

Review of the e-Security National Agenda

Submission from AusCERT

Part A

8 June 2006

1. Executive Summary

As noted in the *Review of the E-Security National Agenda Discussion Paper*, the Internet threat landscape has changed fundamentally since 2001 when the e-Security National Agenda framework was first released.

Based on this fundamental change, this review provides an opportunity for the Australian government to consider implementing a range of practical strategies that will help reduce the level of Internet based attacks emanating from or targeting Australian networks, particularly those motivated by illicit financial gain.

While user awareness is vital and should be improved, by itself it is not sufficient to effectively address the threat. Therefore, the Australian government should look to implement additional initiatives which benefit the broader Internet using community as a whole.

This submission puts forward AusCERT's recommendations based on the knowledge and experience gained as Australia's national CERT.

Due to the sensitive nature of some of AusCERT's work, we have prepared two submissions – Part A (for public release) and Part B (not for public release) which describes in more detail the reasons for our recommendations and aspects of AusCERT's operational¹ activities.

2. Recommendations

In summary, AusCERT recommends:

1. the need for improved international incident response arrangements to deal with Internet based attacks motivated by illicit financial gain;
2. the need for proactive detection, analysis and response arrangements within Australia, including:

¹ AusCERT is a not-for-profit organisation based at the University of Queensland, which must cover its operating costs including its national CERT activities, through a combination of government funding and fee-for-service arrangements.

- greater support for AusCERT's in its role monitoring, detecting, responding to and analysing online ID theft attacks affecting Australian networks and Australian Internet and e-commerce and e-government users
 - enhanced malware analysis capability to support operation incident response arrangements and threat mitigation advice
 - the deployment of national network monitoring capabilities to enhance early warning of serious, widespread cyber attacks affecting Australian networks
3. the need for improved user-awareness
 4. the need for research and development into trusted systems
 5. actions to address the skills shortage for experienced IT security staff.

3. About AusCERT

As the national CERT, AusCERT is an independent, not-for-profit organisation that supports the Australian public interest by helping to protect the security of the Australian Internet using community, primarily by:

- Monitoring, analysing and providing advice about computer network threats and vulnerabilities
- Providing assistance to Australian networks facing attack sourced from within Australia, or more often, overseas.
- Providing advice on how to protect against and recover from computer security attacks.

AusCERT, together with the Australian High Tech Crime Centre (AHTCC), has been at the forefront of monitoring, analysing and responding to incidents of online ID theft in Australia since March 2003. Based on this work AusCERT has written a number of reports about the threat and mitigation strategies. We refer the review to these reports which will be made available upon request:

- AusCERT (2006), Case study – personalised phishing site
- AusCERT (2005), e-government phishing attack was aided by poor coding on legitimate government web site
- AusCERT (2005), Managing Risk Associated with Online ID Theft for Government and Providers of e-Government Services
- AusCERT (2005), Trends and Developments in Online ID Theft – Update No. 2
- AusCERT (2004), Trends and Developments in Online ID Theft, No. 1
- AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, *2006 Australian Computer Crime and Security Survey*, page 24 - 28

- AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, *2005 Australian Computer Crime and Security Survey*, page 24 - 26
- AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, *2004 Australian Computer Crime and Security Survey*, page 24 - 25
- AusCERT, AFP, Queensland Police, South Australia Police, Western Australia Police, *2003 Australian Computer Crime and Security Survey*, page 19

4. Nature of the threat environment

The most significant aspect of the changes that have occurred since 2001 is the prevalence of cyber attacks motivated by illicit financial gain and the focus of attack activity on host systems and applications of both home and enterprise users.

In five years, e-commerce, e-banking and e-government have experienced significant growth. In the same period, we have seen significant growth in the use and uptake of these services by the public and of the adoption of high speed broadband technologies in Australia.

As the information economy grows and matures, there is now increased opportunity and motivation by attackers to compromise computers for the inherent value of information that can be stolen from them and/or to use compromised computers to assist with other forms of cyber attacks, also motivated by illicit financial gain.

