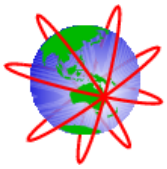
SUBMISSION NO. 30



AusCERT

Australia's National Computer Emergency Response Team

House of Representatives Standing Committee on Communications – Inquiry into Cyber Crime

Background

The House of Representatives' Standing Committee on Communications has commenced an inquiry into cyber crime and its impact on Australian consumers. AusCERT was invited to provide a submission to this Committee inquiry.

In making this submission, AusCERT has addressed the committee's Terms of Reference.

Executive summary

If current attitudes and approaches to dealing with the cybercrime problem by government and industry do not improve, then gains in building an online economy, through the provision of new businesses, services and the physical infrastructure, will provide little benefit to our citizens, communities and economies. Rather, the online information and service economy will simply provide an opportunity for (predominantly overseas based) cyber criminals to prosper at our expense with relative impunity. Indeed, the harm to our citizens, communities and economies, could be far more reaching and serious than many realise as levels of fraud associated with identity theft continues to grow.

Ideally, the software, computer systems and networks should have security built into their design so current significant levels of resources and expertise is no longer required to defend against high volumes of cyber attack. Once it becomes difficult for criminals to conduct cyber attack (as opposed to now being relatively easy), the attacks will also significantly reduce.

About AusCERT

AusCERT[1] is Australia's national computer emergency response team (CERT). [2]

[1] www.auscert.org.au

[2] In May 2009, the Attorney-General's Department advised AusCERT that the Australian government would take over the role of national CERT from AusCERT and that it would contract AusCERT to provide some services to the Department in support of this role. As the new national CERT is not yet established, AusCERT continues to perform the role of national CERT on a self-funded basis.

AusCERT, which was formally established in 1993, is an independent, self-funded, not-for-profit, non-government organisation, based at the University of Queensland. AusCERT employs around 20 information and IT security experts.

As the national CERT for Australia, AusCERT is the primary point of contact for the provision of advice about computer network threats and vulnerabilities in Australia and provides an incident response service for Australian networks for cyber attacks emanating from both overseas and from within Australia.

Based on its unique operational role, AusCERT helps improve Internet security for Australian Internet users by:

- Detecting, monitoring and stopping Internet based attacks in progress directed at Australian Internet users and networks; and where possible taking further action to mitigate the harm that has already occurred from such attacks;

- collecting, analysing and providing advice about computer network threats and vulnerabilities; and

- providing education and advice about issues affecting Internet security in Australia and globally.

In making this submission, it should be recognised that due to AusCERT's substantial experience monitoring, analysing and responding to cyber attacks in Australia and from abroad for over 15 years, AusCERT has a sound understanding of e-security risks more generally. This understanding extends to a strong technical understanding of :

- how cyber criminals are able to defeat the security of computer systems, attack computer systems, take control of them and steal data from them;

- how the underlying infrastructure is open to attack and compromise and the limitations of various security related technologies and mechanisms which are put in place in an attempt to prevent or detect attacks.

Terms of Reference

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and trojans;

The nature and prevalence of e-security risks facing Australian Internet users,[3] including those which result in financial fraud and the theft of personal information, is significant and continues to worsen.

To understand the nature of e-security risks, it is important to understand why cyber crime is able to occur and why it is so prevalent. The issues are numerous and complex and not possible to fully explain within the limited scope of this enquiry.

The National Security Agency (NSA), in its paper, *The Inevitability of Failure: The flawed assumption of security in modern computing environments* (1998)[4] summarised a key aspect of the problem as follows:

> The goal of this paper is to motivate a renewed interest in secure operating systems. [The NSA] argues that the threats posed by the modern computing environment cannot be addressed without support from secure operating systems and, [...] any security effort which ignores this fact can only result in a "fortress built upon sand."[5]

This helps explain why cybercrime is so prevalent. We have built vast networks and information systems using technology that cannot be properly or easily secured, including despite the fact that the software security industry is big business in its own right. Although dated, the points raised in this paper remain as valid and relevant now as they were in 1998. The threat environment, however, has substantially worsened and the modern software environment has not kept pace.

The above paper focuses on operating system software, but the reality is that all software needs to be securely designed as vulnerabilities in application software, including browser plug-ins (such Adobe Flash and Shockwave), can result in the compromise of the entire

---

[3] By Australian Internet users we refer not just to consumers and home users but also governments and businesses that develop online systems to provide information and services for the Australian community more broadly. The security issues we discuss are not just problems for home computers and home computer users – the issues described here affect client computers at home and work and servers operated by businesses and government. We are all broadly consumers of software, IT services and online services across all segments of society.

