E-SECURITY REVIEW 2008

Submission from Microsoft Australia

Introduction

Microsoft Australia welcomes the opportunity to participate through this Submission in the Whole-of Government Review of E-Security. A periodic review of the E-Security 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 - which have revolutionised the way information is created, stored, shared, and used. Today, powerful, affordable and diverse devices, together with expanding broadband networks, create a powerful opportunity for connectivity for individuals and communities.

Over the past two decades, 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.

Our broad reliance on software, services, and communications, along with the benefits they offer, has naturally attracted the malevolent interest of terrorists, criminals, and other sophisticated attackers. To address this threat requires unprecedented cooperation and constant effective action by technology vendors, governments, businesses, and consumers.

Drawing upon work with global partners, coupled with more than three decades of experience, Microsoft has learned that effective critical infrastructure protection efforts will share three central areas of focus: the implementation of trust based plans and policies, the development of resilient operations, and the dedication to innovative investments.

This submission examines the questions raised in this E-Security Review under seven headings:

1. A Framework for Evaluating the Efficacy of the E-Security Environment;
2. The Changing Threat Landscape: The Pursuit of Fortune vs. Fame;
3. Developing a National Security Strategy;
4. Deterring Cybercrime: The Current Australian E-Security Policy Framework and Proposed Changes;
5. Improving Critical Infrastructure Protection and Creating National Incident Management Capabilities;
6. Industry and Government Collaboration: Partnering with the Australian Government for Protection; and
7. Promoting a National Culture of Cybersecurity: Outreach and Awareness.

At the end of each section, where appropriate, a series of recommendations have been included.

Microsoft makes these recommendations on the basis of both the environment we perceive in Australia and the opportunities we consider flow from that environment when considered in the context of our international experience of Cybercrime and best practice in the E-Security Environment.

1. A Framework for Evaluating the Efficacy of the E-Security Environment

The International Telecommunications Union (ITU)'s Study Group Q.22/1 has published a draft report on, "Best Practices for a National Approach to Cybersecurity: A Management Framework for Organising National Cybersecurity Efforts." This report provides national administrations with a management framework for addressing Cybersecurity at the national level and for organising and implementing a national Cybersecurity strategy.

The report is not intended to be prescriptive and its approach was recently discussed at-length with a range of Asia-Pacific regional stakeholders at a Cybersecurity conference jointly sponsored by the ITU and the Australian Department of Broadband, Communications and the Digital Economy (DBCDE) in Brisbane July 15-18, 2008.

While the report largely addresses potential national approaches to Cybersecurity, these approaches can be applied to critical infrastructure protection and, we believe, provide a useful framework for evaluating Australia's national approach to E-Security.

The five key elements outlined in the ITU report are:

1. Developing a National Strategy for Cybersecurity;
2. Deterring Cybercrime;
3. Establishing National Government-Industry Collaboration;
4. Creating National Incident Management Capabilities, and;
5. Promoting a National Culture of Cybersecurity.

Microsoft sees merit in using this framework for evaluating the relative strengths and weaknesses of the current E-Security framework in Australia. The five key elements of the ITU report are sufficiently broad as to allow clarity in definition and actively achievement oriented so as to allow a process evaluation of progress and goal attainment.

2. 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, criminal financial gain is the 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 and 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 our 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," 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 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) 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 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).

Consistent with the global trend observed in 2007, there was a large increase in the detection of Trojan Downloaders and Trojans in Australia. 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.

Microsoft has also monitored categories of "potentially unwanted software" in Australia.

This category of software may include adware, spyware, software bundlers or remote control software. In Australia – as in the rest of the world – adware was the most prevalent form of 'disinfection' performed of potentially unwanted software.

More than 1 million potentially unwanted software disinfections were performed in Australia in 2007 - 415,727 in the first half of the year and 662,208 disinfections in the second half of the year. Disinfections of potentially unwanted software grew more than malware disinfections between the two halves of the year due, in part, to the increased prevalence of adware in Australia throughout 2007.

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 5 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 depends on "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. 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. This was underscored in a recent meeting of Telecommunications Ministers in Korea with an urgent call to tackle issues of identity and privacy.

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 versus 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 BotNets

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*[1].

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.

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 E-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.

