House of Representatives
Standing Committee on Communications
New Inquiry into Cybercrime

Submission from Microsoft Australia

Introduction

Microsoft Australia welcomes the opportunity to participate in the House Standing Committee on Communications' Inquiry into Cybercrime through this submission. We believe that a periodic review of the cybercrime prevention framework, in light of the quickly evolving threat landscape, is both timely and appropriate.

Over the last thirty years there have been dramatic advances in information technology - the development of the microprocessor, the rise of the personal computer, the emergence of the Internet – that have revolutionised the way information is created, stored, shared, and used. These rapid advances in software, IT services and communications have enabled many traditionally separate and disparate infrastructures and business operations to become more connected. Through this connectivity, virtually every aspect of society has experienced a transformation. Businesses and governments have been able to manage and streamline their operations. Individuals have been offered ready access to multiple sources of information thereby expanding knowledge and choice. Across every field of endeavour – commercial, social, scientific and philanthropic – the power of information has been increased and the transaction costs of engagement have been lowered. However, as our reliance on software, services and communications has increased, so too has our vulnerability to online crime and sophisticated cyber attacks.

There are four things about the Internet that make it susceptible to the commission of crime: (1) It is globally connected; (2) It is "anonymous"; (3) There is a relative lack of traceability, and; (4) There are really rich targets – financial data, personally identifiable information, military information, business information. In the physical world, we have historically managed the crime problem because we have preventative systems that have worked – locks and keys, home alarms, police patrols, neighbourhood watches and the like -- and we have reactive structures that work as well, including court systems and law enforcement agencies. Unfortunately, the Internet doesn't provide those kinds of mechanisms, particularly where global or cross-border attacks are perpetrated.

What makes this scenario so daunting is that if the conventional view of the Internet is correct, global connectivity is going to continue to grow. There are a billion people online today, 5 billion who aren't. The Internet is increasingly becoming a gateway for "cloud computing," in which remote data centres host data and serve applications used by devices and IT systems. If Microsoft's vision of cloud computing is right, there will be more rich targets online as more and more information is stored "in the cloud". So, if global connectivity is going to continue to grow, and there will be more and more rich targets, what are we going to do about the criminal population? That is a huge challenge.

Microsoft believes that all of these factors point to the need for a comprehensive and coordinated national strategy around cybercrime as well as greater Government-to-Government collaboration on cross-jurisdictional crime. So too, we need to better understand the threat landscape and to evolve and focus the public-private partnership model as well as international collaboration. Further, we should consider a legislative model designed to ensure that greater regulation, if enacted, protects innovation while providing appropriate government oversight of cyber security issues. Finally, Microsoft maintains that the Internet needs an appropriately deployed identity meta-system if we are to make the Internet dramatically more secure but protect important social values, such as privacy and free speech. We will address each of these issues, in turn, throughout this submission.

The Changing Threat Landscape: The Pursuit of Fortune vs. Fame

Cyber attacks are proving to be increasingly profitable for criminals. As a result, exploits have become more stealthy, pro-actively targeted and damaging. Where publicity was once the primary motivation behind many digital attacks, Microsoft considers criminal financial gain to be the primary driver of many of the prominent attacks we see today.

Criminals seek to exploit common applications to gain access to information or operations that can be translated into financial or strategic gain. The targets of these threats span from desktops to data centres, and consumers to critical infrastructures. As software and services are inherently designed to respond to individual consumer need and are therefore necessarily complex in their architecture and structure, there is no perfect security solution irrespective of the platform.

Given that there are highly-educated, ill-intentioned, and often well-funded individuals and organisations that have access to increasingly sophisticated analysis and attack tools, it is not practically or logically possible to prevent all types of cyber attacks at all times in all circumstances. This reality requires the IT industry and governments to participate in a race against cyber criminals to prevent and deter attacks, as well as to assure critical services.

The Australian Institute of Criminology's (AIC) July 2007 paper on the, "Future of Technology-enabled Crime in Australia," supports this proposition. That paper indicated that there are serious concerns about the way technology advances are increasing opportunities for criminals.

According to the AIC study, dangerous Cybercrime trends include:

- Cyber-terrorism targeting critical information infrastructure, including transportation and financial networks, emergency management systems and the power grid;
- Identity-related financial crime growing exponentially as wireless and mobile technologies flourish, allowing criminals to plunder systems remotely;
- Cyber-attacks becoming more deliberately targeted and sophisticated;
- Strains of malicious software ("malware") becoming more damaging and difficult to detect; and
- Attacks being automated through the use of robotic networks or "botnets[1]," where literally thousands of "zombie" computers are taken over and networked to remotely launch attacks on other computers.

Significantly, the AIC report highlighted the need for more uniformity in cybercrime legislation across jurisdictions to help surmount this trans-national challenge. Microsoft agrees that a greater degree of consistency in cybercrime laws would facilitate international cooperation in fighting these crimes and would effectively prevent the creation of "safe havens" for online criminals. Microsoft also shares the AIC's concerns about identity theft, botnets and malware trends in Australia.

Malware Trends in Australia

In April, 2008 Microsoft released a Security Intelligence Report (SIR v5) with the intent of providing an in-depth perspective on the changing threat landscape. The report detailed information on the experience of software vulnerability disclosures and exploits, malware, and "potentially unwanted software." Data for Australia was gathered by the Microsoft Malicious Software Removal Tool (MSRT) in the second half of 2007.

The MSRT removed malware *from 1 out of every 204* Windows based computers it was executed on in Australia. The good news is that the malware infection rates in Australia were much lower than the *worldwide*

[1] [1] The term *bot* is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a "*botnet*". Criminals use botnets to send out spam e-mail messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes a part of a botnet, your computer might slow down and you might be inadvertently helping criminals.

average of 1 out of every 123 computers infected with malware. The malware infection rates in Australia are comparable to those observed in Denmark and Nigeria, and slightly higher than those in Malaysia (1:216) or New Zealand (1:264).

The more recent Security Intelligence Report (V6) found that the infection rate (CCM) for Australia from July to December, 2008, was 4.7; significantly lower than the worldwide 2H08 infection rate of 8.6. (CCM is the number of computers cleaned for every 1,000 executions of the MSRT), but this is still cause for significant concern.

Consistent with the global trend observed in 2007, there was a large increase in the detection of Trojans in Australia over the course of 2008. The threat landscape in Australia is dominated by malware families, which account for 67.3% of all families detected on infected computers in the second half of 2008. The most common category in Australia is "Miscellaneous Trojans," which includes all Trojan families that are not classified as Downloaders, Droppers or Backdoors. It accounts for 28.3 percent of all families detected on infected Australian computers and 10 of the top 25 families. The second most common category in Australia is Trojan Downloaders & Droppers. Criminals use Trojan Downloaders to install other malicious files on the infected system either by downloading them from a remote computer or by dropping them directly from a copy contained in its own code.