[4] National Security Agency, http://csrc.nist.gov/nissc/1998/proceedings/paperF1.pdf (1998)

[5] Ibid., NSA

computer. This is due to the fact that for these applications to work they need access to privileged parts of the operating system.

Other aspects of the cybercrime problem are explained in more detail in AusCERT's submission to the Australian Law Reform Commission for its Review of the Privacy Act 1988[6] (pages 2-7).

It is difficult to provide comparable, consistent and reliable metrics within or across economies, however, there is ample reliable data from a variety of sources which supports the claim that the e-security risks are already serious and continue to worsen each year. This is well documented in the OECD malware report[7] which AusCERT contributed to.

It is difficult to gauge, through metrics, the impact of cyber crime, particularly cybercrime aimed at financial fraud and identity theft. It is possible to make estimates based on :

- The volume and nature of the attacks seen occurring, including those directed at Australian Internet users (this includes information and systems owned/used by governments, businesses and individual citizens/residents)
- Evidence of the number of known compromised computers arising from such attacks

Redistribution of compromised account information from logging sites

For the period December 2007 until the present, AusCERT processed compromised account information for 246 logging sites, an average of four per week.

A logging site is a compromised web site that is used by criminals to store captured web form data, account access credentials such as usernames and passwords etc, from computers infected with malware designed to capture that information. Typically, these attacks are used by criminals for illicit financial gain and personal identifying information and account credentials are harvested and accessed and/or sold.

The amount of captured compromised data each logging site holds varies but it is not uncommon to process many gigabytes of compromised captured data per log site, involving thousands of compromised computers.

---

6 http://www.auscert.org.au/8510 (2008)

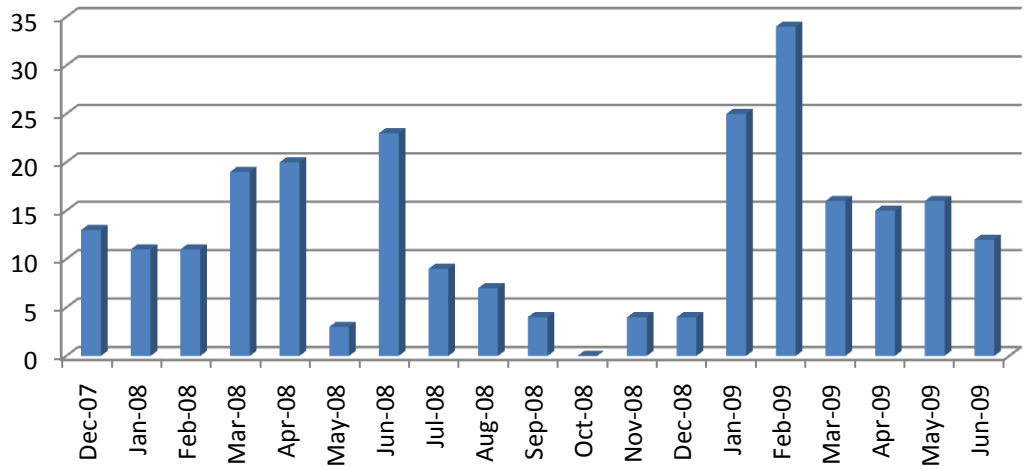
7 *Malicious software (malware): a security threat to the Internet economy*, http://www.oecd.org/dataoecd/53/34/40724457.pdf (2008)

While useful to know, AusCERT does not routinely count the number of unique IP addresses belonging to computers in Australia that were compromised as a result of these attacks. While the number of Australian compromised computers varies for each log file retrieved, in the past, AusCERT has found around 11,000 compromised hosts within Australia as a result of specific malware attacks.[8] This figure represents just a small fraction of the total number of compromises since AusCERT has taken action to mitigate this type of attack.

For the .au namespace, AusCERT found within the captured log data information relating to approximately 10,000 domains.[9] This means that these domains had online customers, clients or visitors to their web site with infected/ compromised computers and the malware captured the session data, including SSL encrypted sessions, from the connections to these domains' web sites/networks. In most cases there will be multiple domains visited and captured for each compromised computer.

[8] AusCERT, *Haxdoor – Anatomy of an ID theft attack using malware*, http://www.auscert.org.au/7069 (2006)

[9] This includes Australian brands that use gTLDs, such as .com.