---

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

Threats to the availability of ICT services: In 2013 the reliance of ICT services delivered via the connected world between Governments, businesses and individuals will be significantly greater than in 2008. Consequences arising from a major disruption or a significant loss of availability could have a profound impact on the economy, national security and social order. This is particularly true as advances are made in delivering technology and services around health care, education and finances – potentially putting more sensitive and valuable personal information and data online.

- ***Economy***: The threat to the Australian economy is not just about disrupting high value transactions and critical infrastructure. It goes further and imagines the disruption of business processes that have been migrated to the ICT world. That disruption is amplified by every user and organisation that cannot complete a transaction, cannot pay a bill, cannot communicate or make a phone call. The net result will be massive financial losses to individuals and commercial entities, reductions in revenues for government and loss of confidence by the public.

- ***National Security and public safety***: In 2013, Australia's ability to protect its national interests and the public will rely even more heavily on the availability of ICT services. A massive disruption to availability would likely impair our ability to respond to a myriad of incidents, from general law enforcement and emergency response activities through to our ability to wage a campaign to protect ours or an ally's sovereignty. Massive disruption would also have direct consequences for critical public services such as energy, health, transport networks and other critical infrastructure services further diminishing the ability to maintain national security and public safety.

- ***Social Order***: The Australian society of 2013 will rely heavily on the availability of ICT services to socially network, communicate, transact and manage daily lives. A massive disruption could unravel parts of Australia's social fabric potentially resulting in civil disorder and other undesirable social impacts. The citizen of tomorrow will rely on ICT services much like they do on electricity today, with dysfunction the consequence of its absence or any significant disruption.

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 2008, 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.

Recommendations: Planning for the Future Threat Environment

1. The E-Security framework must take into account future threats to service availability, identity and trust including well-organised and coordinated threats.

2. The E-Security framework must play a pivotal role in coordinating the efforts across Government, between jurisdictions, business and citizens to address threats; a fragmented approach will not be effective.

3. The E-Security framework must provide a mechanism for regular sampling, testing and review of anticipated short, medium and long term threats. A complementary process must exist within the framework to feed the anticipated threats into planning for E-Security.

4. The E-Security framework should not solely focus on threats that arise from malicious entities; threats that arise from the accidental human factor must also be accommodated.

5. The E-Security framework should pursue a holistic approach that looks to improve the quality of identity trust decisions that get made by Australian users of the internet so as to reduce the number of bad decisions being made that allows the "anonymous" criminal to flourish.

6. This will require the establishment of holistic framework that address risk assessment allocation and management, accountability and redress, the ability to mutually authenticate participants in electronic interactions and the ability to validate various claims made during these interactions. Collaboration between business, government, user groups and the IT Industry will be critical to ensuring a robust, easy to use and economically practical outcome.

3. Developing a National Security Strategy

Australia has been at the forefront of the national cybersecurity 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 is again being reconsidered through this review.

By undertaking this major re-assessment of the ESNA the Government is 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.

Consequently, Microsoft has not critiqued the most recent version of the ESNA but has considered what may need to be achieved through a reinvigorated agenda, keeping the following Government imperatives in mind:

- Reducing the E-Security risks to Australian Government information and communications systems;
- Reducing the E-Security risks to Australia's national critical infrastructure, and;
- Enhancing the protection of home users and small and medium-sized enterprises (SMEs) from electronic attacks and fraud.

Recommendations on Developing a National Security Strategy

1. Continual re-assessment and updating of the E-Security national agenda every two to three years to-date;

2. Continual drawing from a broad range of stakeholder interests and the provision of ample time and context for meaningful input. This may mean providing more lengthy response time for stakeholders during the next E-Security review and perhaps providing the opportunity for field hearings, public forums or additional input once the Review is completed; and

3. The provision of financial and human resources to enable constant examination of programs and proposals from other Governments, multi-national organisations and the commercial sector to source international best practices thereby committing to a principle of constant evolution in planning.

4. Deterring Cybercrime: The Current Australian E-Security Policy Framework and Proposed Changes

The first line of defence in any national Cybersecurity 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 while legislative activity in the E-Security sphere is increasing across the Asia Pacific region and international Cybercrime guidelines are making an impact, there is relatively little information about where countries are placed in terms of their legal and regulatory frameworks to address threats across jurisdictions. Microsoft has sought to obtain a better understanding of how Australia is placed with respect to its E-Security framework vis-a-vis the rest of the region because Australia so often plays a regional leadership role on technology policy issues.

