AUSTRALIAN COMPUTER SOCIETY

SUBMISSION TO THE HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON COMMUNICATIONS INQUIRY INTO CYBER CRIME

The Australian Computer Society (ACS) is the recognised association for Information & Communications Technology (ICT) professionals, attracting a large and active membership from all levels of the ICT industry. As member of the Australian Council of Professions, the ACS is the public voice of the ICT profession and the guardian of professional ethics and standards in the ICT industry, with a commitment and responsibility to the wider community to ensure the beneficial and safe use of ICT.

The ACS believes that the Inquiry into Cyber Crime is very timely, following on from the Government announcement to build a ubiquitous high speed broadband network for all Australians. Evidence shows that cyber crime has increased considerably over recent years and it is likely to do so even further with the introduction of high speed, always on, internet services.

Our increasing reliance on services delivered on-line for work and home life will increase not only the opportunity for fraudulent activity, but also the financial consequences of this activity and its impact on the confidence of consumers and businesses in doing business on-line.

The phenomenal developments in technology, implementation of ultra-fast broadband and the introduction of IPv6 are going to facilitate a quantum acceleration in Australia's (and the global) digital economy.

Goods, services, entertainment and critical infrastructure are increasingly migrating to the Internet. IPv6 will allow control of every day office and home appliances using web based protocols. Water, power, gas and telephony smart grids and sensors will increasingly use internet reachable computer systems to deliver greater efficiencies and greener solutions, while at the same time creating vulnerabilities for critical utilities that have not existed in the past.

Faced with our increasing reliance on technology, networked systems and databases and the money that can be made by perpetration of malicious cyber

attacks and fraud, there can be little doubt that cyber crime will continue to escalate.

Motivation for cyber crime activities typically revolves around fame seeking, financial gain, revenge and political motivations. Examination of the evolution of malicious code shows that while early attackers in the 80s and 90s were primarily concerned with distribution of viruses and defacing websites, current trends show a significant increase in the criminal use of ICT for profit.

While disgruntled employees remain a substantial threat within organisations, organised cyber criminal activity will continue to increase proportionally to the return of investment from illegal cyber activity.

The ACS also believes that there is worrying emerging trend of State based cyber warfare. Titan Rain and the Estonian and Georgian cyber wars provide a rare public window into State endorsed cyber crime. Where States turn a blind eye or covertly fund individuals or groups to attack critical infrastructure or steal commercial and military information, the distinction between cyber crime and cyber warfare becomes blurred.

State endorsed cyber criminal activities can take on a much more sophisticated level of penetration than hackers acting alone. Furthermore, State trained or funded agents eventually find themselves back in the public domain and are likely candidates for organised crime syndicates and terrorist groups.

Factors that are influencing and enabling cyber crime include:

- lack of public, business and government awareness of the full extend of cyber crime activities making cyber crime easier to conduct;
- secrecy surrounding victims of cyber crime, its extent and impacts which is often linked to a fear of public loss of confidence and consequent loss of business, for example, the banking industry;
- no regulatory basis for the registration and control of ICT security professionals and other practitioners managing national and business critical IT based infrastructure;
- intrinsic integration of ICT into our daily work and home lives;
- greater globalisation of networks with data flowing through many jurisdictions with differing levels of trust and security;
- the Internet is difficult to control and the Internet was originally designed for sharing of information, which resists external attempts to control its digital content;

- rapidly increasing speeds of broadband networks and permanent Internet connections[1];
- organised crime activities; and
- State based/funded cyber activities.

With the window between vulnerabilities being detected and associated malicious code designed to exploit the vulnerability getting shorter, it has become more difficult for signatures to be developed in time to prevent the spread of malicious code.

Consequently, firms and community end users can no longer rely on signature and database reliant intrusion detection systems alone. The changing nature of the threat landscape using web technologies (such as web 2.0/AJAX and beyond) requires the development of new security technologies and techniques to counteract these emerging threats. Multi-faceted approaches including reputation based security mechanisms are becoming increasingly important.

To this end, the ACS believes the recent announcement by the Government to develop a Cyber Security Operations Centre to address cyber threats to be a highly praise-worthy initiative to develop new approaches to address online vulnerabilities. The ACS considers that the Cyber Security Operations Centre should actively engage with and cooperate with industry and other well established and respected cyber security organisations such as AusCERT, Crimtrac, GovCert and Austrac for example, to ensure a coordinated approach to cyber security initiatives and to fully leverage expertise and skills available in this area.