Of the cyber crimes motivated by illicit financial gain, the most worrying and certainly most prevalent are the increased incidence of online identity theft attacks.² This relatively new³ form of crime poses the single greatest threat to trust and confidence on the Internet and, if left unchecked, will significantly harm the capacity of the Internet to be a suitable medium for e-commerce and e-government.

The threat of online ID theft for users of e-government and e-commerce services is assessed to be high.⁴ The large rise in online ID theft attacks observed by AusCERT since March 2003 predominantly involves the compromise of client computers (ie. trojan attacks) and/or fooling the users of client computers to disclose their online access credentials (or other personal information), ie, through phishing attacks.

Each phishing or trojan attack that occurs typically leads to the theft of potentially sensitive information from many hundreds of users. The success of these attacks and

² An online ID theft attack is a distributed system of hosts, domain names and in some cases, malware, that is designed to steal online identity credentials, a range of other sensitive personal information and computer system information from compromised computers on a mass scale.

³ Attacks of this nature were first detected in Australia since March 2003 and have been increasing in Australia and in other countries ever since.

⁴ For a more detailed discussion of the threat of online ID theft see: "Trends and Developments in Online ID Theft – Update, No. 2", June 2005, <http://www.auscert.org.au/5769> and "Implications of Trends and Developments in Online ID Theft", September 2004, <http://www.auscert.org.au/5768>

the ability to derive significant financial (and other) benefits with little or negligible risk to the perpetrators are also contributing to the growing levels of attack.

The advent and rapid evolution of online criminal activity has also impacted on other areas of information security including:

- The rise of malicious spam email which is currently the primary vector for both phishing and malicious code attacks.
- A rapid rise in the level and sophistication of malicious code development aimed to compromise computers and gain access to the information they hold and carry.
- A significant increase in “botnet” activity as compromised computers are aggregated as “assets” in a wide range of criminal activity from the delivery of malicious spam to extortions using distributed denial of service attacks. Botnets are also being harnessed as a powerful resource to leverage phishing and malicious code attacks.
- A growing number of Australians being successfully targeted via spam as “money transfer agents” or “mules” with the specific role of engaging in direct criminal activity to transfer illicit financial gains to criminal groups who are invariably based offshore.

The rapid development of online criminal activity, such as ID theft, cannot be viewed in isolation and there are clear indications that the rise of online criminal activity and the associated information resources being gained is in turn being used to support a growing range and level of traditional or physical criminal activity particularly in the area of ID theft and takeover. In effect the criminals are now claiming many of the same benefits that information technologies have provided to government and industry to drive and support their offline criminal activities.

4.1 Remote client side computer security

Computers used to access e-government and e-commerce services remotely may range from home computer systems, to client computers operated by small businesses or large public or private sector organisations. The design weaknesses in main stream operating systems have been recognised for around three decades.⁵ Security features and application layer add-on security counter-measures, such as firewalls, anti-virus (AV) software etc, can all be subverted due to software vulnerabilities in operating system or application software.^{6 7}

⁵ Losocco, P.A., Smalley, S.D., Muckelbauer, P.A., Taylor, R.C., Turner, S.J, Farrell, J.F. (1998). The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments, National Security Agency, <http://www.jya.com/paperF1.htm>

⁶ Reid, J (2005), “Prospects for Improved Operating System Security”, *2005 Australian Computer Crime and Security Survey*, page 28, <http://www.auscert.org.au/crimesurvey>

⁷ Caelli, W and McCullagh, A (2000), “Non-Repudiation in the Digital Environment”, http://www.firstmonday.org/issues/issue5_8/mccullagh/
Caelli describes a trusted computing system as one which “performs in accordance with its documented specification and will prevent any unauthorised activity. Specifically a trusted computing system can be relied upon to enforce a documented security policy”.

