



Review of Australian Government's e-Security Arrangements AusCERT Submission

Table of Contents

Background.....	3
Executive summary.....	3
Submission Terms of Reference	4
Limitations of current e-security policy.....	4
GovCERT.au.....	4
E-Security Policy and Coordination (ESPaC) Committee.....	6
What is the role and function of a national Computer Emergency Response Team?.....	10
How important is the national CERT function?	10
What models exist for national CERTs?.....	11
What roles, functions and services are provided by national CERTs?	12
What AusCERT does to fulfil and support its role as the national CERT.....	14
Risk of failing to fund AusCERT for its national CERT services/role.....	21
Why would it be difficult for the Australian government to quickly and readily develop a national CERT capability?.....	22
Advantages of retaining the national CERT role within UQ	24
AusCERT's current funding model	25
National Broadband Network and Next Generation Network.....	25
Roles and responsibilities of government, business, education sector and home users ..	27
Australian government.....	27
e-Government service providers	28
Business and government web site owners.....	28
Small business and home users.....	29
Recommendations.....	29
References.....	31

Background

1. The Attorney-General's Department, in conjunction with other Australian government agencies, is reviewing Australian government's e-security policy, programs and capabilities.¹
2. This submission outlines AusCERT's² views concerning the development of a new Australian government policy framework for e-security. Such a framework should address the interests of all users of Internet communications and technologies within Australia.
3. In making this submission, AusCERT has addressed particular aspects of the review's Terms of Reference.
4. AusCERT has prepared a confidential and public version of its submission. This is the public version.

Executive summary

5. AusCERT believes the government's current e-security policy and associated strategies do not adequately reduce the risk from the diverse, significant and rapidly increasing and evolving level of threats faced by users and participants of the information and digital economy in Australia. In this context "users and participants" refers to all critical and non-critical sectors, government, industry, business (all sizes), not-for-profit organisations and home users.
6. In particular, the current E-Security Policy and Coordination (ESPaC) Committee arrangements do not take advantage of the existing national CERT capabilities currently provided by AusCERT, which would help provide the needed integrated and coordinated approach to e-security for Australia. AusCERT's work as the national CERT needs be better coordinated and integrated with government arrangements and initiatives rather than isolated from them to provide a comprehensive and holistic e-security framework.
7. AusCERT is seeking sustainable funding for its role as the national CERT to contribute directly to a more effective and integrated approach to e-security in Australia.
8. It is well recognised by the Australian government and many other foreign governments that a national CERT/CSIRT is a key and vital national resource to help protect against, detect, respond and mitigate a range of e-security based threats

¹ <http://www.ag.gov.au/eseecurityreview>

² See pages 14 and 25 which provide more information about AusCERT.

affecting its online users be they government, industry or individuals. As such, it is logical that the Australian government fund AusCERT to perform this role and ensure the ongoing sustainability of this function. This investment in the national CERT capability will also allow AusCERT to continue to adapt and meet the needs of a constantly changing cyber threat environment.

Submission Terms of Reference

9. It is noted that the main purpose of the review is to:

Develop a new Australian Government policy framework for e-security, covering the span of e-security issues across government, business and the community.

10. In relation to the following terms of reference items:

a) those being implemented by agencies under the E-Security National Agenda

b) incident response and crisis management arrangements for e-security, including the recommendations from Australia's participation in Exercise Cyber Storm II.

11. AusCERT agrees that there is a pressing need to address these limitations and significantly strengthen the government's policy objectives and help improve ICT security for users and participants of the Australian digital and information economy through a new integrated e-security framework across government, business and the general community. The main approach AusCERT is advocating is the support of the national CERT function and services which would enable them to be broadened and better leveraged by government (local, state and federal), business and the community.

Limitations of current e-security policy

GovCERT.au

12. GovCERT.au states that it is responsible for:

a) liaising with Computer Emergency Response Teams from foreign governments

- b) *coordinating enquiries from foreign governments about cyber-security issues that affect Australia's critical infrastructure **and business sector***
 - c) *coordinating the Australian Government's policy on how to prepare for, respond to, and recover from computer emergencies affecting the national information infrastructure.*³
13. There is clearly an overlap between AusCERT's contacts and those of GovCERT.au and the similarities in the two organisations' names create the impression that GovCERT.au has a CERT/CSIRT role with related capabilities that are similar to those provided by AusCERT. Traditionally, operational CERT organisations such as AusCERT provide:
- a) Monitoring, analysing and providing advice to the community (including business, government and home users) on common cyber threats and vulnerabilities;
 - b) incident response for Australian organisations or users for attacks sourced abroad and/or from attacks sourced from within Australian that target parties overseas. In this case, AusCERT responds to specific incident requests from third parties.
 - c) capability for detecting, analysing, responding to and mitigating the impact of broad-based internet attacks affecting large sections of the Australian internet using community. In this case, AusCERT proactively seeks to detect compromises or vulnerabilities in public facing systems (such as web applications or domain name servers) which are vulnerable to attacks that could facilitate widespread exploitation of Australian computers.
14. The international CERT community is a diverse group of private and public entities. The members range from vendors, universities, businesses (such as banks), Internet and telecommunication providers such as ISPs and domain name registries, to security vendors such as anti-virus companies with an increasing number of national CERTs. Contacts and assistance arrangements in the CERT/CSIRT community are fundamentally reciprocal. In the 15 years of its operation AusCERT has established a credible reputation as a leader in the global CERT community which is widely respected and trusted. This puts AusCERT into an enviable position of being a national CERT that can both be contacted for assistance, be trusted to share information with, and worthy of a response when requesting help.

