SUBMISSION NO. 5

Submission for Cyber Crime Inquiry

Introduction

First let me say that I very much welcome the opportunity to provide inputs to the Cyber Crime Inquiry. In my view, this is an important inquiry and a timely one, given the dramatic developments in the information and communications technologies (ICT). I applaud the Government foresight in establishing this inquiry.

It is clear that the Internet is transforming the way we live and the recent decades have witnessed dramatic developments in information and communication technologies (ICT). Along with the phenomenal growth in technology enabled information economy has been a growth in computing technology related crimes. *These are posing not only significant technological challenges in the development and deployment of secure, trustworthy and dependable systems and services but also in the areas of policies – how to keep them up to-date and manage them, apply them across different business segments and jurisdictions as well as across international boundaries. It is critically important to increase the awareness of cyber security and cyber crime issues in the community, thereby encouraging the people in the community to take greater precaution and responsibility.* There is a clear need to build and maintain confidence on the infrastructures and systems among the different stakeholders such as ordinary end users, SME as well as corporate organizations. In this regard, the government has a critical role to play in developing research and education programs to address the emerging security challenges and helping to maintain an overall secure information infrastructure ecosystem for society and business. I believe the cyber security challenges are multi-faceted involving technological, business as well as legal aspects. Hence there is a clear need for the new framework to explicitly address this multi-faceted nature of cyber security.

a) Nature and prevalence of E-Security risks

- Convergence of Technologies and the Pervasive Nature of Security

  It is not an overstatement to say that the information and communication technologies have become pervasive. We have been witnessing convergence of many technologies over the last several years. Though it has been talked about for many years now (since late 80s and early 90s), this is actually happening now and will continue to do in the future. We are seeing pervasive infrastructures involving wired (fixed), wireless, mobile, peer to peer networks, small devices from PDAs to embedded systems and smart phones to large scale grid computing and cluster computing systems, large scale distributed information systems and databases to distributed and mobile applications and services. These are changing the way the people work, behave and live their lives (cf. social networking and online businesses).

Given these dramatic developments in technologies affecting our businesses and society, security issues have become even more significant. It is critical to note that *security itself is pervasive*. It is there in every part of technology and business – in financial systems and transactions over the Internet, to healthcare information systems, to transportation systems, to critical information infrastructures such as energy, to provision e-government services, to national security and defense, to doing day to day activities such as car hire or even dating over the Internet. This pervasive nature of security and privacy issues increases the scope and depth of possible security risks and attacks.

- Interconnected Systems of Systems

  This brings me to the next point. Major security technology challenges in the future (and even now) arise due to the *systems nature* (or even *systems of systems* in nature). No problems nowadays come in self-contained neat packages. Take for instance a healthcare system or a transportation system or a telecommunication system. These are all systems of systems with multiple technologies having different policies and different administrative authorities having jurisdictions. Malicious software can move from one system to system and compromise a set of systems and the whole infrastructure. So there needs to be a greater emphasis and focus given to security in systems (or systems of systems) involving networks, distributed systems and applications and above all users of these systems (or systems of systems) and guaranteeing certain levels of assurance are provided, if we are to able to address these risks effectively.

- Changing Nature of Threats and Attackers

  A closely related issue is the dynamic and changing nature of security and privacy threats in this "converged technologies of systems and systems across multiple business sectors". Dynamic security threats and attacks can occur in any of the technologies such as wireless security, 24/7 connected broadband security, to service-oriented architectures and cloud computing and peer to peer Internet applications.

  Perhaps even more important is how these technologies are being used by different people. For instance, security attacks happen due to the way users use (or misuse) the services and applications such as online banking and electronic patient records. There are different classes of users such as individual ordinary home users to tech savvy users to SME to corporations to governments. Similarly attackers can range from individual hackers to hacker networks to corporate espionage to organized crime to state sponsored information warfare.