Evidence from Australia and other countries suggests that Trojans have become the tool of choice among criminals in targeting victims around the world and in Australia. These approaches represent an evolution of an expanding toolset supported by sophisticated software engineering techniques and processes used by criminals to compromise users' digital devices which increasingly include mobile and gaming variants.

Because Trojans, by definition, are primarily carriers or vectors for any desired form of software code, they have the capacity to place multiple agents on a user's device that work in concert at the behest of a remote entity. This sets the conditions for an extremely wide range of cyber-based exploits not yet experienced but fully possible.

Examples could include a group of software agents placed on selected user's machines over time and set to "come to life" at a certain time or triggered by a certain event causing them to act together to compromise a particular network, conduct a denial of service (DOS) attack on a particular web site or extract certain information from organisational IT systems, act on it and send the results to some external entity. The possibilities are enormous and clearly worrying for governments and individuals. The potential damage that could be inflicted on a national economy is considerable.

Future E-Security Threat Landscape – Year 2013 and Beyond

It is not possible to accurately predict the future, but it is possible to review history and analyse trends (always cognisant of the constant of human behavioural shortcomings) to gain an understanding of what may lie ahead.

To understand the E-Security threat landscape 4 years from now it is necessary to firstly set the scene of the future - that scene is best set in the context of *Technology* (what will be used), *Society* (who will use it) and T*hreat Agents* (who may take advantage of it).

Technology: It is safe to anticipate that in all aspects of society the use of and reliance on information and communication technologies (ICT) will be more pervasive in the future. It is also reasonable to expect that today's ICT technologies will continue to evolve into a model that more critically utilises "services" hosted on the internet using interconnected technologies. The pervasiveness and advancements in mobile technology and the demands of consumers will dictate that almost every new electronic device will have some form of anywhere access capacity.

Significant trends already underway include:

- Data being contained or "cached" in multiple locations and synchronised between multiple devices and applications. This means that traditional practices for data management are increasingly impractical;

- A consumer-driven move away from large, centrally managed IT systems towards loosely connected and highly distributed software and services delivered via the Internet ("cloud computing"). This challenges users and the Industry to ensure that both the users and the Internet-based services they suppose are being used are in fact *bona fide*; and
- An increasing need to provide access to information and resources over the Internet in a safe, economical and user-friendly format. Existing practices for identity and access control are starting to break down and require urgent review.

Technology will be relied upon to compensate for shortcomings in the physical world of 2013; the primary example of this is likely to be "telecommuting" where rising costs and the environmental impact of commuting will demand a more technologically enabled mobile work force.

Society: As more of the developing world's citizens and governments become economically prosperous and ICT becomes more affordable, more devices, individuals and organisations will leverage "services" in 2013 creating a greater reliance between the fabric of societies and technology.

The gap between the numbers of novice ICT users and those who are educated will significantly widen – thus creating the potential for more on-line targets for criminals. For those who are educated, the baseline of ICT skill will evolve to higher degrees of competency. It is likely that the advancement in ICT education and skills combined with usability improvements in ICT will create a virtual society of those "who have" and will thereby further increase the gap to the uneducated or less skilled ICT user.

Threat agents: In the year 2013, we can be certain that criminals, terrorists and geo-political instability will unfortunately still exist. It is realistic to expect that criminals will seek to be more organised, better armed, better skilled and more prolific in exploiting the ICT environment for profit and other ends.

Many more organisations and groups (government and non-government) will formalise their ICT weapons capability; that is ready and deploy an ICT capability to engage in cyber-warfare. At this time the true ICT weapons race era will be born and can be expected to take front seat with the challenges posed by nuclear, biological and traditional weapons.

Finally, the Cyber terrorist of 2013 will be truly capable of effectively delivering in the virtual world what is today delivered in the physical world - harm, disruption and life threatening consequences.

Identity Theft and Phishing

Identity theft - when perpetrated using technology - is one of the more pernicious cyber-related activities as it drives to the heart of the trusted technology experience and has perhaps the greatest potential to derail the value that technology brings to all of us.

Various definitions exist of what ID theft is and what it is not. The OECD recently used the following definition, which is suitably generalised and relevant for our purposes here:

> ***ID theft*** *occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes*[2].

A variety of different methods can be used to obtain personal information from ether victims or those data sources holding information about individuals. The most well known exploits of ID theft involve so called "social engineering" exploits which are essentially the cyber-equivalents of the old fashioned confidence trick.

Perpetrators use a variety of techniques and tools to gain access to information. The activation of malware (a stealth program installed on a device) and "phishing" attacks are well known examples of techniques used to gain access to information. Phishing occurs when Internet users are tricked into providing information to perpetrators following the receipt and activation of bogus e-mails or through the use of fake websites.

[2] *Scoping Paper on ID Theft, OECD Ministerial Meeting on the future of the Internet Economy*

Phishing and its variants are examples of an underlying vulnerability that preys upon human nature. In an increasingly Internet-connected world the collection and exploitation of information is easier, safer to achieve and extremely profitable particularly when victims lack the knowledge or sophistication to understand the technology they depend upon for financial transactions.

Threats in 2013 and Beyond

Traditional threats that exist today will still be present, in one form or another, in 2013. Those existing threats will evolve over time using blended and more complex technologies, resulting in stealthier attacks yielding better results for the criminal. It's also likely that the traditional low-tech threats that employ "social engineering" such as scams, phishing and spoofing will flourish as criminals target the less educated and newest internet citizens. This is especially a problem for people whose first language may not be the language that they embrace over the internet. In a world with greater population mobility this is an increasing issue.

The advance in technological tools will make it significantly easier for criminals to commit financially motivated crimes against larger numbers of end users and against organisations who are ill prepared. Without diminishing the importance of the aforementioned threats, it is important to focus on those cyber security threats that are likely to be of more holistic concern to the Australian Government in 2013 - those that stand out above the rest and have significant consequences on our national security, economic and social well being.

The Threat to Identity and Trust

A direct consequence of increased activity by criminals targeted at users of the online world could be a significant loss of trust in the identity of connected devices, software, people and data. For example, a failure to develop robust solution and management strategies may mean the economic losses caused by electronic fraud reach a level where business and other users lose confidence and trust with online services resulting in a return to legacy transactions (for example in the context of banking a return to over the counter service delivery).

While it is unlikely that this threat would be fully realised in 2013, ineffective actions taken between now and then may result in a tipping point that steers many users back to a more trusted legacy world. This would have massive consequences on current and future investments in the ICT of the future internet and on the economic viability of organisations that see growth and cost efficiencies in delivering business service via online methods.