PREVALENCE OF CYBER CRIME

CSO recently reported[2] that Australia has comparatively high rates of cyber crime and that Australians are now more likely to experience cyber crime than burglary, assault or robbery.

The Australian Institute of Criminology report number 60[3] indicates that 32 percent of online traders experienced online fraud in 2004 and that 60 per cent of online fraud victims had an annual turnover of $500,000 or less, indicating that SMEs were most vulnerable to online fraud attacks.

An ABS 2007 study[4] found that 5% of the population or 806,000 people had fallen victim to fraud including credit card fraud, identity theft, phishing and financial

---

[1] Choo, K K R., Smith, R G., & McCusker, R., "Future Directions in Technology Enabled Crime: 2007-09", Research and Public Policy Series No. 78, Australian Institute of Criminology

[2] www.cso.com.au/article/224070/australia_tops_global_cyber_crime_impact_survey

[3] Charlton, K., & Taylor, N., "Online Credit Card Fraud Against Small Businesses", No 60, Research and Public Policy Series, Australian Institute of Criminology

[4] http://news.smh.com.au/national/personal-fraud-cost-1b-per-year-abs-20080627-2y1m.html

advice and other scams, costing around $1 billion. A 2003 study by AUSTRAC[5] found a similar cost of identity fraud for businesses as being around $1.1 billion.

The Symantec Internet Security Threat Report for 2008 reports that it detected 1,656,227 malicious code threats in 2008, representing 60 per cent of the 2.6 million threats it has detected over time, showing a very dramatic increase in the proliferation of malicious code.

These are fairly staggering statistics. They provide a good indication of the extent and prevalence of online fraud and attacks with malicious code within the Australian community and that it is a highly profitable undertaking for the perpetrators.

This issue has been brought starkly into the light with recent bombardment of online phishing attacks on banking and Australian Taxation Office customers, during May and June 2009, seeking to steal account and credit card passwords. Emails were seemingly on bank or ATO letterhead and bore the ABN number and other credentials. What's more, the attack included an automated call centre requesting account number details and passwords that were clearly linked to a payment gateway that was attempting authorisation on any credit card details provided.

The very low level public response or campaign from the financial institutions involved or the ATO to inform the community of the danger, indicates how ill prepared we are for these types of attacks and the difficulties government and industry face in knowing what the best response is to limit the damage from such widespread attacks.

These statistics provide a clear demonstration that current security frameworks are not proving effective in meeting current and emerging security threats. It also demonstrates that community end users are not well educated in the use of personal protective measures to counter these threats.

IMPLICATIONS OF RISK ON WIDER ECONOMY INCLUDING GROWING IMPACTS OF BOTNETS

Internet based fraud is impacting on consumer and business confidence in doing business over the Internet and so impacting the development of our digital economy.

The Sensis e-Business Report for July 2008 indicates that security is the primary barrier for SMEs moving to online business models.

---

[5] http://www.zdnet.com.au/news/security/soa/ABS-Australians-slugged-with-AU-1-billion-fraud-bill/0,130061744,339290236,00.htm

Further, changing work practices based on mobile and wireless technologies are creating a more mobile workforce. End user clients represent the weakest link in the e-security framework and firms are increasingly required to provide access to their networks to support mobile working arrangements.

Many offices now have connections to their internal (and trusted) networks from home offices. An employee's home network is increasingly becoming part of the corporate network and employees may need to connect from internet cafes, hotels, internet hotspots or other external environment where security measures are unknown. Web based attacks are now the primary vector for malicious activity[6] and most web based attacks are launched from legitimate web sites that have been compromised.

This largely means that for many firms, the perimeter of their trusted internal network is breaking down with changing workforce, business requirements and the increase in the extensive array of work activities that rely on access to the Internet.

This has major implications for how firms and end users think about their business intelligence gathering, risk assessment and security measures in that cyber security and associated risks to business and data need to be incorporated into wider security programs. Business intelligence and business continuity plans should also include online criminal intelligence analysis and threats to critical business ICT infrastructure.

Business risks associated with cyber crimes are increasingly likely to involve attacks from inside the organisation because of changing workforce practices and, because of potential financial and other motives (such as revenge), workers will increasingly be persuaded to execute attacks on firms for which they work.