Processed means parsing and distributing the captured malware data according to domain name groupings to trusted third parties who can help identify and notify the owners of these computers that their computers are infected.

In general each logging site represents a single attack. It is only possible to obtain and locate access to logging sites for a small proportion of overall attacks that occur. The variability of the number of logs processed is not a reflection of variability in attack numbers, but rather the difficulty in obtaining these logs.

Figure 1

Malware and phishing site attacks

Generally, malware hosted on web sites and phishing attacks hosted on web sites exist to facilitate the theft of large volumes of personal information (identity theft) and to conduct financial fraud. In most cases, criminals compromise legitimate web sites and computers belonging to third parties to host these attacks. Most of the attacks included in the graph below targeted Australian Internet users.

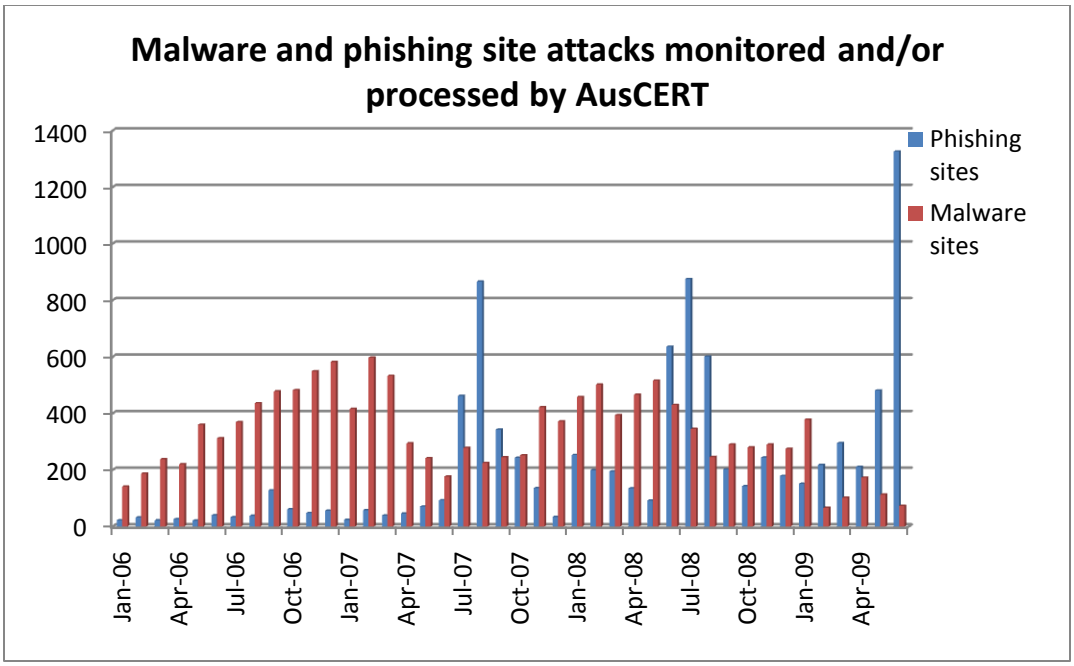


Figure 2

Impact of the phishing and malware attacks

Phishing mostly involves seeking to capture online banking access credentials, credit card details and to a lesser degree other personal information which could also be useful in facilitating online financial fraud.

At present, the banking community is bearing the direct cost of this form of financial fraud by reimbursing fraudulently transferred funds. Similarly the banking community has put in place significant counter-measures aimed at detecting and stopping fraudulent transactions, where possible.

Malware attacks, however, have a far greater potential impact and it is more difficult to quantify the range of actions which could ensue. Typically a Trojan malware attack will have the following characteristics and features:

- The ability to conduct information theft/fraud

  a) capture all passwords in protected storage (saved to the computer, via the browser)

  b) capture all keystrokes, mouse clicks and screen shots during log in sessions to obtain passwords not in protected storage

c) capture all form data submitted or accessed via a web site, especially for any https sessions which usually indicates more sensitive information. E-government web sites typically allow the submission or ability to access detailed personal information suitable to facilitate identity theft, now including individual's e-health records.

For some more concrete examples of the types of personal identity information being stolen, which provides an insight into the potential impact on individuals and businesses, refer to the following examples:

- *Haxdoor - Anatomy of an ID Theft Attack Using Malware,*[10] page 21
- *AusCERT Home Users Computer Security Survey 2008* ,[11] page 25

The theft of this personal identity information facilitates identity theft and financial fraud.