What I refer to is the "*increasing threat velocity*" with more and more vulnerabilities and attacks arising in different types of technologies of systems of systems, an evolving set of bad guys, attacks happening sooner and faster (with less and less grace period) and increasingly sophisticated attacks using easily available tools. This is the environment we are dealing with and

to address the challenges, we need a comprehensive framework providing programs and initiatives in the areas of research and development, educations and skills, policy and governance, partnership and collaboration.

b) Implications of these risks on the wider economy

It is clear such threats and attacks are serious especially in an ever increasing digital economy. Cyberspace touches practically every part of our society and lives. It provides a platform for services and businesses, for innovation and more generally the security and welfare of the nation. Hence attacks on the cyber infrastructure can affect the whole economy and country's welfare.

For example, recently in March 2009, there was a severe power blackout that brought chaos to downtown Sydney, causing peak-hour traffic jams as street signals failed, leaving workers in lifts as they tried to make their way home. Sydney Opera House had to cancel performances and stock exchange had to close. In this case it was due to some accidental mistakes such as a backhoe or similar interfering with the cables. It is possible to imagine other instances where it could be more malicious. Imagine such security attacks conducted by malicious intruders or even malicious software and botnets. Because of the interconnected nature of systems and networks (mentioned above) such botnets can spread easily (if there are not adequate security and protection mechanisms) and affect different parts of the economy from financial to healthcare to transportation to telecommunication systems. These attacks have the potential to disrupt economies and paralyze the country (and even potentially causing reduction in the sovereignty of countries). As President Obama in his recent speech on national security priority on setting up the cyber security office, referred to terrorist attacks could "not only come a few extremists in suicide vests but from a few key strokes of a computer – a weapon of mass disruption".

Such malicious botnets with varying degrees of sophistication are easily available over the Internet to even inexperienced users and attackers. Therefore it is critical to have adequate security mechanisms (software and hardware) installed in systems and network infrastructures and keep them up to date (with regular security patches updates) to maintain the security of the systems and network infrastructures. It is necessary to be pro-active, actively predict the types of attacks that may be possible and develop adequate measures and precautions and deploy them effectively, if one wants to be ahead of the attackers in this continuous security race.

c) Level of understanding and awareness of E-Security risks within the Australian community

Given the pervasive nature of security and the impact of security attacks and threats on the economy and the country, it is critical to maintain and promote a greater level of understanding and awareness of such e-security issues in the Australian community. This is not an easy task as it involves different "levels" understanding and awareness by "different" part of the community. It needs to be on a continuous basis, that is, it is a process and just a one off event.

In the community, we have different types of people in the society from young to old, technology savvy to novice to small businesses to large corporations and government agencies. Some organizations and people will have an excellent understanding of the issues whereas many others may not be aware of the risks at all. In this context, I would like to express my strong support to initiatives such as the DBCDE on E-Security Week held each year in June. This serves a very useful purpose and such initiatives need to be strengthened.

I would also like to add that it is critically important for Australia to be in the forefront of security technologies and their applications. So there is a clear need to strengthen research and development activities in security, trust and privacy. In this context, I would like to emphasize the need to ensure that there is "relevancy" in the research and development; here I mean increasing our research and development efforts in security and privacy issues in emerging systems and information infrastructures -- such as security in wired, wireless, mobile and broadband networks, security in distributed systems and applications, secure virtualized systems, trusted computing, secure mobile software systems, secure Internet applications etc.; and not in esoteric cryptographic algorithms per se (of which there are already several to choose from, and the real challenges at present are in *securing systems and infrastructures* as mentioned earlier in (a) above).

d) Measures currently deployed to mitigate E-Security risks

There are a range of measures that the industry and education sectors as well as government agencies are currently using to mitigate e-security risks. For instance, technology vendors have developed and continue to develop security products, systems and tools and many of these are being deployed to varying degrees. There is a clear recognition of the need to share trusted information on the nature of vulnerabilities and attacks internationally between countries. There are different Australian government initiatives in this regard (such as TISN, Cyber Storm etc.). There are also attempts to share such information between different corporations and government agencies, as well as between corporations in the industry. Education wise, several Universities have incorporate as part of their undergraduate and postgraduate programs courses in security (for instance, at Macquarie University, we have a Masters Program specialised in Security offering courses in Advanced System and Network Security, Security Technologies, Security Management and Forensics).