Well-Organised and Coordinated Threats

In the world of 2009, physical and virtual threats are seldom combined effectively to create a force multiplier effect. For example, an adversary could employ a physical attack to destroy sections of a network (primary path) and then use virtual attacks to deny service to a back-up network path – rendering an organisation or country or ICT communications infrastructure effectively useless.

In the world of 2013, where there will be a number of non-traditional organisations that have a true ICT weapons capability that can be tactically deployed with or without a conventional physical threat, this scenario of virtual viral warfare has potential resonance. With the correct application and timing of combined physical and ICT threats a massive force multiplier effect could be gained, and the consequences are likely to be grave.

It's right to think that threats above are couched in the language of "doomsday" but the reality in 2013 - with the advances in, and increased dependence on technology, reflected changes in society and a much smarter adversary who will take advantage of these developments - is that the chances of those threats being realised will be higher than at any previous time in history.

Developing a National Security Strategy

Australia has been at the forefront of the national cyber security awareness and response curve by virtue of the drafting of a national strategy as early as 2001: The E-Security National Agenda (ESNA). This was reviewed in 2006 and was reconsidered through the recent E-Security Review.

By undertaking this major re-assessment of the ESNA, the Government seems to be indicating its belief that there may be room for improvement and that input from a range of stakeholders with a broad array of perspectives is critical in helping to achieve the best possible outcomes. We believe that continually drawing from a broad range of stakeholder interests is critical to this process as is re-evaluating this strategy every two to three years.

Microsoft submits that it may be time for Australia to consider an even more expansive strategy going forward. It is clear that Australia's future success requires a comprehensive cyber security strategy that engages the relevant agencies of the government and brings to bear all elements of national power, including economic, diplomatic, law enforcement, military and intelligence authorities. When one recognises the breadth of the challenge and the need for a massively decentralized but coordinated response among the federal, state and territory agencies, we believe that the Committee should consider whether or not Australia's national cyber security strategy and its implementation should be led by a single coordinating authority at the highest Executive level, like the Department of Prime Minister and Cabinet or through an appointed "cyber security czar". As the Committee would be aware, the US is moving to a similar model, where their national cyber security strategy will be led and coordinated by the White House.

Deterring Cybercrime: Proposed Legislative Changes

Where regulation is concerned, ideally, the government and private sector should jointly determine the level of security provided by markets, the level of security needed to protect national security, and how the gap between what the market will provide and what national security demands can be filled most effectively. Certainly, appropriately tailored legislation – legislation that is technology neutral and recognises the best practices created by the innovative private sector -- will be an important component of any national cyber security effort. The fact is, markets respond to customer demand and most customers, though more aware of security issues today than in the past, will not pay for the level of security necessary to protect national security.

Indeed, the first line of defence in any national cyber security strategy should be to ensure that the appropriate policy frameworks are in place. If there is not robust legislation on the statute books, law enforcement won't have the tools to investigate and prosecute the crimes.

So too, deterrence is only one part of the equation. Effective enforcement of the laws requires that there be sufficient resources allocated to prosecutors and the court system. A decision to prosecute should not be a matter of competing resource priorities. Additionally, in a technical area like information technology prosecutors need resources to develop capacity in order to understand and appreciate the subtleties of law in a technological environment. While it is commonly accepted that technology will always outpace policy and that political processes often take longer than is desirable when there is a pressing legislative need, it is nonetheless critical that these frameworks are regularly reviewed and updated.

Based on independent analysis, Microsoft has found that legislative activity in the cyber security sphere is increasing across the Asia Pacific region and international cybercrime guidelines are making an impact. We found that there was relatively little information about where countries are placed in terms of their legal and regulatory frameworks to address threats across jurisdictions so Microsoft sought to obtain a better understanding of how Australia is placed with respect to its cybercrime framework vis-a-vis the rest of the region.

In an effort to better understand the state of play in the Asia Pacific region, Microsoft conducted a detailed analysis of the computer security, privacy, spam and online child safety laws in 14 countries across the region, including Australia. "*The Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws,"* was released in November, 2007, and can be found in its entirety at www.microsoft.com/asia.

Overall Study Findings and Benchmark Legislation

Overall, the study found encouraging signs of a growing acceptance in the region of the role of international norms, such as the Council of Europe's (COE) Convention on Cybercrime (also referred to as, "The Budapest Convention" and in this submission referred to as, "the Convention"), in shaping new laws.

The Convention is the only binding treaty in the world today, serving as a guideline for nations that want to develop their own similar laws. Microsoft's report also found significant variation in the degree to which benchmark legislation has been implemented by different countries and for different types of cybercrime, with computer security laws being the most well-developed and, worryingly, online child safety laws the least. For the purposes of this submission, however, we will only be focusing on the security and cybercrime components of this study.

The analysis found that Australia's cybercrime laws overall had the strongest alignment with the benchmarking criteria in the region. It was the only country of the 14 with favourable alignment to the draft international standard for child safety legislation. It was also in the top category for alignment with computer security guidelines.

Microsoft used Titles 1, 2 and 5 of the COE's *Convention on Cybercrime* as the benchmark legislation for the cybercrime portion of the analysis.[3] As mentioned above, the *Convention on Cybercrime* is widely recognised as an international norm on the criminalisation of computer-related conduct, having been widely adopted by European States and signed by several non-European States, including the United States, Canada, Japan and South Africa.

Title 1 of the Convention contains a number of "core offences" that criminalise unauthorised access to, and illicit tampering with, systems, programs or data.[4] In particular, Title 1 obliges Member States to enact offences for illegal access, illegal interception, data interference, system interference and misuse of devices.

Title 2 of the Convention, on the other hand, criminalises the computer-facilitated commission of fraud and forgery. Title 5 provides for ancillary liability for those that assist in the commission of the core and computer-related offences discussed above.

At a high level, Microsoft found that there was very strong alignment between Australia's current cybercrime framework and the Cybercrime Convention in the areas of: (1) The data interference offence; (2) Computer-related forgery and fraud offences; (3) Ancillary liability for attempting, aiding or abetting Cybercrimes, and (4) Corporate criminal liability for Cybercrimes.

The analysis also found that there was scope to strengthen provisions around: (1) Illegal access; (2) system interference, and (3) The misuse of device offences.

The Australian 'Gap Analysis' of the Council of Europe's Cybercrime Convention

Microsoft looked at both Federal and State/Territory legislation but principally focused on the Federal Criminal Code Act of 1995 (Code) as amended in 2001. The amendments to the Code introduced a range of computer security offences based on Chapter 4 of Australia's Model Criminal Code. Although this regime is broadly equivalent to that found in the Convention on Cybercrime, its application is narrower: for Constitutional reasons, the Code's offences only apply in respect of data held by, or on behalf of, the Federal Government or in relation to acts undertaken by means of a telecommunications service.