- The ability to take control over the computer (bots)

d) The Trojan malware also typically turns the computer into a bot under the control of the attacker. This allows the attacker to update the malware code to perform new actions at any time.

e) It allows the attacker to use the compromised computer to support and facilitate other forms of cyber crime such as sending out spam, hosting a malware web site, phishing or logging web site, or to participate in a distributed denial of service attack. Access to the compromised computer (bot) may be rented or sold to other criminals as a further source of criminal revenue.

f) The malware is also designed to defeat, bypass or deactivate other security counter-measures on the computer to prevent subsequent detection and removal.

These actions are aimed at maintaining control over the compromised computer and using it for other types of cyber crime beyond direct access to personal identity information and/or financial fraud.

Basically any client computer compromised with the type of malware described in this submission, and which are in widespread circulation, should not be used to conduct any trust-related transaction, including e-government or e-commerce transactions, without

[10] http://www.auscert.org.au/7069 (2006)
[11] www.auscert.org.au/usersurvey, page 25

expecting to suffer serious forms of financial fraud due to the theft of personal identity information.

Cyber attack data affecting Australian Internet users held by AusCERT demonstrates that the online cyber threat environment is harmful and aggressive. There is no shortage of Internet based attacks targeting Australian interests from criminals (interested in illicit financial gain) and vulnerable systems are being quickly exploited.

The incident data provides evidence of how efforts to prevent cyber attacks have failed in the community more broadly. We can potentially point to a variety of causes such as ignorance, negligence, lack of resources and capabilities or the sophistication of the attack vectors. The question should also be asked why should efforts to prevent cyber attacks require Internet users to:

- be experts in cyber defence
- have adequate resources and capabilities to devote to cyber defence

And even then we still may find that some attacks are so sophisticated that the aforementioned is not sufficient to prevent the attacks. The approach we are taking globally needs to change. Ideally, the software, computer systems and networks should have security built into their design so we no longer need significant resources and expertise to defend against high volumes of cyber attack. Once it becomes difficult for criminals to conduct cyber attack (as opposed to now being relatively easy), the attacks will also significantly reduce.

b) The implications of these risks on the wider economy, including the growing economic and security impact of botnets;

It is safe to estimate that many thousands of victims' computers are being compromised due to malware attacks that occur every day in Australia.

The cumulative impact of compromised systems, by their very nature, contributes to the cycle of attacks against other victims, including in Australia. The consequential harm for those computers, the data on the systems, and the personal and intangible impacts arising for the people and businesses affected are also substantial but are difficult to quantify.

Cumulatively it is likely that these attacks would erode confidence in the information and digital economy. This in itself can significantly harm Australia's economic interests.

The OECD report, *Malicious software (malware): a security threat to the Internet economy*, which AusCERT contributed to, provides useful background about the botnet problem and their role with malware, as the main tools of cybercriminals.[12]

The OECD report asserts that:

> A strategy for a global partnership against malware is needed to avoid it becoming a serious threat to the Internet economy and to national security in the coming years.
>
> Today, communities involved in fighting malware offer essentially a fragmented local response to a global threat.
>
> [...] Over the last 20 years, malware has evolved from occasional "exploits" to a global multi-million dollar criminal industry.[13]

If current attitudes and approaches to dealing with the problem by government and industry do not change and improve, then gains in building an online economy, through the provision of new businesses, services and the physical infrastructure, will provide little benefit to our citizens, communities and economies. Rather, the online information and service economy will simply provide an opportunity for (predominantly overseas based) cyber criminals to prosper at our expense with relative impunity. Indeed, the harm to our citizens, communities and economies, could be far more reaching and serious than many realise.

The aggregation and accumulation of large volumes of personal information that can be accessed or submitted online provides cybercriminals a smorgasbord of data for identity theft and the associated financial fraud. They have developed the attack tools (malware) and have access to vast numbers of compromised computers (botnets) which enable them to attack, steal and process stolen information on an industrialised scale.

This means that information that is meant to be private is, to a large degree, obtainable if we participate in e-commerce, e-health and other e-government services that involve providing or accessing our personal information.

The threat, however, is not only of widespread identity theft to the citizens of Australia, but industrial espionage, sabotage and nation state espionage and potentially sabotage, or other forms of politically-motivated disruption to services that are delivered through

---

12 OECD, http://www.oecd.org/dataoecd/53/34/40724457.pdf, page 22-27

13 Ibid. OECD, page 6

our online environment (such as the prolonged and widespread DDOS attacks directed at the Estonian and Georgian governments, business and citizens).

c) Level of understanding and awareness of e-security risks within the community;

In responding to this question, we wish to address the level of understanding and awareness as it applies to all levels within the community including home users, people in the work place, businesses and organisations that build and host public facing networked systems such as web sites/servers, mail servers, domain name servers, etc.

