TELSTRA SUBMISSION

HOUSE OF REPRESENTITIVES COMMUNICATIONS COMMITTEE

INQUIRY INTO CYBER CRIME

Overview

This submission has been prepared on behalf of Telstra to provide Telstra's view on specific areas that should be focused on by Government as part of its inquiry into cyber crime.

In summary, Telstra has focussed on providing tangible recommendations in this submission addressing:

1. The need for greater industry engagement/collaboration in identifying and managing cyber crime;

2. The need to greatly increase the public's awareness and education of cyber crime risks through mass media awareness campaigns;

3. Telstra's views on operational improvements required by Government to better understand the potential impacts of cyber crime and the processes for cyber incident response (eg. botnet activity); and

4. Telstra's views on cyber safety programs as a community focused response to cyber crime activity.

On an ongoing basis, Telstra provides confidential briefings to Government agency executives on emerging network security threats and the latest methods of attack being deployed. Telstra would appreciate the opportunity to meet with members of the 'Inquiry into Cyber Crime'.

1. Drive greater industry engagement/collaboration – identifying and managing cyber crime threats

Telstra builds, operates and manages Australia's largest and most diverse cyber infrastructure which is used for e-commerce, business, security, Government, defence and recreation. As a consequence, Telstra is often more aware of emerging global and regional cyber crime trends before many government or industry organisations are in Australia.

There is evidence of a continuing upswing in the number of computer systems infected with malware running across Australia's telecommunications networks. These systems are being used in many different ways by a wider criminal element; the most concerning trend is carefully targeted malware designed to steal specific personal identifying information as enablers of fraud and identity theft; 'zombies' within global botnets to launch distributed denial of service (DDoS) attacks against legitimate government and business websites within Australia and acting as the origin for large scale unsolicited email, used in phishing attacks against Australian citizens. For example, security company McAfee identified 12 million new IP addresses in the first quarter of 2009 belonging to 'zombie' PCs that were part of larger botnets[1]. Such compromised devices are actively sought in Telstra's networks to provide their owners an opportunity to address them.

The distributed global nature of botnets and rapidly changing methods of attack mean that government policy and legislation is limited in its effectiveness. Collaboration and partnering with industries at the forefront of Internet development will provide Government with the technical knowledge and agility to develop appropriate responses to cyber crime.

This viewpoint is gaining momentum. For example, the recent cyber security review requested by US President Barak Obama highlighted the need to strengthening public/private partnerships rather than impose legislative requirements on industry. The review also recognised the requirement for greater international cooperation and collaboration in relation to developing 'legitimate' capabilities (ie technology, legislation, policing etc) to address cyber crime activities.

In Telstra's experience such cooperation has been most effective for information gathering, preventing delivery of fraudulent emails, containing DDoS attacks and removal of problematic web sites. Telstra views the development of such informal National and International networks as a priority for securing Australia's cyber infrastructure.

Current situation

There is the need for a more defined public/private sector cooperation structure for jointly developing policy, and the sharing of cyber crime intelligence and cyber security capability in relation to cyber crime. Telstra has been pro-active in this space however, pursuing closer operational relationships with individual law enforcement and security agencies.

Telstra's collaborative arrangements with law enforcement agencies provide access to knowledge, skills and on-site expertise for developing technical capabilities in

[1] http://newsroom.mcafee.com/images/10039/q1threatreport_2009may_5_2009.doc

relation to cyber security. These types of relationships provide a good foundation and future model for addressing and responding to cyber crime.

Within the current national critical infrastructure framework of the Trusted Information Sharing Network (TISN) and Infrastructure Assurance Advisory Group (IAAGs), focus is specifically on the national security context of cyber crime (ie e-security). The existence of this framework may provide an opportunity to extend the TISN focus into cyber crime and its impact on Australian society more broadly.

Recommendations:

- Designate AusCERT as the recognised Australian national Computer Emergency Response Team (CERT). AusCERT represents one of the single largest bodies of expertise and experience in the Australian context. Industry cooperation with AusCERT will significantly benefit Australia's ability to manage cyber crime.
- Expand the scope of TISN to establish a cyber crime arm for industry, government and research sectors to drive the national agenda in this area. Telstra would welcome the opportunity to be part of driving a National Cyber crime Advisory Committee focussing on strategic leadership and information sharing between public and private sectors, federal, state and local entities.
- Expand the use of formal arrangements (such as MOUs) between relevant law enforcement/security agencies, appropriate industry organisations and research bodies to actively develop strong skill/knowledge/people sharing arrangements.
- Develop formal educational links with universities that encourage research in cyber security and develop sponsored courses to produce cyber security specialists.