In addition to firms increasing their focus on cyber crime, it is becoming increasingly imperative that governments and industry give more focus to cyber threats in securing critical infrastructure.

In Australia, critical infrastructure includes banking and finance, emergency services, energy and utilities, food, health care, IT and communications, mass gatherings (event spaces, national monuments and the like), transportation and water. These services are increasingly going online or becoming reliant on online systems, creating opportunities for cyber crime and sabotage of critical infrastructure that did not previously exist.

Two Australian examples provided by the Australian Institute of Criminology[1] include:

---

[6] Symantec Internet Security Threat Report Trends for 2008, Volume XIV, April 2009

- an employee hacking into the Maroochydore sewage management system software to release sewage into a public area causing significant environment damage; and
- inappropriate access by a Centrelink employee to customer records.

Perceptions that cyber crime is difficult to trace and that sanctions for those who are caught are lenient, do little to deter cyber criminals.

In fact, many cyber criminals operate from emerging countries that do not have strong sanctions, checks or controls or an effective law enforcement capacity for cyber crime activities, so exploiting jurisdictional differences and poor international coordination and cooperation on cyber crime activities.

Use of Botnets

Botnets are at the forefront of commercialisation of cyber crime and are becoming the tool of choice for organised cyber criminals. They can be designed to disrupt target systems and fast flux and peer to peer botnets are difficult to locate and difficult to close down.

Botmasters rent botnets and their technical services significantly lowering the technical barriers for cyber crime. Non technical criminals can now effectively commit cyber crime using rented botnets.

The CRS January 2008 Report for Congress[7] on botnets and cyber crime estimates there were 237 million security attacks globally in 2005 with the most frequent attacks against government agencies, financial institutions and health care providers.

In 2007 there were 1,400 command and control botnets active on the Internet controlling some three million infected computers.

More recent reports[8] estimate that by 2008 there were over 1.2 million infected computers in China alone.

Botnets are used for a range of activities including money laundering, phishing, disseminating malware, hosting data, spamming and crippling web sites with denial of service attacks by, for example, hitting the site hundreds of times per second.

---

[7] Wilson, C., "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", January 2008, Congress Research Service

[8] http://www.cw.com.hk/content/chinese-regulations-target-rising-cybercrime

In 2006 it was estimated that an unprotected computer had a 50 per cent chance of being enslaved into a botnet within 30 minutes of being connected to the Internet[1].

All e-security commentators agree that botnets are going to grow in their sophistication and use with the greatest number of threats originating from China and Argentina. And while botnets predominantly consist of fixed computers, mobile devices (phones, PDAs etc) are now poised to become the predominant means of accessing the Internet, so creating a new target for cyber criminals[9].

Given that many people synchronise their mobile devices to their fixed computers (both at work and home) this creates new opportunities for cyber criminals to gain access to sensitive information in emails and passwords for internet banking and the like.

Mobile banking is typically done using an SMS banking program which exchanges transactions with an SSL enabled web server running at the bank. While this protects transactions from the mobile provider to the bank, there is no such protection between the mobile device and the mobile provider.

Current mobile operating systems are not proving to be any more resilient to attack than those of fixed computers[9]. Most new smart phones now include similar operating systems to desktops and allow users to install programs from the Internet. This allows attackers to target popular mobile software download sites to gain access to the mobile phone population.

HTTP based botnets are on the rise and coupled with the ubiquitous use of instant messaging and peer to peer protocols, this places botnet development on a convergent evolutionary path with mobile platforms, as they move towards direct IP internet access.

The ACS believes that the rise of use and sophistication of mobile devices means they will become a clear focus of cyber criminals over the next 2 to 3 years with the potential for significant economic impacts (in terms of loss and implementation of protection measures) on users, businesses and mobile service providers.

LEVEL OF UNDERSTANDING AND AWARENESS WITHIN AUSTRALIAN COMMUNITY

The Australian Institute of Criminology[1] reports that organisations have, over recent years, worked to improve their protection from cyber attacks through the use of security technologies, information security policies and procedures and

---

[9] Vanhorenbeeck, M., "Mobile botnets: an economic and technological assessment" avail at http://www.daemon.be/maaten/mobbot.html

information security standards. Key areas of vulnerability that remain are in inadequate staff training and poor security culture.