As mentioned above in (a), the technology scenery continues to change, and the nature of threats and attacks continues to change and is dynamic, and hence the need to continuously being pro-active (and just reactive) and to be ahead in research and development and develop new security techniques and technologies (especially in the relevant areas for the challenges in the emerging information infrastructures - see the end of (c) above and (f) below).

e) Future Initiatives that will further mitigate E-Security risks to Australian Internet users

Following on from the above discussion, let me mention a few which I believe to be important

- **Research and Innovation in E-Security**: Establish targeted strategic initiative in E-Security that supports research and development and innovation in security technologies and techniques to counteract cyber crime in emerging information infrastructures.
    - In particular, I would like to suggest that this initiative emphasizes and supports programs in areas such as large scale distributed systems and services, trusted computing, counteracting epidemic style attacks (such as botnets, phishing, spam etc), secure virtualization systems, secure cloud computing, mobile and wireless networks security, broadband security, secure peer to peer Internet applications, security and risk management, security and usability, and high assurance systems. These areas are in my view important not only from the point of view of technological trends, but also from the view point of protecting systems and infrastructures and maintaining Australia's competitive edge in the international context (note my comment on relevancy at end of point (c) above). These areas highlight the important emerging threats in the changing E-Security landscape and are significant from the point of view of R&D in E-Security in Australia. It is important to note that it is in these areas where there is a shortage of expertise and lack of skills in the Australian scene.
- **Promote Partnerships and Awareness**: Industry – Academia – User Community Partnerships
    - Establish specific initiative and programs in E-Security that target and enhance partnerships between industry, academia and user communities. Here again, in my view, it is important to focus on the current problems and the emerging challenges in the E-Security space and on the effective deployment of technologies in the community. In this regard, programs such as the Research Support against Counter Terrorism (administered by the Dept of PMC) as well as the Infosec programs of the DSD are deserve support and expansion. I would also encourage establishment of programs and mechanisms that would enable agencies such as DSTO, DBCDE and AG to nurture partnerships with both academia and industry.
    - Increase e-security awareness programs such as the E-Security Week, targeting different sectors in the community: ordinary home users, SMEs, users of e-Government services etc.
    - Establish programs that enable security professionals to move between industry, academia and government agencies, thereby increasing the transfer of knowledge between them.

- **Education and Training in E-Security**: Specific measures addressing security education and training in Australia such as the following:

    - Establish schemes that support to Security Courses and Programs in the targeted areas, e.g. by
        - Providing funds to recognized research and education groups at Universities in Australia to develop appropriate information security and assurance programs targeted at areas mentioned above
    - Increase and retain the pool of suitably trained information security professionals by
        - Providing financial support to Universities in terms of scholarships for undergraduate, postgraduate and research students in information security and assurance and to recruit and retain staff with security expertise and skills in these areas.

- **Dedicated E-Security International Collaborations**

    - The global nature of security issues makes international collaboration and cooperation particularly significant. Programs that promote cooperation between Australian and international organizations (e.g. Universities, Industry, International Forums such as OECD, ITU, International Standards Bodies and EU) targeted at E-Security.