2. Increase public's awareness and education of cyber crime through intensive mass media education and awareness

In its E-Security Review submission to Government, Telstra identified the need for extensive education across all levels of government and the wider community, including families, education institutions, government departments and law enforcement agencies.

Even though the E-Security Review was completed less than 12 months ago, it is evident that in this time cyber crime has become a more prominent and pressing issue for governments globally. This is shown by the US President Barak Obama's cyber security review outcomes, in which a national campaign to promote cyber security awareness is a key activity. More recently, the UK government has announced the establishment of a Cyber Security Centre as a central and highly visible body for anti-cyber crime activity.

As previously noted the global growth of botnets as a tool to conduct cyber crime is a key driver for governments focusing their efforts into cyber security. Australian industry and law enforcement agencies cannot hope to address individually the malicious use of tens of thousands of zombie PCs. The only viable option is to ensure the public is aware of the risks associated with being on-line and what action they need to take to protect themselves. This will become more important to not only consumers but business in the NBN world.

Current situation

Telstra remains committed to public awareness and education of cyber crime, evidenced by it being a major corporate sponsor of the Government's National E-

security Awareness Week campaign. The Awareness Week is the Government's more significant public awareness campaign focused on helping Australians understand e-security risks and educate home and small business users about the simple steps they can take to protect themselves, their families and their businesses when online.

While the Awareness Week has strong support from industry, its communication is limited to on-line promotion. As an awareness campaign, it has limited community penetration due to lack of cross-communication mediums (ie print, TV) and on-going messages that extend beyond a single week per year.

Telstra strongly believes that a concerted campaign of cyber security education and awareness in the Australian community is an essential element of any effective strategy to improve the nation's ability to manage cyber crime.

Recommendations:

- Develop an ongoing mass media campaign similar to the Government's national security public information or road safety campaigns to educate the Australian public on cyber crime and cyber security.
- Develop and publish effective on-line and paper resources to provide the public with key information on what they need to do to protect themselves on-line (ie cyber security kit of effective tools for households).
- Engage the communications industry through Internet Service Providers (ISPs) to support and drive out campaign resources to their customers.
- Develop educational curriculum requirements (including teacher resource kits) that focus on teaching cyber crime aware behaviour to schools, vocational institutions and universities.
- Encourage the development of information security as a 'profession' by tertiary education institutions and industry to develop and attract specialist skills.

3. Opportunities to develop the operational capability of Government

Recent activities by global governments indicate that a tipping point has been reached in terms of recognising the seriousness of the cyber crime threat to societies the world over. The current Government's previous e-security review, this cyber crime inquiry, and the UK and US governments' major announcements in relation to developing cyber security capability are all responses to a significantly escalating threat.

While the need has been recognised, current government frameworks, policy, regulation and legislation need to align with the need for an intense focus on cyber crime.

Current situation

In the event of cyber crime activity there is no formal process for the telecommunications industry to advise or alert any government department or agencies of the threat or impact so they may respond appropriately. Law enforcement and security agencies often lack the resources and capability to investigate and respond to cyber crime incidents.

From the outside, it is not always clear to industry who to approach in government in the event of a particular type of cyber crime incident or who has responsibility to provide advice to the public/private sector when responding to an incident.

Telstra gathers cyber intelligence and alert information from its own network, security professionals and contracted security vendors and strategic partners. As previously noted in its E-Security Review Submission, Telstra receives limited cyber intelligence information from government. Often when intelligence is received Telstra has been aware of the issue for some time and has been working on an effective response.

Telstra also notes that there is a need for a legal process to allow the company to protect its networks and those of customers from cyber crime by taking down communications links that have been identified as a source of a cyber attack or PCs that are participating in a botnet.

This is particularly important for maintaining secure communications links that are used to deliver intercepted information to enforcement agencies, banking and financial institution data emergency calls to emergency service organisations and providing information to national security and law enforcement agencies in times of an attack or a life threatening situation. This gap was evident in the February 2008 Cyber Storm Cyber Storm II exercise.

Under current telecommunications regulations, Telstra is required to provide and protect its cyber infrastructure from attack, but if Telstra was to take action against a retail or wholesale customer who has been identified as a source of a cyber attack, then that customer may initiate civil court action if Telstra disconnected that customer in order to protect its infrastructure and other customers from attack.

