat was highlighted in the 2008 case of an Australian bank recalling two thousand credit cards which had been compromised due to a security breach. In the case of anti-spam the content of a communication (as a final security measure) is scanned automatically from the machine looking for keywords or patterns to determine whether the email is malicious. The purpose of the scanning is to protect the employee from unwanted communications that consume corporate resources and can be a source for malware that can threaten an organizations infrastructure or inappropriate content, such as pirated and counterfeited goods, or pornography. The cost of spam is not to be underestimated; with the increasing amount of spam being sent globally (Symantec Hosted Services' MessageLabs Intelligence Report for 2010 had put the average global spam rate for 2010 at 89.1%, and increase of 1.4% over the previous year).

6. In the light of the remarks above regarding the current threat landscape and its evolution Symantec believes that the need for security technology in the workplace becomes apparent and unquestionable, as in fact a number of recent high-profile security incidents, such as the on-going investigation into an Australia-based telco where customer records has been compromised due to a security breach, demonstrate. In the ISTR, it can be seen that a significant percentage of all data breeches (26% from insecure IT policies and 9% from insiders) is a result of internal threats, which encompasses well-intentioned employees who made a mistake or maliciously-intended employees acting against the interest of the organization.

7. The effective protection of an organizations computer and network resources is not only a question of reputation, productivity or business confidentiality. It is also part of our collective responsibility when going online. It is a question of ensuring that the organizations resources are not used to attack and compromise other systems in our connected society. In addition it is also a question of protecting an organizations employees and respecting their individual right to privacy.

8. It should be taken into account that the more pervasive the use of the internet, social networks, mobile broadband and the new communications tools becomes, the greater merging will we see between our personal and professional lives online. As a result the protection technology that an organization affords to its employees is often extending to protect personal information of these employees both in their employment as well as in their capacity as individuals.

9. Under the current Federal Privacy Law, The Office of the Australian Information Commissioner does not mandate the reporting of a security breach, but recommends that in the case of a data breach, under certain situations, affected

individuals should be notified. Without proper technological tools to detect, prevent, manage, respond and determine the nature and breadth of a security incident that may or may not lead to a breach, it would be difficult for enterprises to meet this recommendation.

10. **Symantec concurs with the need and continued relevance of the *Workplace Surveillance Act*** in laying out the key responsibilities and rights of enterprises and employers in enacting appropriate defenses to secure their Information Technology infrastructure against cyber attacks. Symantec further believes that these measures will continue to be necessary and are proportionate in a democratic society and will enjoy broad social acceptance.

For further information, please contact

Kai Koon Ng
Senior Manager, Legal & Public Affairs

Symantec Asia Pacific Pte Ltd
10 Eunos Road 8, #09-02
Singapore 408600

Tel: +65 6413 4307 / +65 9002 0214
kaikoon_ng@symantec.com