Given the level of attack AusCERT has previously described which is directed at home users, businesses and business/government web sites, domain name servers, mail servers etc then this is an indication that the level of awareness and understanding is lower than it needs to be across the community.

Without wishing to identify particular organisations in the public and private sector, sometimes the advice being provided to the public about how to mitigate particular threats is simply wrong and demonstrates their own lack of awareness of the problem.

For further information about home users' awareness of computer security issues, refer to the AusCERT Home Users Computer Security Survey (2008), [14] which demonstrates that certainly some home users hold misconceptions about the level of protection provided by various security technologies. This provides a false sense of security, and may lead to them taking unnecessary online risks.

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:

i) Education initiatives

[14] AusCERT, *Home Users Computer Security Survey 2008*, http://www.auscert.org.au/usersurvey page 23-26

By education initiatives, it is assumed that ordinary home users as consumers would not be required to receive formal education and training, in the way IT professionals would, to mitigate the security risks which they themselves can directly control.

Awareness raising, which is a 'softer' form of education, will only achieve very basic levels of security capability and for that to work consumers need to be motivated to learn about basic security counter-measures and apply them. Not all users are motivated and some will not have the ability to implement even basic security practices.

Bruce Schneier[15] argues that other parties, who have more capacity, should do more to protect individuals from e-security risks. He summed up his position by reference to his mother: "... She is not stupid; she is very intelligent, but this is not her area of expertise. If I tell her, 'You have to be responsible for your Internet security', she will not be able to. It is too technical, in ways she cannot deal with." [16]

Awareness raising initiatives sometimes underplay the reality of security risks and the difficulties involved in mitigating those risks. This is because some of those involved in awareness raising:

- Do not fully appreciate the complexity of the security threats and vulnerabilities themselves; and/or
- Are concerned that providing more accurate or detailed information will scare consumers off from participating in the online economy, which would be counter-productive to a range of other interests, including interests such as encouraging users to use online services to reduce business delivery costs.

The House of Lords report concluded that:

> The current emphasis of Government and policy-makers upon end user responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. It is time for Government to develop a more holistic understanding of the distributed responsibility for personal Internet security. This may well

15 Bruce Schneier is a well known US cyber security expert and has written several books on cryptography and cyber security issues more generally.

16 House of Lords, Personal Internet Security (page 55)

> require reduced adherence to the "end-to-end principle", in such a way as to reflect the reality of the mass market in Internet services [17]

Security awareness-raising is valuable and beneficial for many Internet users and the government is correct in providing resources to assist those users now[18] in the absence of better alternative policies/strategies. But for many others, it is not. As such governments need to step in to help those in other ways who cannot adequately protect themselves. We believe that ISPs, governments, software vendors, domain name registrars – all have a capacity to implement strategies to reduce the risk as outlined later in this submission.

By education, it is assumed to mean formal computer and information technology qualifications that enable IT professionals and practitioners to develop secure software, build secure web sites, mail servers, domain name servers etc. Universities report a significant drop in students enrolling in IT since the dot com crash, and courses have been reduced accordingly.

Similarly, most computer science/technology courses have very few dedicated security topics. Even then further professional development is most certainly required to achieve a level of proficiency necessary to understand and know how to mitigate common cyber attacks against public facing systems – web applications, web servers, database servers, mail servers, domain name servers, routers, firewalls, etc.

This situation has created a lack of competent IT professionals and in particular a lack of IT security professionals.

Many cases of attack described in this submission relate to the compromise of web sites and provides an indication that many business and government organisations have not implemented adequate levels of security. This may be due to lack of resources, lack of IT staff or adequate education/qualifications in cyber/IT security.

Anecdotal discussions with IT professionals shows there is an alarming lack of knowledge of malware capability or understanding of how security controls can be easily subverted. If this is the case for organisations that employ a team of IT staff, it is doubtful that small

---

17 UK House of Lords, Science and Technology Committee, *Personal Internet Security*, Volume I, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (2007), page 26

18 It does this primarily through its Stay Smart Online initiatives.

businesses, or those who provide computer after-sales services through such organisations computing retail stores, are likely to be suitably qualified to deal with the current and emerging range of threats facing consumer computers.

ii) Legislative and regulatory initiatives

Cybercrime legislation is adequate but is not a deterrent for perpetrators of cybercrime. It enables law enforcement to investigate and prosecute those within Australia who commit cybercrime.