³ <http://www.ag.gov.au/govcert>
[http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(CFD7369FCAE9B8F32F341DBE097801FF\)-t000Fact+sheet+-+GovCERTau+-+October+2007.PDF/\\$file/t000Fact+sheet+-+GovCERTau+-+October+2007.PDF](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)-t000Fact+sheet+-+GovCERTau+-+October+2007.PDF/$file/t000Fact+sheet+-+GovCERTau+-+October+2007.PDF)

Recommendation

- R1 The new e-security framework should formally recognise the status, role and function of the national CERT including the key aspect of acting as a single Point of Contact (POC) for Australia in the global IT community (as was intended by creation of the national CERT function within AusCERT) and more clearly defined set of complementary roles for AusCERT and GovCERT.au. Through its national coordination role, AusCERT can then triage information and redirect or call upon the participation of GovCERT.au as appropriate. This would be wholly consistent with the existing MOU between AusCERT and the Australian Government.*
15. With regard to 13(c) above, AusCERT plays a significant and vital role in helping respond to a variety of cyber attacks affecting the Australian digital and information economy. In seeking to protect the CII and help the CII better protect itself, it is counter-intuitive for the Australian government to not draw directly upon AusCERT's unique knowledge and experience in mitigating cyber attacks and the threat environment where they may impact/affect the CII along with the rest of the Australian digital and information economy.
16. The primary Australian Government operational framework for dealing with cyber threats and vulnerabilities is the Joint Operating Arrangements (JOAs). Although AusCERT is recognised as the national CERT for Australia, AusCERT, as a non government entity is not currently involved or included in the JOAs. This situation is in stark contrast with other national CERTs which are directly involved in national frameworks, particularly at the operational level, where the technical knowledge, and understanding and experience of the CERT is regarded as being essential. It would seem prudent that the Australian Government integrate the national CERT into these existing Joint Operating Arrangements as part of its development of a new integrated national framework for information security.

Recommendation

- R2 As part of the government's framework to protect the CII, AusCERT should be formally identified within the framework as a source of reliable and unique expertise about cyber threats and vulnerabilities affecting the Australian information and digital economy, including the CII.*
- R3 As part of the government's framework to protect the CII, AusCERT as the national CERT should be included in the JOAs.*

E-Security Policy and Coordination (ESPaC) Committee

17. The current e-security policy divides focus and resourcing among protecting Australia's critical information infrastructure and general users/participants in the

online economy,⁴ such as business, government, non-profit organisations and home Internet users. But the government's approach to non-critical interests is generally recognised as fragmented and lacking coordination.

18. A consequence of this is that government funding, resources and strategies are not comprehensively and systematically applied for the benefit of large sections of the Australian digital/information economy. Nor do large sections of the Australian information/digital economy have access to adequate resources, expertise or support to help them prevent, detect or mitigate a range of threats they are likely to face as participants in the online economy.

19. Similar concerns were noted in the previous 2006 e-security national agenda review:

*The Review found that the whole-of-government arrangements needed to reflect the changes in the e-security environment and support an integrated approach to address e-security issues across the Australian economy.*⁵

20. The reality is that many cyber and online threats and vulnerabilities in the public domain affect both critical and non-critical sectors in common ways that can be harmful to the interests of both, albeit with different risks or consequences. This view is given weight by the government's own position in this regard:

The Government recognises that the security of each of these sectors is often influenced, both positively and negatively, by the policies and practices of the others. In recognition of these inter-dependencies, the framework will acknowledge the differing role that the Government has in supporting each sector.