In terms of state and territory legislation, New South Wales, Victoria, South Australia and the two territories (Australian Capital Territory and the Northern Territory) have implemented the Model Criminal Code and thereby established computer security regimes that are materially similar to their federal counterpart. The Queensland, Tasmanian and Western Australian regimes are less aligned with the Model Criminal Code; they appear to focus on computer hacking and misuse offences. Importantly, all state and territory computer security offences apply generally in the jurisdiction to which they pertain and thereby regulate conduct that falls outside the federal

[3] Title 3 of the Convention requires signatories to criminalise certain types of computer-facilitated dealing in child pornography; these offences are addressed in section 5 (Online Child Safety Laws) of this overview. Title 4 of the Convention requires signatories to criminalise certain types of intellectual property infringement; these offences are beyond the scope of this overview.

[4] Convention on Cybercrime (ETS No. 185) Explanatory Report.

legislation for constitutional reasons.

Core offences (Title 1 COE): Illegal access, illegal interception, data interference, system interference, misuse of devices

The Code's unauthorised access offence only applies in respect of data that is protected by an access control system (this qualification is permitted by the Convention). The Code's data interference offence is likely to regulate a broader range of conduct than its Convention counterpart due to its application to reckless data interference as well as that caused intentionally.

The act of illegally intercepting communications is not regulated by the Code, although dealing in and possessing interception devices is regulated.

The Code does not contain an equivalent to the Convention's system interference offence, but its unauthorised impairment of electronic communications offence is targeted at denial of service attacks in the same way that the Convention system interference offence is (at least in part). Similarly, the Code's offences in respect of producing, supplying, possessing or procuring data (which is defined as including computer programs) with intent to commit a computer security offence, are best viewed as a partial implementation of the Convention's misuse of devices offence.

Contraventions of the Code attract terms of imprisonment ranging from 2 to 10 years depending on the seriousness of the offence. Where unauthorised access or data interference is preparatory to the commission of another offence under the Criminal Code, offenders face the penalty associated with the latter offence.

Computer-related offences (Title 2 COE): Computer-related forgery, computer-related fraud

Although the Criminal Code does not contain a specific computer-related forgery offence, its general forgery offences in Part 7.7 of the Code are likely to cover the same conduct. This is principally because "document" is defined in section 143.1 of the Code to include material capable of being responded to by a computer, machine or electronic device, or from which information can be reproduced.

Similarly, the Code's general fraud offences are capable of regulating computer-related fraud; "deception" is defined to include conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

Those who offend the Code's forgery and fraud offences are liable to imprisonment for up to 10 years. These provisions, along with the Code's financial information offences, are likely to assist with the prosecution of credit card and phishing schemes.

Ancillary liability (Title 5 COE): Attempt and aiding/abetting, corporate liability

Generally it is an offence to attempt to aide or abet the commission of each of the above mentioned computer security offences. However, there is no accessorial liability for producing, supplying, possessing or procuring data with intent to commit a computer security offence, or in respect of the offence of unauthorised access or data interference that is preparatory to the commission of another offence under the Code.

The Code also addresses corporate criminal liability. In most cases, corporate criminal liability is established by attributing an offence's fault element to the body corporate where the body corporate can be said to have expressly, tacitly or impliedly authorised the commission of the offence. Bodies corporate can face fines of up to 5 times the amount that can be imposed on an individual for the same offence.

As can be seen in the analysis above, Australia has demonstrated a solid commitment to robust legislation, but could further strengthen some of these provisions in closer alignment with the Cybercrime Convention. Australia has already been playing an important role in achieving regional and global consistency. It is effectively functioning as a policy bellwether for the region.

Scope for Closer International Collaboration and Harmonisation

It is interesting to note that while Australia is clearly aligned with the goals of the Convention, it is not yet a signatory and no country in the region has ratified the Convention. This stands in contrast to the forty-seven nations around the globe – both developed and developing nations - which have signed the Convention and the nineteen that have ratified it, including the USA. So too, Japan is a signatory to the Treaty, the Philippines and Sri Lanka have requested accession to the treaty and Indonesia expects to do so soon.

Particularly in view of the Australian Government's increasing engagement/cooperation with multilateral processes and forums, Microsoft believes that Australia could further assert its leadership in this space and benefit from a number of the provisions a treaty of this nature would provide, by considering accession to the Convention.

There are a number of benefits that will extend to Australia by it becoming a party to the Convention, including 24/multilateral access to information sharing agreements and the opportunity to help frame future versions of the Convention. Microsoft considers that the benefits to Australia from acceding to the Treaty will ultimately outweigh some of the immediate challenges and would further establish Australia's leadership credentials in the Asia Pacific region.

Microsoft is not aware of a specific reason as to why the Australian Government might be resistant to ratifying the Treaty. We would certainly be interested in having a clearer understanding as to the issues, whether policy or political, that may be impeding Australia joining this global treaty.

Legislation around Identity Theft and Criminalisation of Malware and BotNets[i]

As new technology threats emerge, it is sometimes necessary to re-evaluate whether current national and local laws – or major Conventions – may need to be updated. In a number of jurisdictions, there has been a proliferation of new legislation addressing specific offences around identity theft, malware and botnets, which may be something for the Australian Government to consider.

In terms of identity theft legislation, the Australian Government is clearly working to improve identity security, combat identity crime and protect the identities of Australians in general through current initiatives, including:

- The National Identity Security Strategy;
- The National Document Verification Service (DVS); and
- The ID Theft Kit.

The Model Criminal Law Officers Committee (MCLOC) is currently preparing a final report in which it is expected to propose that all Australian jurisdictions, including the Commonwealth, enact model identity crime offences.

It is likely that the model offences will prohibit:

1. Identity theft;
2. Identity fraud;
3. On-selling identity information; and
4. Possessing equipment to manufacture identification information where the offender is reckless with respect to the information being used for an unlawful purpose.

It is interesting to note that the COE, as part of the "Project on Cybercrime," has commissioned a paper prepared by Dr. Marco Gercke of the University of Cologne, entitled, "Internet-Related Identity Theft," which compares the US approach to identity theft legislation with the approach taken in the Budapest Convention to legally addressing Cybercrime.

The paper notes that:

> *"The Convention on Cybercrime and the criminalisation of identity theft in 18 U.S.C. § 1028 and 18 U.S.C § 1028A are based on two different systems. § 1028 and § 1028A create separate offences that – in addition to the offences they are referring to – criminalise the transfer, possession and use*

of means of an identification of another person with regard to criminal offences. The Convention on Cybercrime follows a different concept. It does not create a separate offence that criminalises the unlawful use of identity-related information in cybercrime related cases, but instead criminalises certain acts that are related to identity theft scams."