Australia has not yet agreed to sign the Council of Europe Cybercrime Convention, which would provide greater assistance to Australian law enforcement for serious cases of cybercrime where overseas based law enforcement assistance was required. Most police officers complain that current cooperative arrangements for law enforcement assistance overseas is not practical or adequate when dealing with cybercrime due to the need to secure digital evidence in multiple foreign jurisdictions very quickly if the evidence is to be retained and to ensure the forensic quality of the evidence is preserved, ie not contaminated.

Within Australia there is a lack of regulatory initiatives designed to help prevent or mitigate the types of cyber crime AusCERT encounters and responds to on a daily basis. Significantly more could be done by the Australian government in this regard. Areas which could also be regulated include raising the bar on level of security of web sites in particular as they are commonly being compromised to serve malware to the public for illicit financial gain and identity theft.

"Self-regulation" exists among ISPs[19] and domain name registrars but can be problematic as potential conflicts of interest arise between taking action that is in the interests of the external community to what may be perceived to be detrimental to their own commercial interests. For example, domain name registrars could be more discerning and adhere to more stringent processes before registering domains designed to support criminal activity.

[19] ACMA is the telecommunications regulator for ISPs but has not provided any rules in relation to mitigating compromised hosts, which are used to actively attack third parties – hence most decisions made to act are voluntary, if they occur at all. Inadequate response lies mostly with the smaller or budget ISPs rather than larger ones.

The deregistration of domains used for fraudulent activity could also be substantially improved.

The APWG has provided a Best Practice Guide for Domain Name Registrar which if implemented by registrars around the world would help prevent some types of cyber crime.[20]

iii) Cross portfolio and inter-jurisdictional coordination

No comment.

iv) International co-operation

AusCERT has extensive experience seeking international cooperation to mitigate cyber attacks that have already occurred and are targeting Australian interests.

International cooperation among the 'self-help' security community by groups such as Shadowserver and Castlecops, the CERT community – particularly national or industry wide CERTs, and some proactive ISPs and security service providers around the globe is engaged on a daily basis to help identify new cyber attacks and work together, as required, to mitigate the attacks. This type of cooperation is useful and largely based on good will arrangements and is by no means a guaranteed or reliable approach to cyber attack mitigation but represents the principle area where cyber attack mitigation currently occurs.

Most of this activity, is ad hoc, based on good will alone and is not underpinned by any regulatory imperative. While some parties do provide rapid and effective response, there are many that do not – who are either slow to respond or refuse to provide assistance in the face of clear evidence of criminal activity. Therefore, often useful cooperation to resolve an ongoing attack is missing.

International cooperation on cybercrime for all parties is an area that could and should be improved, including and beyond law enforcement arrangements.

[20] http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf

e) Future initiatives that will further mitigate the e-security risks to Australian internet users; and

The House of Lords report concluded that:

> The current emphasis of Government and policy-makers upon end user responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. It is time for Government to develop a more holistic understanding of the distributed responsibility for personal Internet security. This may well require reduced adherence to the "end-to-end principle", in such a way as to reflect the reality of the mass market in Internet services. [21]

Recognising the merit in the House of Lords' view, the following initiatives seek to provide a more holistic approach and share greater responsibility for prevention, detection and response across various community stakeholders.

Short term

Goal to improve current attack mitigation

The faster an existing cyber attack can be stopped the less harm it does to potential victims and the more effort is required by criminals to obtain an attractive return on investment.

1. At the national level implement regulations which require ISPs to have counter-measures and processes in place, on notification, to help mitigate:
    - DDOS attacks
    - Restrict the activity of identified bot hosts used by their customers which are part of the ISP network address range (such as through walled gardens)

[21] UK House of Lords, Science and Technology Committee, *Personal Internet Security*, Volume I, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (2007), page 26

2. At the national level implement regulations which require web hosting companies to have counter-measures and processes in place, on notification, to take action:

    - To remove malware from legitimate web sites that have been compromised.

Goal to prevent cyber attacks from occurring

At the national level, implement regulations which require

1. any organisation hosting a commercial web site (as opposed to a web page) to adhere to web application security standards, such as those by OWASP.

2. any organisation hosting a commercial web site (as opposed to a web page on an pre-existing web site) to be certified by a qualified and competent third party and display a certification on their web site that it adheres to various security practices which makes their web site 'safe' from a consumer perspective to visit.