Recommendations:

- Further develop the expertise and resourcing of law enforcement and security agencies to investigate cyber crime. This can be done through previously identified points, such as educational sponsorship to attract skilled graduates and MOU arrangements to facilitate 'sharing' of capability between government, industry and research bodies.
- Identify and support a central coordination point for government, industry and research groups to undertake intelligence gathering and profiling on cyber crime activity. Given the prominent operational role of AusCERT in Australia's cyber crime response capability means this function can potentially be undertaken by this body.
- Establish a central reporting and response function within government (ie law enforcement/security agencies) for significant cyber crime activity. This function should allow for effective operational cooperation and coordination between government and industry to respond to and recover from a major cyber crime incident.
- Provide legislative protection for a carrier or Internet Service Provider (ISP) from third party claims when it undertakes activities, in good faith (or as agreed with government and/or industry), to protect their networks and services and customers from being used in, or in relation to, the commission of offences against the laws the Commonwealth or of the States and Territories. (This would be similar to the protection given under section 313(5) of the Telecommunications Act 1997).

- Give industry the certainty and legislative tools to be able to respond and protect Australia's cyber infrastructure and services from attack and in particular its national emergency Triple Zero service. This could further be enhanced by Government supporting the work being undertaken in Communications Alliance.

4. Views on cyber-safety programs as a community focused response to cyber crime

The nature of cyber crime threats are extensive, ranging from financial gain, including online fraud, to exposure to inappropriate content, such as cyber-bullying, online stalking and child exploitation. The nature of these threats is evolving and they face all users of the Internet.

The onus is increasingly on internet users to manage their own safety, with existing regulations and laws becoming increasingly ineffective for managing cyber crime. The ability of cyber 'criminals' to operate remotely from outside Australia through distributed networks and exploit extensive vulnerabilities in software and hardware makes them nearly impossible to track and when identified difficult to prosecute due to domestic/international jurisdictional issues.

In this environment, the public must increasingly see themselves as their own front-line cyber safety defence rather than rely on the support of traditional community-based services such as the police.

Current situation

Telstra strongly supports the Government's cyber-safety policy objectives. Telstra's commitment to a safer online experience is fundamental to our particular customer base and our official status as a Family Friendly Internet Service Provider (ISP). This commitment is embodied in the support from Telstra's Executive Management, its public policy and its consumer offerings.

Telstra also actively cultivates close networks and trusted relationships with key National Security and Law Enforcement Agencies (LEAs) responsible for tackling the challenges of cyber-security. We also provide valuable information under legislative regimes to support LEAs and assistance in areas such as take-down notices and blocking of prohibited websites.

Most recently, Telstra accepted a role on the steering committee for the proposed ISP e-Security Voluntary Code of Practice. The Internet Industry Association (IIA) proposed the code be used by the ISP industry to help industry and consumers address the issue of compromised computers which can be used for illegal and harmful activities.

Telstra remains focused on driving a number of ongoing initiatives designed to protect our three million plus internet customers and broader members of the community from the many risks they face in the online environment. Key initiatives include:

- **Representation on the Consultative Working Group on Cyber-safety (CWG)**. The CWG is a key plank of the Governments cyber-safety strategy. The role of the Group includes: considering those aspects of cyber-safety that

Australian children face, such as cyber-bullying, identity theft and exposure to illegal and inappropriate content; providing advice to the Government on priorities and measures required by government and industry to ensure world's best practice safeguards for Australian children engaging in the digital economy.

- **Spotlight on cyber-safety program.** This Telstra Foundation program focuses on building the protective factors for children and young people so they can develop their skills and enjoy the use of modern communications technology in safe, supported environments. We have recently announced a further $3million commitment for another 3 years taking our total commitment to this important initiative to $6million since June 2007.

- **Virtual Global Taskforce (VGT).** Telstra's BigPond is an original partner of the VGT, an international alliance of law enforcement agencies working together to prevent and deter online child abuse. In joining the VGT as an industry partner, Telstra demonstrated how it is working with law enforcement agencies to help reduce the threat to children on-line and our commitment to community safety and crime reduction. BigPond is the only ISP accredited as an industry partner in Australia.

Recommendations:

- Given the nature of cyber crime, it is not uncommon for innocent people and businesses to become inadvertently involved through compromised computers and systems. A working group should be established from enforcement agencies and industry to consider regulatory processes which could be introduced to deal with and minimise the impact of this type of cyber crime activity. The Internet Industry Association's (IIA) proposed ISP e-Security Voluntary Code of Practice may assist as a starting point in this area.