In an effort to better understand the state of play in the Asia Pacific region, Microsoft recently 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 such 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 E-Security portion of the analysis.[2] As mentioned above, the *Convention on Cybercrime* is widely

[2] 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.

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.[3] In particular, Title 1 obliges Member States to enact illegal access, illegal interception, data interference, system interference and misuse of device offences.

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 E-Security 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' to 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 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.

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

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.

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 (24/7 multilateral access to information sharing agreements and the opportunity to help frame future versions of

the Convention, for instance). 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.

Legislation around Identity Theft and Criminalisation of Malware and BotNets

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.

Recommendations for Deterring Cybercrime

1. Strengthen current security provisions around: (1) Illegal access; (2) system interference, and (3) The misuse of device offences, in accordance with the Budapest Convention;

2. Request accession to the Budapest Convention and seek to ratify the Council of Europe Convention on Cybercrime within the next 2 years.

3. Seek to enact comprehensive Federal legislation around identity theft that will give law enforcement the best possible tools to protect victims and prosecute offenders;

4. Consider looking at the need for new forms of legislation to criminalise growing cyber threats including the proliferation of malware, spyware and botnets;

5. Continue providing adequate Federal support for national law enforcement agencies and efforts around Cybercrime and E-Security. Work with the states and territories to ensure that resources are also provided at the local level, where they are greatly needed; and

6. Continue playing an important regional and global leadership role in E-Security and Cyber safety through both increased bilateral engagement but also through continued engagements with organisations such as APEC, the Council of Europe, the ITU and OECD.

5. Improving Critical Infrastructure Protection and Creating National Incident Management Capabilities

Microsoft and Critical Infrastructure Protection

Microsoft broadly defines Critical Infrastructure Protection (CIP) as a continuous set of risk management and operational response activities aimed at improving the security and resiliency of critical infrastructure supporting essential services, public health and safety, the economy, and national security.

Due to the complexity and global interconnectedness of these critical infrastructures, their protection is an important national and international policy concern. Securing and maintaining critical owners and operators, technology vendors, and governments is a critical component of this equation. Critical infrastructure protection is not an end state, but a continuum of processes; that draws upon the shared expertise of all of these stakeholders.

Providing secure, private and reliable computing experiences across the information technology ecosystem is central to Microsoft's vision for software and services. In 2002, we established the Trustworthy Computing Initiatives as a top company priority. Our commitment to Trustworthy Computing extends beyond the computer desktop to that broad cyber ecosystem on which we all depend. In 2007, we established the Trustworthy Infrastructure Policy and Programs to work closely with governments, infrastructure owners and operators, and technology vendors to understand and mitigate emergent risks to critical infrastructures.

Drawing upon work with global partners, coupled with more than three decades of experience, Microsoft has learned that effective critical infrastructure protection efforts will share three central areas of focus: the implementation of trust based plans and policies, the development of resilient operations, and the dedication to innovative investments.

CIP: Trustworthy Plans and Policies

The concept of trustworthy infrastructure extends beyond technology and into broad social, political, and economic institutions.

Trustworthy partnerships, policies, and practices build the foundations for enduring security; the key to their success is establishing trusted collaboration. Specifically, when governments, infrastructure owners and operators, and technology vendors collaborate to establish clearly defined goals and create transparent policymaking processes, they foster trustworthy public private partnerships for understanding and resolving challenges.

Such partnerships can advance critical infrastructure policies that are technology neutral, flexible, and adaptable to the dynamic cyber threat environment. Building and maintaining trustworthy partnerships, policies, and practices requires a clear value proposition, defined roles and responsibilities, and above all trust.

Trustworthy policies include those as highlighted in the earlier section of this document around security and Cybercrime legislation. Partnerships can prove to be another challenge – and opportunity - such partnerships are not easy to establish, but they are an essential foundation for the trusted collaboration needed to realize critical infrastructure security goals.

CIP: Resilient Operations

Critical infrastructure protection focuses not on preventing 100% of disruptions or attacks; indeed, infrastructures face operational challenges - from weather to human error to intentional attack - every day. Instead, critical infrastructure protection focuses on building resilient operations, which mitigate risk and increase security. Such resiliency is built – not through legislation - but by collaborative efforts that identify critical functions and establish processes for assessing, prioritizing and managing risks.