3. Any organisation hosting, developing or maintaining a commercial web site to use qualified IT security personnel – employed directly or outsourced and for that individual to demonstrate their qualifications through appropriate security certifications.

4. Any organisation or business found to breach these regulatory requirements to suffer stiff financial penalties and be required by law to take action to become compliant within a particular reasonable time frame.

5. Require Australian registries/registrars to follow a Code of Conduct adopting the APWG Best Practice Guide.

6. Require network level secure protocols to be implemented as broadly as possible by network owners in Australia and anyone operating under the .au ccTLD (eg, DNSSEC, IPSec, SBGP, etc).

7. At the national level provide financial incentives for students and universities to provide access to more IT security courses.

8. At the national level provide financial/tax incentives for employers and employees to undertake further professional development in areas of information security, network security, cyber security management and obtain relevant certifications etc.

In this market, there is nothing preventing any individual from setting up a computer repair business. Consumers have no ability to judge whether these businesses are

qualified or not. Knowing how malware has the ability to hide itself, AusCERT doubts whether many computer repair businesses understand the risks and are competent to detect and remove it. Computers are complex systems. Like cars, we can do a few basic things regularly to keep our cars in good shape, but if something goes wrong with it, most of us need to obtain professional assistance to fix it. Professional assistance should be sought from appropriately qualified people.

9. At the national level, ensure that anyone who sets up a business to 'repair computers' and 'remove malware' has received formal IT security training and certifications before doing so. Ensure that these certifications are displayed to enable consumers to have confidence that they are obtaining professional assistance.

10. At the national level provide financial/tax incentives for employers and employees to undertake further professional development in areas of information security, network security, cyber security management and obtain relevant certifications etc.

Medium term

11. Later, if the proposed regulations outlined in 1-4 above prove to be effective in reducing cyber attacks in Australia, extend arrangements to any public facing network systems such as routers, mail servers, domain name servers etc. It is recommended focusing on web sites and web applications primarily as they are very popular target for attack and have the greatest ability to exposing ordinary internet users to malware attacks.

12. Work with governments internationally to improve current levels of cooperation between CERTs, registrars and ISPs to mitigate identified attacks in progress in a more timely manner than current arrangements provide.

Long term

The following will be vital in the longer term but should be commenced now to ensure that action has occurred to allow the goal to be achieved in the long term, rather than waiting another 10 years and made no progress towards these goals:

The UK House of Lords reported made the observation that:

> *efforts to promote best practice are hampered by the current lack of commercial incentives for the [software] industry to make products secure: companies are all*

> *too easily able to dump risks onto consumers through licensing agreements, so avoiding paying the costs of insecurity. This must change.*
>
> *[...] a comprehensive framework of vendor liability and consumer protection should be introduced* [22]

David Rice[23] also advocates 'consumer protection'. However, liability is a negative incentive; fear of being sued as reason to provide better security may not always be effective in practice as it assumes the victims of attack have the financial resources to take civil action; this is often not the case; and many vendors may believe liability is not a serious a risk. Rice supports positive incentives, which are more likely to be adopted as ultimately they are likely to affect sales between competing products.

Rice proposes using 'consumer centric signalling' to provide strong incentives for software vendors to invest in developing more secure software. Recognising that producing more secure software is more expensive than producing software that provides the desired functionality but is insecure, there is currently no financial incentive for software vendors to invest seriously in security when many of their counterparts do not and can price a comparable product at a lower price. If software vendors that invested more effort to produce a more secure software product could signal that their product was more secure than their competitors, which justified the increased difference in price, then consumers could choose to buy the 'more expensive' more secure product or the cheaper insecure product.

To work, the scheme requires the government to create an equal playing field and regulate to require the software industry to display accurate labels about the security of their software for consumers in a similar way that the car industry is required to do so for car safety. It also requires the government to set up an independent body that is able to conduct software security assurance.

13. At the national level, implement regulation which requires software manufactures that sell products in Australia to display consumer labels that provide independent evaluation of the product's security, ie the ability of the product to protect itself from attack. (This is similar to the program used by car manufacturers through ANCAP, to provide consumer information about the car's crash safety, relative to other similar cars on the market).24

---

22 House of Lords, Personal Internet Security, page 41 and 42

23 Author of *Geekonomics – the real cost of insecure software*. See "Further reading"

24 http://www.ancap.com.au/

It should be noted that software assurance already occurs as part of the Common Criteria program but there is no requirement for products to undergo security assurance checking before being released to the market, nor is there any requirement for those that do to display the level of security assurance obtained in the marketing process.