Specifically, the paper notes that the Convention approach uses separate articles and provisions including misuse of devices (Article 6), computer-related forgery (Article 7), and computer-related fraud (Article 8) to address identity theft. The paper can be found in its entirety at: www.coe.int/cybercrime . As such, it may bear consideration for Australia to look at implementing a comprehensive federal statute that gives Australian law enforcement the best possible tools to enforce this proliferating crime type.

A number of developed countries are also looking at additional legislation to criminalise botnets and malware and provide stronger protections in the wake of these more virulent strains of Cybercrime. The Japanese Diet is currently considering a bill to amend the Criminal Code to address the creation, dissemination and use of "illegal instructions" such as computer viruses and malware.

Specifically, the Draft Law for Partial Amendment of Criminal Code in Response to Growing Criminal Internationalization and Organization and More Sophisticated Information Processing criminalises the acts of:

- preparing or providing, for the purpose of execution on a third party's computer, an electromagnetic record which, when a person uses a computer, gives an illegal instruction to avoid an action or perform an action not intended by the user (maximum penalty: 3 years' imprisonment with labour or a fine of up to JPY500,000);

- acquiring or keeping, for the purpose of execution on a third party's computer, an electromagnetic record which, when a person uses a computer, gives an illegal instruction to avoid an action or perform an action not intended by the user (maximum penalty: 2 years' imprisonment with labour or a fine of up to JPY 300,000, and;

- attempting to commit the crime set out in Article 234 of the Criminal Code, which criminalises the act of intentionally, knowingly and illegally causing disruption to, or interference with, a computer system that is used, or intended to be used, for business transactions.

In addition to criminalising the production, dissemination and use of files that contain viruses and malware, the bill also appears to criminalise the preparation and production of electromagnetic and other records which set out the "illegal instruction".

So too, there are a number of pending bills in the United States that look at variously creating offenses to target botnets, malware, spyware and Cybercrime driven by organised criminal operations. These include bills such as the "Internet Spyware (I-SPY) Prevention Act, "the Cybersecurity Enhancement Act," and the "Counter Spy Act."

As online criminals increasingly access and control protected networks of computers remotely and without authorisation, creating "botnets" of literally hundreds of thousands of machines that are used to attack other machines, perpetrate identity theft, spread spyware and malware, or disrupt Internet functions, more needs to be done to identify, stop and prosecute these criminals ("botherders").

Microsoft considers that this needs to be done in a way that doesn't discriminate between one technology and another – that may be used for either good or ill purposes – and that the legitimate downloading of software – such as Automatic Updates, to patch vulnerable machines – should not be criminalised in the process.

Finally, Microsoft commends the commitment and resources the Government has already put into providing additional resources for the Australian Federal Police (AFP) and other Federal law enforcement agencies to stay ahead of the increasing scourge of cybercrime.

The need for more dedicated law enforcement personnel and advanced forensic tools to investigate and assist in the prosecution of computer crimes is critically important in the states and territories as well – there may be a role for the Australian Government to help bridge this gap and provide greater resources, access and capacity building

opportunities for local law enforcement.

Partnering with the Australian Government for Protection

Any successful strategy must include protecting one's own networks from attack – Microsoft provided our detailed view on critical infrastructure protection (CIP) in the National E-Security Review. For both CIP and cybercrime cooperation, it is critical that the government and private sector work together to improve the state of computer security. Partnership in this realm is critical because the private sector drives the design, development and implementation of the products and services that power cyberspace. For years the goal of the partnership has been "information sharing" which will not, without more effort, secure Australia's infrastructures or bridge the current gaps in policy. We must establish a more meaningful public-private partnership, where the partners work in complementary fashion towards the clearly identified objective of securing Australia's networks. Consistent with this philosophy, the partnership should focus on sharing information that is actionable and building mechanisms that enable meaningful action to be taken.

That said, Microsoft commends the Australian Government's efforts at encouraging broad-ranging, multi-sector partnerships to facilitate industry and government collaboration. Of particular note in the E-Security and CIP space, we would like to applaud the Government's efforts around the formation of the Trusted Information Sharing Network (TISN), the IT Security Experts Advisory Group, the Business-Government Advisory Group on National Security (BGAG) and the Supervisory Communications and Data Acquisition (SCADA) Community of Interest.

So too, Microsoft was fortunate to participate in both Cyber Storm I and II. Microsoft, like every organisation that participated, had its own exercise objectives, as well as supporting other players to achieve their objectives. In doing so Microsoft gained significant insight into the international exercise and was able to successfully exercise its own Software Security Incident Response (SSIRP) processes.

Microsoft Australia, in the after-action reporting for Cyber Storm II, provided feedback on three key areas that we felt needed focus on from Government and industry directly to the participating agencies and as part of our submission to the E-Security Review. Microsoft looks forward to participating in Cyber Storm III.

We would encourage the Government to evaluate the efficacy and contribution of each of these groups, assess where there might be duplication and overlap as well as areas that may require greater consultation and collaboration, to determine what Government-sponsored collaborative efforts should continue into the future.

Partnerships between Government and the information technology industry offer the potential for achieving progress in the protection of citizen interests in the online world.

Identity and End-to-End Trust

As people look to engage in an increasing number of personal and commercial activities online, it is important to address their growing demands for both security and privacy. To meet these demands requires evolving a security strategy that facilitates the creation of a "Trusted Stack" and enabling "End to End Trust" in an online experience. "End to End Trust" is Microsoft's vision for a safer, more trusted Internet that can only be achieved through broad cross industry collaboration and alignment.

Fundamentally, if we want the Internet to reach its full potential, we need a safer, more trusted online environment. To that end, Microsoft and other companies continue to make progress on security and privacy issues. For seven years, and as a result of our focus on Trustworthy Computing , Microsoft has made significant progress toward improving the security and privacy of our products and services. We embraced the Security Development Lifecycle (SDL), as well as "defense in depth" and threat mitigation technologies. Along with our industry partners, we continue to build a more secure, private and reliable computing experience. But Microsoft and the technology industry alone cannot create a trusted online experience. For that to happen, industry must not only band together but must work with customers, partners, governments and other important constituencies on a road map for taking Trustworthy Computing to the Internet.

To explain this vision further, we believe that there are three key pieces to creating greater trust on the Internet. The first is creation of a trusted stack where security is rooted in hardware and where each element in the stack (hardware, software, data and people) can be authenticated in appropriate circumstances. The second piece involves managing claims relating to identity attributes. We need to create a system that allows people to pass identity claims (sometimes a full name perhaps, but at other times just an attribute such as proof of age or citizenship). This system must also address the issues of authentication, authorization, access and audit. Finally, we need a good alignment of technological, social, political and economic forces so that we make real progress. The goal is to put users in control of their computing environments, increasing security and privacy, and preserving other values that we cherish such as anonymity and freedom of speech.