In particular, the development of robust incident response capabilities is central to effectively managing critical infrastructure risk. To this end, governments and non-government stakeholders can together foster responsible disclosure practices that ensure that newly discovered product vulnerabilities are shared only with the vendor in a way that does not jeopardize the security of the broader cyber ecosystem. Similarly, establishing and testing recovery and reconstitution plans increase the readiness level of the stakeholders and promote infrastructure resiliency.

Building resiliency requires sustained, sophisticated and multi-layered efforts on the part of all stakeholders. For example, vendors employ secure development policies and practices such as Microsoft's Security Development Lifecycle that reduce the attack surface of products and services. Owners and operators, for their part, can implement security best practices and make it more difficult for criminals to execute successful attacks.

Finally, governments that enact and swiftly enforce laws against cyber crime diminish criminals' incentive to engage in such activities. Collaborative efforts to manage risk, establish response and recovery capabilities and deter cyber crime together support greater resiliency across critical infrastructures.

CIP: Innovative Investments

People, processes and technologies all contribute to a critical infrastructure's ability to advance, evolve and respond to ever-more sophisticated threats. That is why innovations in practices, programs, education and research are all essential investments in critical infrastructure protection. Through collaboration, stakeholders are able to jointly identify the key processes, research, and education and investment needs of tomorrow's secure critical infrastructures.

All stakeholders make important contributions to innovation in critical infrastructure protection. For operators, these innovations may involve updating practices for managing risk, collaborating with vendors on emerging and evolving threats, as well as improving 'line of business' applications, security operations, and incident response. Vendors invest in research and development of technologies to mitigate emerging cyber security threats, as well as improve their software development processes, security features, and products.

Governments, on the other hand, can make much-needed investments in fundamental security research; in infrastructures, such as developing mechanisms to support secure collaboration among disparate organizations, including vendor-neutral information sharing, or strengthening education and training programs for information technology professionals. Universities can also play an important role by ensuring that security is actually integrated into university curricula for computer scientists and engineers.

Cyber Storm II

As mentioned Microsoft is strong proponent of CIP initiatives and exercises; and was fortunate enough 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 looks forward to participating in Cyber Storm III.

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. All key areas of feedback are relevant to this E-Security framework review and tie-in with the need for improved crisis management and coordination. They are outlined below.

Recommendations for CIP and National Incident Management Capabilities

1. In activities to test the ability for CIP such as Cyberstorm a common theme was that communications between players and coordinators significantly degraded at the slightest technical hiccup. Exercise control was "tethered" to the end of an unreliable satellite link and the mobile phone became the device of choice. More redundancy and alternate communication mechanisms such an instant messaging, VoIP and video conferencing are required to successfully secure Australia' CIP. The Government should establish an effective communications framework to deal with CIP.

2. In terms of evaluating the Australian security ecosystems preparedness to respond to matters of CIP there needs to be more regular testing and smaller exercises. In Microsoft's view the big bang approach of a major CIP exercise involving industry taking place once every two years is not optimal. Our view is that in the ICT space exercises between Government and Industry should occur more frequently, this will ultimately deliver a better result in larger exercises and in the real world. Smaller exercises more often that are aligned towards the larger Cyber Storm outcomes would be an effective approach.

3. To better accommodate future exercises around testing CIP response capabilities our recommendation is that a more permanent facility is provisioned by the Australian Government that provides the required ICT infrastructure, communications and accommodation for coordinators and planners. This facility could also double as a hot site in the event of a real incident. Due to the Australian economic dependency on an effective ICT environment the capability for ensuring its ongoing availability needs to be recognised as an ongoing need.

6. Industry and Government Collaboration: Partnering with the Australian Government for Protection

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.

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.

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.

The security solutions employed to date are primarily defensive technical measures that, while effective in mitigating particular avenues of attack, do not address an adversary who is adaptive and creative and who will rapidly shift their tactics. Determining trust on the Internet is a very complicated matter. Although trust may be a complex issue, this does not alter the fact that certain foundational elements must be in place to create a more trustworthy environment.

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
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 absent 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 five 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.