Similarly, most of the products that are voluntarily submitted for evaluation to the CC do not achieve an evaluation better than EAL4, which for the purposes of reducing cyber crime is not sufficient. Any product that achieves EAL4 could not reasonably be considered a secure product in its ability to defend itself from attack. Hence, a lot more work needs to be done by software manufacturers to attain a software evaluation that allows consumers to have confidence that they are buying products that are relatively secure to deploy, ie are able to reliably defend themselves from attack. This applies to both operating systems manufacturers and application software, both proprietary and open source.

f) Emerging technologies to combat these risks.

In general, there are no emerging technologies, which in the foreseeable future (next five years), will address the breadth of these e-security risks adequately.

The vast majority of two factor authentication is capable of being attacked/subverted by malware. There is one form of two factor authentication which is worthwhile implementing where ever transaction integrity is the paramount security goal. Typically this would be applicable in financial transactions for online banking, online share trading etc. This is the EMV solution which allows for transactions to be digitally signed, off an untrusted device. The digitally signed hash function is created on a trusted device[25] and then manually copied to the untrusted client computer. The bank server then compares its transaction request details with those submitted by the client, verifies the digital hash and if the values are the same, then this provides verification that only the person with the smart card was able to have authorised the transaction.

This technology is currently being used in the UK by a number of banks.

[25] It is a simple smart card reader which looks much like a calculator with keypad and LCD display.

The value of this approach is that even if the untrusted client computer is fully compromised by malware, the malware cannot change the hash function without it being detected by the server as different and therefore probably fraudulent.

Note that the mere use of the EMV card technology does not provide absolute transaction integrity security. It depends on how it is implemented in relation to the web interfaces by banks and other financial providers. The key is to follow the recommended implementation and not deviate from that.

The EMV transaction signing facility provides a robust security solution for financial transaction integrity and authenticity but at present we do not believe it is necessarily required in Australia at present. While the Australian finance sector is willing to reimburse consumers with lost funds due to fraudulent online account transfers arising from malware compromise or phishing, it is not considered vital to deploy. If the risk for fraudulent online transactions is shifted to the consumer/account holder then there is merit in deploying it.

While the banks bear the losses they should have the ability to determine appropriate levels of security for their needs.

The EMV solution, however, does nothing to address the theft of personal identity information, where attacks on confidentiality occur. There is no technological solution for this when the client computer is compromised.

As such, due to the inability to rely on technology to provide security for the vast majority of attacks discussed in this paper, then non-technological approaches to achieving e-security will be vastly more important in the next 10 years, such as the holistic approaches described in paragraphs 1-13 above.

Recommended reading (listening) for further information about issues raised in this submission

AusCERT, *Managing Risk Associated with Online ID Theft for Government and Providers of e-Government Services*, http://www.auscert.org.au/5777 (2005)

AusCERT, *Haxdoor - Anatomy of an ID Theft Attack Using Malware,* http://www.auscert.org.au/7069 (2006)

OECD, *Malicious software (malware): a security threat to the Internet economy*, http://www.oecd.org/dataoecd/53/34/40724457.pdf (2008)

UK House of Lords, Science and Technology Committee, *Personal Internet Security*, Volume I, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (2007)

David Rice, *Geekonomics, The real cost of insecure software*. (2008)

See also: http://blog.geekonomicsbook.com/

Podcast: http://risky.biz/netcasts/auscert/rb2-auscert-podcast-david-rice-customer-centric-signalling

AusCERT, Submission to the Australian Law Reform Commission, Review of the Privacy Act 1988, http://www.auscert.org.au/8510 (2008)

AusCERT, Submission to Attorney-General's e-Security Review, http://www.auscert.org.au/9771 (2008)

AusCERT, *Home Users Computer Security Survey 2008*, http://www.auscert.org.au/usersurvey

AusCERT, Submission to .auDA, Review of the .au domain name policy framework, http://www.auscert.org.au/8396 (2007)

AusCERT, Submission to ASIC, Electronic Funds Code of Conduct Review, http://www.auscert.org.au/7536 (2007)

AusCERT, Submission to .auDA, Review of the structure and operation of the .au Internet domain, http://www.auscert.org.au/7019 (2006)

AusCERT, Submission to DCITA, Review of the e-Security National Agenda, http://www.auscert.org.au/7037 (2006) (confidential and public submissions)

AusCER Submission to ACMA, Review of the Spam Act 2003, http://www.auscert.org.au/6200 (2006)