Microsoft believes the opportunity is *now.* Some serious issues, such as botnets, ID theft and child safety have served to focus people's attention on security and privacy issues. Some important technologies, such as public key infrastructure (PKI) and smart cards, are now mature enough for broad deployment. Some important debates, such as how to achieve more security and more privacy instead of trading one for the other, have led to new thinking about how we can create a more secure *and* privacy-enhanced Internet. And we have learned through past experience how to align technology, social forces, political will and market dynamics to achieve great progress on important issues, just as we have learned why important efforts sometimes fail.

The Australian Government can establish key capabilities with industry which will establish an environment where reasonable and effective trust decisions can be made. Any security strategy must include an ecosystem strategy and product, and/or service strategy that maps to it. Home and car alarms are not valuable without neighbours and/or police who can and will respond.

The following outlines the capabilities as part of the "Trusted Stack" that Microsoft views the Australian Government can assist to enable:

1. Claims based Identity ecosystem;
2. Software reputational services;
3. Product assurance;
4. Trusted Data and transactions, and;
5. Information sharing.

The following sections discuss each of these capabilities in more detail.

The most important element is an authenticated identity claim (e.g., name, age, or citizenship). In the absence of the ability to authenticate a person (or a personal attribute), machine, software, and/or data and in the absence of the ability to combine that authenticated data with other trust information (e.g., prior experience, reputation), effective trust decisions cannot be made.

Who does the person or what does the device or software claim to be? As a starting point, someone may claim to be a given person (e.g., John Smith) or simply claim to have a certain attribute (e.g., I am over 18 years of age). A device may claim to be an eBay server or a router, and an application may claim to be a particular version of Microsoft Office Word. The claim may also relate to source or integrity (this is a packet from an X Company router, or this spreadsheet was sent from John and has not been altered since being sent).

An identity claim is only one part of the equation. In many contexts, reputation is equally critical and (especially because it is hard to speak about identity in absolute terms) will serve to add additional layers of assurance to an identity claim. This will be the case regardless of which element the claim attempts to validate.

Robust reputation policies, processes, and systems will need to be built out to support the many trust decisions people need to make. Put another way, if a person claims to be John Smith, but you have never met John Smith before, the identification does not provide enough information to warrant a trust decision. Thus, closely related to the issue of identity are other attributes that are linked to that identity (e.g., past experiences, relationships, reputation). A current example of this dilemma exists in the area of child online safety where authorities are seeking to look —mostly unsuccessfully—for ways to distinguish minors from adults. In the absence of evidence capable of independent verification, a claim to be a minor is no more than that – a claim.

The problem relates to how identity is determined in an electronic world. It is well-known that there are three ways to establish identity: what you know (e.g., a shared secret), what you have (e.g., a token or smartcard), and what you are (a biometric). For the most part, electronic identities have been established by having people disclose information that is known only by parties to the transaction, information sometimes called a "shared secret" (for example, your mother's maiden name).

In the Internet context, this form of enrolment is no longer a sound method. The problem is that these shared secrets are increasingly stored and accessible online and, due to the increasing effectiveness of search tools and the increasing number of data breaches, shared secrets are no longer secret at all. In sum, the claim of identity is not robust and the authentication mechanism is flawed.

A safer Internet needs to support the option of identities based directly or derivatively upon in-person proofing, thus enabling the issuance of credentials that do not depend upon the possession of a shared secret by the person whose identity or identity claim is being verified. To some extent, government activities and markets themselves are driving in-person-proofing regimes. For example many governments are issuing (or considering issuing) e-ID cards for government functions.

In-person proofing need not be controlled by governmental or quasi-governmental organisations. Banks often have relationships with their customers that start with branch visits. Schools have relationships with students and may routinely take in-person attendance. Employers know their employees and often issue identity cards based upon in-person proofing.

The creation of a distributed identity system that avoids shared secrets and has in-person proofing at its base has another salutary purpose: it allows us to devalue personally identifiable information (PII) and make a serious effort to reduce identity theft. This being true, it becomes clear that the key to combating ID theft is to devalue PII. If in-person proofing allows the issuance of true secrets (public-private key pairs), which can then be used for authentication, then criminals with access to PII do not have the key piece of data needed to consummate a transaction (e.g., obtain a line of credit at a bank), and the value of both social engineering attacks and intrusions into databases containing PII drops.

The Australian Government should work with industry to support the option of electronic claims-based identities based directly or derivatively upon in-person proofing.

Computers were designed to run code, without concern about its authorship or the intent of that author. Today there are multiple ways to help protect people from software vulnerabilities and malicious code. To protect users from vulnerabilities, code can be rewritten in safer languages, checked with analytic tools, compiled with compilers that reduce vulnerabilities (e.g., buffer overruns), and sandboxed when executed.

To protect against malicious code, there are firewalls, anti-virus programs, and anti-spyware programs. But although these approaches make users safer, criminals are not deterred by such preventive measures. To increase accountability, there is another effort that must be undertaken: code signing so that source can be better identified.

Knowing source permits users to consider prior experiences, reputation, and other factors in deciding whether to install software. This is more problematic than it sounds for a host of reasons. For example, many exploits use code injection to bypass the loader which checks to make sure code is signed. Assuming users routinely reject unsigned code the market response will be to provide signed code.

Even if code is signed, however, it will still fall into one of three buckets. There will be code that is signed by a known entity (e.g., Microsoft, Oracle, Adobe) that is trusted due to past experience, brand reputation or some other factor. There will be code that is signed but known to be malware (e.g., spyware, which can then be blocked). Finally there will be code signed by entities that are not known to the user.

Depending upon the criteria for obtaining a signature, the signature process itself may provide some deterrent to misconduct, much as extended validation certificates do today by providing a more extensive background investigation of the organisation seeking the certificate. If code-signing signatures remain easy to obtain with no proof of physical identity, then any deterrent effect is lost and users have no assurance that malfeasance caused by

the code can be addressed.

Even assuming the signing process is robust users may not find signing sufficient to make a trust decision. Although users could address such concerns by simply refusing to run any code from a source not very well known, this would seriously undermine some of the advantages of the software economy: low barriers to entry and inexpensive global distribution channels.

Microsoft uses the Security Development Lifecycle (SDL) - an industry-leading software security assurance process. A Microsoft-wide initiative and a mandatory policy since 2004, SDL has played a critical role in embedding security and privacy into Microsoft software and culture.

To support the growth of the software market, a reputation platform will also be needed to provide users with data about software publishers. This data may come from many sources: expert reviewers and researchers, other users, and reports of complaints (e.g., to consumer organisations, business organisations, and governments).

The Australian government should work with Industry to establish a reputation platform that facilitates code signing so that better informed trust decisions can be made by end users.

Many governments worldwide are seeking a better way of assessing the security and assurance of software. While the international Common Criteria provides a framework for evaluating a product's security features, they have not proven effective at recognising products that are likely to resist hostile attack.