Recommendations for Industry and Government Collaboration

1. The E-Security framework should consider implementing a mechanism (policy, resources, organisational) to better leverage the benefits of programs for information sharing such as those established with Microsoft; SCP, GSP and MSRA. These types of programs should be more broadly leveraged across all levels of Government, businesses and citizens. Currently SCP and GSP information and resources are inadvertently focused at the Federal level. Additionally the government should look at how to establish these programs to embrace other key security ecosystem players.

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

3. The Australian Government should more actively pursue the evolution of schemes such as Common Criteria to better align with the need to build ICT products from the ground up with security-oriented development practices in mind.

4. Government should consider a “stock-take” and assess the efficacy and impact of the current Government-industry collaboration efforts they have established thus far with the view of

continuing those that are most successful, integrating others where there is shared purpose or "overlap" and retiring those that may have already reached their peak.

5. 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.

6. Consideration should be given to how the VANGuard program could be leveraged with Industry to provide a trust authentication framework for electronic transactions.

7. 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, 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 player 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-taking of current Government-Industry efforts that serve to further the interests of cybersecurity might be considered to maximize resources and ultimately, impact on consumers.

E-Security 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) and the Australian Media and Communications Authority (ACMA), 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 will be launched this year as part of National Child Protection Week. Through this pilot program, Microsoft, ACMA and AFP volunteers will team up to be deployed to local schools in NSW, Victoria and the ACT 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.

Recommendations for Promoting a National Culture of Cybersecurity: Outreach and Awareness

1. Continue with Government-led, industry and NGO collaborative efforts around E-Security awareness including Scams Target You and National Security Awareness Week. However, consider where there might be initiatives that may be duplicative and look for ways to increase more consistent "surges" of security and safety education awareness to the Australian public.
2. Consider expanding planned E-Security and Cyber safety education efforts in the schools more broadly and consistently. Consider looking at the prospect of mandatory internet safety education as a requirement for school curricula nationwide.
3. 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 and Summary of Recommendations

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.

The Australian Government can play a key role by:

1. Enabling this environment through establishing the right regulatory framework;
2. Establishing a framework to continue to adapt and evolve the security ecosystem; and
3. Enacting legislation to support specific elements that will enable the Australian security ecosystem to be established.

This will empower users to make trust choices. In general the goals of E-Security should be:

1. To substantially mitigate common risks so that public faith in the safety of the IT ecosystem is restored and/or enhanced;
2. To permit security professionals to reduce their current efforts to address existing threats and allow them to redeploy those resources to address more intractable risks and forward planning for future risks;
3. To make it more difficult to conceive and deploy new criminal schemes because authentication and audit make it more difficult to complete crimes successfully; and
4. To enable law enforcement to find and prosecute a greater number of Cyber criminals, thus increasing deterrence on the Internet.

To achieve these goals, it will be necessary to address all of the complicated social, political, economic, and technical issues raised in this paper.

Policy

The Australian Government is able to support the existence of an effective ICTR security capability within Australian through the provision of a supportive regulatory framework. There are additional regulatory aspects that the Australian government could enact that would enhance the already existing regulatory framework. This will ensure that all key security ecosystem players are aligned not only locally but also internationally.

The following are key regulatory enhancements that Microsoft views that the Australian government should consider:

1. Strengthen current security provisions around:
   - Illegal access;
   - System interference; and
   - The misuse of device offences, in accordance with the Budapest Convention;
2. The Government should actively investigate and seek accession to the Budapest Convention and seek to ratify the Council of Europe Convention on Cybercrime over the next 2 years.
3. Seek to enact comprehensive Federal legislation around identity theft that will give law enforcement the best possible tools to protect victims and prosecute offenders;
4. Consider looking at the need for new forms of legislation to criminalise growing Cyber threats including the proliferation of malware, spyware and botnets;
5. Increased bilateral engagement in regional and global forums and extended engagements with organisations such as APEC, the Council of Europe, the ITU and OECD.

Process

The Australian Government has a key role to play in providing the framework to facilitate an evolving security framework for Australia. To do this and to ensure this security framework evolves and adapts the Australian Government should establish a number of enabling processes.