The nature of cyber attacks currently being launched against the users of home computers and client computers on corporate networks is such that a range of security counter-measures (both technological and procedural) must be applied on an ongoing basis in order to be capable of preventing most attacks.⁸

Even when computer users follow the ‘minimum’ recommended security practices,⁹ it is still possible for their computers to be compromised. Attackers have shown they understand and are willing to exploit periods of heightened vulnerability when operating system and application security counter-measures are more likely to fail. That is, attackers are developing exploits which take advantage of new vulnerabilities, especially in browser software. Attackers are also well-practised in modifying trojan variants deliberately to ensure they are undetectable by most AV products at the time of release.

Regardless of whether users *should* take more responsibility and interest in the security of their own PCs, government and industry cannot reasonably expect that all, or even most, users will take the minimum security precautions or necessarily understand how to secure their computers before they use e-government and e-commerce services. It is unreasonable to expect there will be a high level of security on such computers given user habits and users own expectations with regard to their “online” behaviours.

4.2 Future threat

AusCERT assesses that the level of online ID theft and other financially motivated cyber crimes will continue to grow as:

- More Australians adopt broadband technology;
- More Australians and Australian organisations in the public and private sector provide services and information online with a direct or potential financial value¹⁰;
- Single factor authentication remains the primary means of authentication for e-government and e-commerce transactions;
- The underlying security of mainstream operating systems continue to be vulnerable to compromise;
- The level of skill required to effectively secure a remote client computer and to recognise common techniques attackers use to fool users into taking risks online increases; and
- Attackers succeed in generating illicit financial revenue from the attacks with a low level of risk when they operate abroad from the countries and computer users which they target.

⁸ AusCERT recommends specific minimum mitigation strategies be used before using e-government or e-commerce services. See “Protecting your computer from malicious code”, www.auscert.org.au/3352

⁹ The quality of advice in the public domain varies. Some advice is inadequate, misleading or misinformed.

¹⁰ Personal information has a potential financial value if an attacker uses that information to commit other forms of financial fraud.

- The risk of successful prosecution or even identification of the criminals themselves is low to negligible. At this stage there is no credible deterrent to online criminal activity in the face of staggering economic returns. The development of a whole underground economy based around on-line attack activity is testament to the success of this new type of criminal activity.

5. Review questions

5.1 What do you believe are the respective roles of government, industry, home users and the research community in addressing the management of e-security threats and vulnerabilities?

Government's role is to provide support for prevention, detection and response strategies, particular when the nature of the threat is such that it is difficult for the individuals and organisations impacted to do so directly or adequately.

The cost and expertise involved in preventing or responding to a single breach can often be disproportionately high and is not representative of the cumulative impact of many breaches, particularly if this occurs over a wide range of target individuals or organisations or for society as a whole.

If left to individuals or individual entities, appropriate prevention, detection and response strategies may never be established due to the classic risk versus reward trade off. Therefore, it is incumbent on the government to implement and support strategies and initiatives which will reduce the number of attacks occurring in Australia and globally; and to put in place measures to help detect and respond to attacks that are occurring. Further, it is in the governments' interests to do so as high levels of attacks will lower confidence in and uptake of e-commerce and e-government services.

It is also government's role to follow best practice examples in the way it delivers e-government services and in the way it provides advice to users and the public about security and privacy impacts for users of those services.

Privacy is being breached by those launching online ID theft attacks and there is nothing in the privacy provisions which will help mitigate the risks associated with this threat. The privacy provisions relate solely to how the government and large companies handle and store personal privacy information. There is no requirement to assess, or to provide warnings about, whether the remote client computers being used to access e-government or e-commerce systems are fit for purpose. Insecure remote client computers can be used (ie, compromised) by criminals to steal or modify personal information as a direct consequence of using e-commerce or e-government services.

Discussions of the security of e-government and e-commerce systems, must by their very nature, consider and incorporate the remote client computers and the users which make up part of that system, not just merely focus on the security of the server side and communication channel.

5.2 How can these various segments of the Australian economy work together to address e-security threats and vulnerabilities?