Several governments have conducted an experiment aimed at developing and evaluating a new evaluation paradigm that would recognise the benefits of security-focused development processes. One aspect of this experiment was a trial evaluation of a Microsoft product (Virtual Server 2005 R2) that had undergone the SDL. The evaluation experience was successful for both Microsoft and the evaluation agencies, and Microsoft has encouraged the international Common Criteria community to evolve the Common Criteria to a process that would recognize the importance of effective security-oriented development practices such as the SDL.

The Australian Government can assist in this process of developing more secure software by focusing further investment on research, especially basic research, into information technology security. This investment should seek to address both future problems as well as address those existing challenges in current software. Government investment can also encourage capacity building and support the education of those who will in the future be responsible for managing software security.

Applications should incorporate seamless mechanisms for applying signatures to their outputs, and read signatures before opening documents, so that data origin and data integrity can be easily checked. At the same time, management tools should permit users to apply policies based upon data origin and integrity so that fewer ad-hoc trust decisions are required.

While it may be important to know the source of data, it is also important to ensure that data is not accessed by unintended recipients. One of the benefits of creating this authenticated infrastructure for data and transactions is that it also permits senders to restrict access to data to authenticated individuals.

Improved authentication and audit capabilities would generate a host of other opportunities, especially if robust management tools permitted users to increase the amount (or change the type) of audit data collected, depending on the trust level based on the data or transaction being accessed. This helps to balance the need for evidence with the cost of collecting and storing data.

This is an important privacy protection. Far too often, sensitive data is shared too broadly or is too easily accessed by unauthorised individuals. As the firewall continues to diminish in importance, it is important to focus on protecting data as opposed to simply protecting the machines that store such data. Using the "Trusted Stack" to limit the flow of data mitigates the privacy harms that stem from unauthorised data flows and unauthorised data access.

The Australian Government has been undertaking market leading efforts with the VANguard Program which provides authentication and notary services to facilitate online business with government agencies. Consideration

should be given to how the VANGuard program could be leveraged with Industry to provide a trust authentication framework for electronic transactions. The Notary services to be provided by VANguard in providing agencies with independent, verifiable electronic evidence of the date, time and integrity of an electronic document could be used as a model and framework to be leveraged by Industry.

By expanding this service the Australian Government could provide this authenticated infrastructure for data and transactions.

The imperatives of commercial action are often seen as a barrier to the development of trusted relationships between those commercial entities and governments. In reality, there are common interests that can support a trust relationship between the public and private sectors. Governments can help to build information-sharing relationships, operational response mechanisms and strategy frameworks that include both public critical infrastructure operators and commercial entities for the purpose of maintaining situational awareness and rapid response to prevent, mitigate, and recover from nationally or globally significant threats

Microsoft has been engaged in a number of such relationships with the Australian Government over the past six or more years:

> **Microsoft Security Co-operation Program (SCP)**: The SCP is a global initiative that provides a structured way for governments and Microsoft to engage in cooperative security activities in the areas of computer incident response, attack mitigation, and citizen outreach. Currently, DSD operates the SCP within Australia.
>
> **Government Security Program (GSP):** The GSP is a global initiative that provides governments with access to the Windows source code, technical information, and development staff. GSP helps governments to better evaluate their existing systems and to more securely design, build, deploy, and maintain future computing infrastructures, while developing partnerships and mutual trust for future collaboration. Currently, DSD operates the GSP in Australia primarily driven by the needs to evaluate the assurance of Microsoft products.
>
> **Microsoft Security Response Alliance (MSRA)**: MSRA allows Microsoft to take lessons learned from those individual alliances (Virus Information Alliance, Microsoft Virus Initiative, Microsoft Security Support Alliance, Global Infrastructure Alliance for Internet Safety, Microsoft SCP) and use them to build a comprehensive, consolidated alliance framework that can help meet the security response needs of Microsoft customers. Currently the Australian Government has access to the MSRA via its SCP agreement.

Societies and governments and the critical infrastructures on which they depend face significant and growing cyber-security challenges. Working with our government partners and industry peers, Microsoft is committed to pre-empting, detecting, and deterring cyber-criminals both to protect the computing experiences of our customers and the cyber-security of the critical infrastructures that unite us.

A lot of good work has been done to improve the security and privacy of Australian citizens however a key question remains - as we become increasingly dependent on the Internet for all our daily activities, can we maintain a globally connected, anonymous, untraceable Internet and be dependent on devices that run arbitrary code of unknown provenance?

If the answer to that is “no,” then we need to create a more authenticated and audited Internet environment - one in which people have the information they need to make good trust choices. It is critical to understand the end goal: a more secure and trustworthy Internet ecosystem.

To that end, creating the ability to identify what person and which device is sending a particular data stream in cyberspace must be part of an effective cyber security strategy. Even sophisticated attackers face difficult challenges – and find their access restricted – because of better authentication. Stronger authentication can also help us create safe places for our children to learn online, for businesses to interact with customers, and for government to serve its citizens. In addition, because the use of digital IDs also reduces the need to authenticate people by having them provide private details about themselves, stronger authentication can enhance both security and privacy.

Thus, as part of an overall cyber security strategy, the government should accelerate the adoption of authentication technologies by actions such as issuing and accepting digital credentials in appropriate circumstances, and working to integrate privacy issues into the design, development and operation of the resulting identity meta-system.

Promoting a National Culture of Cybersecurity: Outreach and Awareness

Improving public awareness around both the benefits and risks that technology and Internet access can provide is an important frontline defence for creating a safer and wiser populace.

To help keep consumers, businesses, organisations, and developers current with the latest news and trends in security, privacy, and Internet safety issues, Microsoft offers education and guidance through newsletters, updates, online and offline training, and through various partnership efforts. Our "one-stop shop" for all privacy, security and online safety information is accommodated in our "Protect" web site which has been localised into 24 languages and deployed in 35 countries across the globe.

In Australia, you can find localised and up-to-date information on www.protect.com.au/protect. We also make all of the information contained on the Protect website available to any organisation for free and neutrally-branded "content syndication". This is just one of many efforts Microsoft undertakes to help raise awareness and help consumers protect themselves but we believe that much more can be accomplished through partnership.

As internet safety information proliferates and a range of companies, Governments and other entities make such guidance available, there does run the risk of creating confusion amongst consumers. This is one important area where we believe that Government's can take an important leadership, stewardship and coordination role, as Australia has demonstrated through a number of recent initiatives.

Two good examples of such coordinated, multi-sector efforts include the "Scams Target You: Fraud Fortnight" initiative and National E-Security Awareness Week initiatives. The creation of the related www.scamwatch.gov.au and www.staysmartonline.gov.au websites do a great job at consolidating important information and resources for Australian consumers and businesses in two well-structured and rich web sites. The joint collaborative outreach efforts help achieve great cut through and awareness which is more powerful when delivered by multi-sector partners.