Users of mobile platforms are reported to be the most significant risk for corporations with 75 per cent of mobile users reportedly ignoring security threats when working on the go[10], with 28 percent saying they hardly ever consider security risks associated with mobile platforms.

CSO has reported[2] that most Australians have a relatively high awareness of internet security and demonstrated the second highest level of confidence in the protection provided by their software security vendor. The reports also indicated that 77 percent of users were aware of the need to keep their security software up to date.

While this is essentially good news in terms of traditional security concerns for PCs and laptops, looking at the implications of the above factors seems to suggest that Australians are placing their confidence in intrusion systems and software that rely on signature and database mechanisms but are not aware of the risks and problems associated with new emerging cyber crime techniques or that mobile devices represent a significant cyber security risk.

Obfuscated malicious code or other dynamic attack vectors are being developed to get around traditional security systems. In fact, attacks using infected email attachments are decreasing. However there has been a rapid increase in web based malicious vectors using code obfuscation to avoid detection.

The ACS believes that government and industry (hardware and software vendors) need to work together to improve education and awareness across business and end user communities to ensure they are aware of e-security threats, emerging trends and the measures they can take to ensure their online safety.

Education programs must include emerging trends associated with the security risks from using mobile platforms.

The ACS believes that governments should look to developing agreements with vendors to ensure that computer systems and mobile devices are not sold without supplying adequate e-security and cyber safety information that covers not only current threats but also emerging threats.

INITIATIVES PRESENT AND FUTURE TO MITIGATE E-SECURITY RISKS

The ACS believes that initiatives like E-Security Week and the recently announced Cyber Security Operations Centre are important developments in both promoting e-security and in setting up the infrastructure to combat cyber security threats.

---

[10] http://www.pcauthority.com.au/news/90352,mobile-workers-still-clueless-about-security.aspx

The best form of defence is for the Government to regulate and control practitioners who lead and manage our nations' ICT based critical infrastructure. Registration of practitioners will allow trusted authorities to share timely updates and information about threats. Education standards can be stipulated and disciplinary actions can be taken over poor practice. These are standards that industry and the public takes for granted as being integral to the practice of many other high trust occupations such as law, medicine, teaching, accounting, electricians, plumbers and the like.

ACS believes it is essential we require these standards for ICT professionals as well.

Businesses can better protect themselves by:

- participating in information sharing with government agencies and other firms within their industry sector;
- better employee background checks;
- employing ICT professionals who are certified and who subscribe to a code of ethics and code of professional conduct and practice;
- conduct employee awareness programs and develop appropriate policies and procedures; and
- ensure data and systems are protected by up to date practices and intrusion detection software that is resilient to botnet and malware attacks. This should include patching, malware and intrusion detection, network segmentation and incident management procedures.

Firms can also help reduce their susceptibility to cyber attack by:

- creating a more heterogeneous systems environment so that common avenues of attack are harder to find;
- developing differing architectures;
- being careful about the use of commercial off the shelf software for mission critical areas;
- implement education programs that put responsibility onto individual behaviours instead of reliance on technology alone; and
- undertake regular, frequent, systems level reviews to determine vulnerability to attack.

Taking the above actions and a basic risk management approach is estimated to prevent around 80 per cent of attacks. However, even with an appropriate cyber security plan and methodology in place, firms need to cater for an attack so that it can be effectively contained, data and financial loss minimised and restored if necessary.

International Cooperation
Cyber crime is a global industry that operates across jurisdictional borders. Ultimately, to reduce the impacts of this industry, governments and industry also need to be able to operate effectively across jurisdictional borders to investigate and close down attacks and threats.

This requires the need to share information, intelligence and expertise across jurisdictional borders to anticipate and address new tends in cyber crime.

We need greater harmonisation of international laws with improved, globalised cooperation and consistent regulation, enforcement and punitive regimes to reduce jurisdiction shopping.

Proposals have been floated recently that would provide for each nation's Computer Emergency Response Team (CERT) to have the authority to enforce penalties and order take downs of command and control botnets for example. This approach would require global coordination and consistent approach amongst CERTs.

Addressing cyber crime will increasingly involve the cooperation of ISPs across multiple jurisdictions and domain name registrars for access to data and to take down sites.

As the governing body for internet registrars, ICANN can play a significant role in reducing the level of internet based cyber crime by ensuring greater professionalism amongst its Registrars and greater vigilance on domain name and IP address registration.