There is already close working relationships between AusCERT, the AHTCC and the banking and finance sector in dealing with this problem, and through and between AusCERT and its international CERT counterparts. This model can be extended more broadly, with appropriate support for AusCERT and the AHTCC in their complementary roles.

5.3 How can government and industry work together to improve e-security awareness raising activities in Australia?

- By providing more direct support for AusCERT as the national CERT to provide a better service to the Australian Internet using public as a whole. This will benefit all Internet users in Australia. A good model is CERT.br which is centrally funded by the Brazilian Government from the proceeds of Internet delivery revenues as a service to the Internet Community of Brazil.
- By promoting a single organisation to provide authoritative, independent, expert Internet security advice to the Australian Internet users, the process of selling the right messages is made easier for everyone. Certainly the recipients of that advice will receive accurate, timely and consistent messages over time.
- By reducing dependence on government and various industry associations as the primary advice providers, the public is likely to have increased confidence in the advice by eliminating any perceived or actual conflict of interest which may arise from being both a provider of e-government services and by encouraging and promoting the online information economy.
- Government can help bring together and coordinate the wide array of agencies, departments and relevant industry groups trying to deal with the real and present threats to the online environment. One example would be to coordinate and assist the state and federal consumer protection bodies that are grappling to understand and deal with online activity.

5.4 Which awareness raising initiatives are you aware of that have been successful?

4.1 Without a scientific study to measure awareness levels before and after a specific program it is difficult to assess what initiatives have been successful in Australia.

4.2 Given the increasing number of phishing attacks that continue to be directed against Australian Internet users, it would appear that efforts to date have not been successful. While phishing attacks continue to effective for a small percentage of those targeted, they will continue to occur. For example, there will always be new users across a variety of age groups that are not aware of what a 'phishing' attack is; and how to recognise such attacks who

will therefore be fooled into breaching their own security. Of course any awareness campaign needs to focus – not just on phishing attacks – but on a whole range of common Internet based threats and the relevant mitigation.

4.3 It is more important to identify what are the desirable features of an awareness raising campaign for the target group, ie, home users and small business owners. AusCERT believes that the best approach is to ensure that the advice is provided from a single independent, authoritative source of expertise on computer security.

4.4 This ensures that the message being given by all tiers of government is consistent, comprehensive, accurate, timely and authoritative based on the advisory body's direct experience in monitoring, analysing and monitoring different types of Internet based attacks affecting the target group.

4.5 The advice must be reasonably detailed and comprehensive but conveyed clearly and concisely, using wherever possible diagrams or simple step-by-step guides.

4.6. Some existing web sites designed to raise awareness (eg scamwatch.gov.au), are lacking in useful information about common attacks, eg, phishing scams and trojan attacks – both of which are online mechanisms designed to steal simple authentication access credentials and personal information with a potential financial value.

5.5 What role do you believe international collaboration should play in Australia's e-security capabilities?

- International agreements between governments, CERTs and law enforcement are vital to address this global problem. The reality is that most attacks directed at Australians are sourced overseas and vice versa. In other words we are frequently dependent on overseas based CSIRTs, law enforcement, domain name registrars, ISPs to help resolve or mitigate an ongoing attack against Australian users or organisations.
- Improved responsiveness is therefore required from these sources at various times. This must be a reflection on the rapid and near real time nature of the Internet itself. Attacks in the Internet domain are measured in hours and minutes not days and weeks. Responses therefore need to be authoritative, flexible, rapid, well organised and practised.
- As attack levels against Australian interests sourced from overseas increase, so too must local response arrangements. It is unreasonable to expect assistance from overseas entities if Australia is unable to offer the same level of responsiveness in return.
- The government has a critical role to play internationally to put in place bi-lateral and multi-lateral agreements to facilitate this. This is work is a logical extension of the work done by ACMA in gaining support for improved anti-spam legislation internationally and enforcement within

countries abroad, as this has a direct bearing on the spam being directed against Australian Internet users.