Such efforts require a substantial amount of planning, resources and coordination amongst a broad range of players over an extended period of time. Notwithstanding this investment, the surge in activity penetrates the airwaves for only short periods of time once or twice a year. To achieve greater cut through would require a continual reinforcement of these messages over an extended period of time. Only then could behavioural change be expected.

As a first step, it is important to consolidate potentially overlapping efforts. Secondly, it may make sense to keep the current structures of annual "surges," or mass consumer campaigns for Scams Target You and NEAW, but punctuate these with smaller periodic (perhaps quarterly) campaigns around various designated E-Security or Cyber safety issues with a smaller subset of the coalition players. Again, an analysis or a stock-take of current Government-Industry efforts that serve to further the interests of cybersecurity might be considered to maximize resources and ultimately, impact on consumers.

Cybersecurity Education

There are important synergies that could be leveraged through the Government's commitment to the Digital Education Revolution and internet safety education. The Government's goal of equipping every Australian child with the necessary tools, skills and capacities to prosper in the digital age is forward looking and revolutionary. However, without guidance, training and support in internet safety and online security, the program could place many young people in situations of high personal or financial risk.

For many years Microsoft has partnered with a number of organisations worldwide to help create robust educational curriculum for internet safety education in the schools, including partnerships to foster the

development of the "iSafe" and "Look Both Ways" internet safety curricula. As such, we are very supportive of the Government's planned efforts to roll out E-Security curriculum to Australian students in grades 3 and 9.

With the passage of the National Safe Schools Framework, and other related initiatives, a number of schools across Australia are already teaching basic internet safety practices, but many do not and many others do so incompletely.

In a number of jurisdictions around the world consideration is being given to making internet safety education an integral part of the curriculum. The US state of Virginia currently has a law requiring mandatory online safety education in its public school system. Other states in the US are considering such laws and are taking steps to promote online safety, which is increasingly viewed as a basic element of the basic curriculum, just as schools currently teach basic drugs, fire, traffic and crime-prevention safety.

Safety education is one of the most effective means of helping to protect children online and we encourage the Government to look at deploying its E-Security curriculum efforts beyond grades 3 and 9 – particularly as many children at very early ages are now readily accessing the internet either via home personal computers or mobile devices. Starting early to building core awareness of the facts of online interactions, helping children to recognise threats, and encouraging them to discuss issues with parents and guardians, helps kids avoid online risks before real harm occurs.

In some ways, internet safety education may be more effective than regulating what content kids and other citizens have access to on the Internet. Safety education need not be mandated, unfunded or difficult to implement. A number of curricula and resources exist and are available for free, including the programs from NetSmartz, "Look Both Ways," WebWiseKids, Wired Safety/TeenAngels, and the i-SAFE 'iLearn' online modules Microsoft helped develop.

Just as the Federal Government is stewarding the Digital Education Revolution effort and bringing laptops and related computer technologies to schools across the nation, so too should there be consideration – through co-operative Federalism - for a consistent, national baseline curriculum that is taught around E-Security and Cyber safety in schools.

Basic curriculum to teach Australian students basic Internet awareness might include:

- Cyber Safety: How to interact online safely and recognize and avoid sexual solicitation, child predators and other sexual risks;
- Cyber Security: how to recognize and avoid identity theft and internet fraud; and
- Cyber Ethics: how to be a responsible cyber citizen.

Microsoft, in cooperation with the Australian Federal Police (AFP), is seeking to play its part in the spreading of basic internet safety and E-Security education for parents, teachers and carers through the ThinkUKnow pilot, which was launched in pilot form in February, 2009 and will be rolled out nationwide in Term 1, 2010. Already, our collective volunteers have reached more than 2100 parents, teachers and carers. Through the national roll-out, Microsoft and AFP volunteers will team up to be deployed to local schools to help educate parents, teachers and carers be better educated about how kids are using technology, how to stay involved in their online lives, what risks to look out for and how to address problems as they arise.

This is just one program and by no means a substitute for the level of education that is truly required to target kids through age-appropriate curriculum delivered in the schools.

As part of the current SCP agreement the Australian Government has access to collaborative educational resources to enhance computing safety and increase IT security awareness for a broad audience including government employees, students, and the general public. The collaborative educational and outreach resources include the following:

- On-site training event for government employees;
- Delivery of computing safety training to students in a mutually agreed upon set of educational institutions, and;
- Distribution of syndicated Microsoft-developed content providing safe computing guidance,

including videos for broadcast television public service announcements, radio public service announcements, and Web content.

Microsoft believes that Government-led, industry and NGO collaborative efforts around E-Security awareness including Scams Target You and National Security Awareness Week should continue. However, there may need to be consideration as to where such initiatives may be duplicative and consideration given to ways to deliver more consistent "surges" of security and safety education awareness to the Australian public. Further, as the Internet and IT become key tools for education, the Government may want to consider expanding planned E-Security and Cyber safety education efforts in the schools more broadly and consistently.

Another important consideration would be looking at the prospect of mandatory internet safety education as a requirement for school curricula nationwide. Finally, the Government may want to evaluate how to incorporate more security collateral into ICT curriculum and training programs to raise the level of security awareness capabilities across the ICT industry.

Conclusion

As indicated by our broad reliance on IT, it is clear that a country's success is dependent upon information, knowledge, and communications. While the growth of the Internet in the early 90s created new beneficial opportunities for all, including individuals, businesses, and governments, it also created unprecedented opportunities for those who would misuse technology. It permits individual criminals, organised crime groups and nation-states to target all types of sensitive information, from personal information to business information to military information.

As such, Microsoft Australia would ask that the Committee consider five major themes and considerations.

The first is whether Australia should consider a comprehensive national cyber security strategy coordinated by a single entity at the highest level of Government, like the US has implemented with a White House-led strategy. Secondly, what can be done in Australia to further evolve and focus the public private partnership model? Third, what changes to legislation could be made to protect technology innovation while providing appropriate government oversight of cyber security issues? Fourth, as the Internet needs an appropriately deployed identity meta-system if we are to make the Internet dramatically more secure but protect important social values, such as privacy and free speech what role can the Australian Government play in helping to both achieve these goals and balance these imperatives? And finally, an important priority should be to consider what more Australia can do to continue serving as a bellwether for legislative policy in the region as well as a global contributor to greater harmonisation and cross-border collaboration.

Microsoft would submit that becoming a signatory to, and ratifying the Council of Europe's Cybercrime Convention, would be an important step in that direction.

Microsoft Australia very much appreciates the opportunity to provide this submission. For further information, please contact Julie Inman Grant, Director of Internet Safety and Security.