The following are key processes that Microsoft views that the Australian government should undertake to maintain an effective security framework for Australia:

1. Continue re-assessing and updating the E-Security national agenda every two to three years, as the Government has done to-date;
2. Continue drawing from a broad range of stakeholder interests and provide ample time and context for meaningful input. This may mean providing more lengthy response time for stakeholders during the next E-Security review and perhaps providing the opportunity for field hearings, public forums or additional input once the Review is completed;
3. Continue evolving engagement and discussion with other Governments and multi-national organisations in search of new ideas and best practices;
4. Continue sharing best practices through relevant international fora; and
5. Conduct a “stock-take” and assess the efficacy and impact of the current Government-industry collaboration efforts they have been established thus far with the view to continuing those that are most successful, integrating others where there is shared purpose or “overlap” and retiring those that may have already reached their peak.

Enablement

There are specific activities that Australian Government can undertake as a provider of capability that will assist to enable the establishment of an effective ICT security ecosystem for Australia. The following are key areas that Microsoft considers the Australian government play a role in providing capability:

1. Continue providing resources to enable national law enforcement agencies to pursue, with all available tools, efforts around Cybercrime and E-Security;
2. Work with the states and territories to ensure that resources are also provided at the state and local level to build capacity and support active law enforcement; and

3. Dedicate resources to establishing a common, robust communications framework between players and coordinators involved in major critical infrastructure protection. Provide more redundancy and alternate communication mechanisms such an instant messaging, VoIP and video conferencing to ensure effective and constant communication channels are available in the event of a Cyber attack on Australia.

Response

In terms of evaluating the Australian security ecosystems preparedness to respond to matters of CIP Microsoft's preference is for more regular testing around smaller more specific exercises. In Microsoft's view the big bang approach of a major CIP exercise involving industry once every two years is not optimal. ICT space exercises between Government and Industry should occur more frequently.

To better accommodate future exercises around testing CIP response capabilities a more permanent facility should be provisioned by the Australian Government that provides the required ICT infrastructure, communications and accommodation for coordinators and planners. This facility could also double as a hot site in the event of a real incident. Given Australia's economic dependency on an effective ICT environment the capability for ensuring its ongoing availability and viability needs to be recognised as a priority.

Collaboration

The Government-led, industry and NGO collaborative efforts around E-Security awareness including "Scams Target You" and "National E-Security Awareness Week" are valuable. Consideration could be given to where there might be duplication in initiatives. The Government could adopt a strategy of seeking in its public education campaigns more consistent "surges" of security and safety education awareness.

1. Expand E-Security and Cyber safety education efforts in schools to deliver a broader and more consistent set of messages to students in all age groups and across all academic years. Consider the merit of mandatory internet safety education as a requirement for school curricula nationwide.

2. Evaluate the incorporation of more security collateral into ICT curriculum and training programs to raise the level of security awareness capabilities across the ICT industry who can then assist to evangelise security to all citizens.

3. Work with industry to support the option of electronic claims based identities based directly or derivatively upon in-person proofing.

4. Work with Industry to establish a reputation platform that facilitates code signing so that better informed trust decisions can be made by end users.

5. Actively pursue the evolution of schemes such as Common Criteria to better align with the need to build ICT products from the ground up with security-oriented development practices in mind.

6. Consider how the VANGuard program could be leveraged with Industry to provide a trust authentication framework for electronic transactions.

7. Evaluate implementing a mechanism (policy, resources, organisational) to better leverage the benefits of programs for information sharing with industry such as those established with Microsoft; SCP, GSP and MSRA.

E-Security Planning Framework

The Australian government has a clear role to play in facilitating an environment that enables a more secure and trustworthy ICT ecosystem. The E-Security framework should:

1. Consider future threats to service availability, identity and trust and well organised and coordinated threats.

2. Play a pivotal role in coordinating the efforts across Government, jurisdictions, business and citizens to address threats; a fragmented approach will not be effective.
3. Provide a mechanism for regular sampling, testing and review of anticipated short, medium and long term threats.
4. Create a complementary process to feed the anticipated threats into planning for E-Security.
5. Not solely focus on threats that arise from malicious entities - threats that arise from the accidental human factor must also be planned for and have appropriate responses agreed and capable of deployment.
6. Pursue a holistic approach that looks to improve the quality of identity trust decisions that get made by Australian users of the internet, to reduce the number of bad decisions being made that allows the "anonymous" criminal to flourish.

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 on juliei@microsoft.com or Scott Deacon, Government Strategic Security Advisor on sdeacon@microsoft.com.