Traditional methods of international legal and jurisdictional cooperation and mutual assistance are not nimble enough to adequately address cyber crime where changes in exploitation methods and jurisdiction can occur daily. A much more nimble approach is going to be needed if we are to successfully track down and prosecute perpetrators of cyber crime.

Combating Future Risks
Ultimately, many cyber crime risks can be mitigated by industry developing more secure hardware and software and integrating improved security into the software and hardware development cycles.

Technology must become more trustworthy in terms of its security vulnerabilities.

The competitive nature of computing and the rush to market to achieve first mover advantages appear to be driving a less thorough testing of code, system and hardware vulnerabilities.

The ACS would like to see vendors embrace secure development of applications (SDA) more fully, on a voluntary basis and in accordance with international standards to which all hardware and software developers and suppliers sign up to comply with. This would allow end users to purchase from those who advertise compliance and improve trustworthiness of technology amongst end user businesses and consumers.

In particular, the ACS believes that an essential part of decreasing vulnerability to cyber crime is for developers to have a greater willingness to test and retest software and hardware to ensure vulnerabilities are removed.

Retrofitting security patches and updates for released systems is costly and allows exploitation of end users during the window of vulnerability.

ACS believes that jurisdictional Computer Emergency Response Teams (CERTS) have a major role to play in protecting critical infrastructure, information sharing, enforcement and education of communities on current and future threats.

AusCERT and GovCERT are in a prime position to spearhead Australia's efforts (in accordance with international agreed standards) and through international collaboration, increase our knowledge of victim and offender behaviour so that we can more effectively respond to and prevent cyber crime.

Finally, the ACS believes that improved training and education of businesses and end users and improved professionalism of ICT practitioners must be considered equally along with any law enforcement and international cooperation methods of combating cyber crime.

Improved ICT literacy amongst end users, knowledge of vulnerabilities and the appropriate actions to take in case of infection are key weapons in reducing the impacts of cyber crime.

KEY MESSAGES AND RECOMMENDATIONS

The ACS wishes to put forward the following key messages and recommendations which we believe will significantly improve cyber safety for all business and end users in Australia.

1. The ACS applauds the recent Federal Government announcement to establish a Cyber Security Operations Centre and believes that to achieve the best outcomes, it should work collaboratively with industry and other cyber safety agencies such as AusCERT, GovCERT, Austrac and Crimtrac to ensure cooperation and information sharing to achieve the best results and maximum leverage from the resources devoted to cyber crime in Australia.

2. Changing work force dynamics, the reliance on web based technologies and the increasing use of mobile platforms means that the perimeter of trusted networks is breaking down for many firms. All firms should be encouraged to develop business intelligence and business continuity plans for their critical ICT infrastructure.

3. The ACS believes that smart phones and other mobile devices will become the clear focus of cyber criminals over the next few years with the potential for significant economic impacts on businesses, governments and end users.

4. Given the changing nature of security threats, it is critically important for Australia to invest in R&D in security technologies which are relevant to protecting computing systems and information infrastructures in the digital economy. These include secure and trusted distributed information and network systems, mobile software systems and networks and secure applications and web based online services.

5. Governments must establish a basis for registration and control of ICT security professionals who work with business and national critical ICT based infrastructure. The standards that industry and the public takes for granted as being integral to the practice of many other high trust occupations such as law, medicine, teaching, accounting, electricians, plumbers and the like must also apply to ICT professionals.

6. All firms, particularly SMEs, should be encouraged to develop and keep up to date their knowledge and an appropriate cyber security plan and methodology to that they can respond to and effectively contain a cyber attack to minimise damage and financial loss.

7. The ACS believes that Governments should look at developing agreements with vendors to ensure that computer systems and mobile devices are not sold without supplying adequate e-security and cyber safety information that covers current and known emerging threats.

8. The ACS would like to see vendors embrace secure development applications (SDA) more fully on a voluntary basis and in accordance with internationally agreed standards. This would allow users to purchase products that comply with international secure development applications standards.

9. ACS believes that jurisdictional Computer Emergency Response Teams (CERTS) should have a greater role to play globally in protecting critical infrastructure, information sharing between countries, enforcement and shut down of sites and education of communities on current and future threats.

10. Increased professionalism globally amongst ICT practitioners, training and education of business and end users and improved ICT literacy of communities must form an integral part of any program to reduce the impact of cyber crime.