    - Support participation of Australian organization in international programs in security and trust such as EU FP7 and Future Internet

- **E-Security as a Key Mainstream Activity in Government**

    - To achieve the above as well as to ensure that security considerations are given priority in the decision making and governance of all parts of the government, it is timely and appropriate to consider the establishment of an overarching organization that is responsible and accountable and which can coordinate and oversee the various security priorities in the different departments in the government. As we have seen, one of the unique aspects of security is that it permeates many parts of the economy and this will continue to increase in the future. Given this pervasive nature, it is important that security considerations should form a core part of the decision making and such an organization could help to achieve this; this will also provide the ability to be more proactive and respond better to dynamic changes in security threats.

(f) Emerging Technologies to combat emerging and new risks

I have already mentioned a few of these in the above paragraphs. Here I will give brief outlines of the important ones.

- Technologies for Securing Large Scale Distributed Systems and Cloud Computing Services: With the developments is technology and communications over the next decades, the mobile distributed pervasive computing infrastructure could lead to billions of information appliances connected to wired and wireless infrastructure with numerous applications and huge number of users. We are not equipped to deal with large scales at present. We need to understand better how to design large scale secure systems and services and manage them in a dynamic environment.

- Technologies for Counteracting Epidemic-style Security Attacks Security Attacks
  There is a clear need to understand better, detect, monitor and develop techniques and mechanisms to counteract epidemic attacks such as DDoS, botnets, malware, virus, spam etc. in heterogeneous broadband network infrastructures.

- Mobile Software and Security in New Generation Networked Systems
  Movement of mobile code and content to achieve the deployment of services and applications as well as distributing content is becoming prevalent in the pervasive new generation networked computing environment. This raises a range of security issues including protection and transfer of privileges and their attachment to content, protection of software and content over the network, and the secure management of privileges and their policies

- Wireless Mobile Networks and Security
  Increasingly wireless mobile ad hoc networks and sensor networks are emerging as a new tier in the information network infrastructure ecosystem. Such networks poses some unique security challenges due to their decentralized management, limited computational capability, dynamic network connectivity, ad hoc mobility and physical vulnerability and susceptibility of wireless communications.

- Trusted Computing
  Many of the security challenges proposed above form part of this and it is clear that without "trust" (whichever way one defines it), it would be difficult if not impossible to achieve security. Much depends upon developing trust models, mechanisms and tools to create and manage trust between unfamiliar entities over the Internet for enabling them to trade and interact in a secure manner. A range of topics need to be addressed from trusted operating systems to trusted applications to trusted networks to trusted hardware.

- Security and Risk Management in Future New Generation Information Architectures
  We are likely to see the growth in distributed virtual enterprises that are not only geographically separated but also dynamic, in the sense that they exist for a period of time and disband and reform again with different characteristics. There will be an increase in ad hoc peer to peer applications and new convergent networks. We will need to anticipate new threats in these emerging new generation networks and applications and analyse risks and

develop security baselines and security policy management. For these distributed virtual organizations and new generation infrastructures and networks, we need to understand better the formulation of security policies, quantification of risks and their management as well as their implementation and monitoring.

In this context, at Macquarie University, we have an internationally recognized research group, Information and Networked Systems Security Research (INSS) carrying out research in the above mentioned areas such as distributed systems security, network security, mobile software security, secure service oriented architectures, mobile and wireless security, trusted computing, secure virtualization and peer to peer Internet applications security. (www.comp.mq.edu.au/research/inss).

Concluding Remarks

I am thankful to the Australian Government for this opportunity to provide inputs to this important Cyber Crime Inquiry.

I hope the brief set of comments and suggestions given here will be of some help to the Committee in its deliberations. I will be most happy to elaborate on any of these issues mentioned here and other related matters if required by the Committee.

Best Regards

Vijay Varadharajan FIEE, FACS, FIEAust, FBCS, FIMA

Professor and Microsoft Chair in Innovation in Computing
Director of Information and Networked Systems Security Research (INSS)
Dept of Computing, Macquarie University, Australia

Email: vijay@ics.mq.edu.au
Web: http://www.ics.mq.edu.au/gen/person/vijay.html
Tel: +61 2 9850 9534
Fax: +61 2 9850 9511