21. To address this, the government established:

A new whole-of-government interdepartmental committee, the E-Security Policy and Coordination (ESPaC) Committee, will be established to coordinate e-security policy throughout the Australian Government. The Attorney-General's Department will chair the committee, and its membership will be comprised of representatives from the following Australian Government agencies:

- *Australian Communications and Media Authority*

⁴ It is not appropriate to label the general users/participants in the online economy as non-critical when collectively they represent a significant proportion of the online economy. General users/participants include ordinary home users, e-commerce business providers, educational institutions, e-government providers and any business or entity which uses online services, such as the web, email. Without the involvement and participation of these general users

⁵ http://www.dbcde.gov.au/__data/assets/pdf_file/0011/71201/ESNA_Public_Policy_Statement.pdf

- *Australian Government Information Management Office*
- *Australian Federal Police*
- *Attorney-General's Department*
- *Australian Security Intelligence Organisation*
- *Department of Communications, IT and the Arts (now the Department of Broadband, Communications and the Digital Economy)*
- *Defence Signals Directorate*
- *Department of Defence*
- *Department of Prime Minister and Cabinet, and*
- *Office of National Assessments.*⁶

22. However, the current approach does not fully or effectively provide an integrated approach to address e-security issues across the whole Australian economy and does not foster or allow the participation of the private sector in the arrangements to “address e-security issues across the Australian economy”.
23. There is advantage to be gained in monitoring threats and vulnerabilities in the public domain which can affect and harm both sectors. AusCERT currently provides significant monitoring of computer and online vulnerabilities and threats. This is not widely available to both the critical and non-critical (but largest part) of the Australian digital and information economy because much of this is limited to AusCERT subscribers on a fee-for-service basis.⁷ Ideally, if this function was government funded, it could be made available to all Australian organisations who would benefit from it. The reality is that many organisations will not pay for security advice or services, no matter how reasonably priced. Like many other public services, these basic services would be of significant benefit to the Australian community if made available in a centrally funded manner for participants in the digital economy.
29. The main area where the current policy fails is that the ESPaC operates without an overarching or e-security framework or plan that involves, incorporates or acknowledges AusCERT's contribution, expertise and role as Australia's national CERT even though:
- a) AusCERT is recognised as the national CERT by the Australian government;
 - b) there is an expectation by government that AusCERT provides certain services in this regard (without government funding);⁸

⁶ Ibid.

⁷ This service is distinct and different in substance from the free Stay Smart Online Alert Service. The latter is designed for home users and SMEs with very low technical comprehension. This limits the range of advice that can be usefully applied by this group.

⁸ See MOU between AusCERT (University of Queensland) and the Attorney-General's Department (The Commonwealth), dated 24 May 2006

- c) it was recognised by the government in 2003 that “as a national CERT, AusCERT has a critical role to play in NII protection arrangements as the central point for collection and dissemination of threat and vulnerability advice in Australia;”⁹
 - d) AusCERT contributes substantial resources and expertise to the national CERT role and in doing so is actively minimising risk to users and participants in the Australian digital and information economy by the preventing, detecting and responding to cyber security threats and vulnerabilities affecting Australian interests.
30. The best approach is one that integrates across the whole of the digital economy and draws upon all available expertise, experience and strategies for preventing, responding to and mitigating cyber attacks.
31. For further details of the services and functions undertaken by AusCERT as the national CERT see page 14.

Recommendation

- R4 To develop a more effective and integrated national approach to e-security for all interests (critical and non-critical, business, government and home users) within the Australian information and digital economy, the new policy framework should recognise and articulate the role of AusCERT as the national CERT and, together with GovCERT.au, clearly delineate complementary roles and functions.*

In doing so, it should be recognised that AusCERT has a long standing history and reputation of helping to protect Internet security in Australia and, through its actions here, abroad. As such it would be counter-productive to pursue the government’s e-security policy goals without better utilising, in a coordinated manner, the services, expertise and capability provided by AusCERT.

The best way to achieve the latter is through a formal integration of AusCERT into a truly national e-security framework including a funding relationship which binds funding to fulfilling particular role/functions and achieving outcomes.

The ESPaC would benefit from substantial involvement by AusCERT and it is difficult to see how it could operate effectively without such involvement.

⁹ Attorney-General’s Department, CIP Newsletter, Volume 1, No. 1, November 2003, Available at: [https://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/\(930C12A9101F61D43493D44C70E84EAA\)~Vol+1+No+1.pdf/\\$file/Vol+1+No+1.pdf](https://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~Vol+1+No+1.pdf/$file/Vol+1+No+1.pdf)

What is the role and function of a national Computer Emergency Response Team?

32. In making a case for government funding of the national CERT role provided by AusCERT, it is useful to clarify what is the national CERT role and how an effectively resourced and experienced national CERT is a vital part of each country's cyber security plan.

How important is the national CERT function?

33. For a number of years international government forums, such as the OECD, APEC Tel and more recently the ITU,¹⁰ and others¹¹ have recognised the importance of the national CERT (also known as national CSIRT – computer security incident response team) function as a vital component to improve national and international cyber-security arrangements. These forums, which include the Australian government, have promoted national CERT development and deployment.^{12 13 14}
34. At last count there are 38 national CERTs,¹⁵ including AusCERT.¹⁶

Case study

In some countries such as the UK, there is no clear national CERT. There is only a government CERT function, such as GovCertUK¹⁷ and various specific industry-sector CERTs. .

This has been identified as a serious concern by groups in the UK such as APACS¹⁸ (UK Association for Payments and Clearing Services) with whom AusCERT works closely. Since 2003, AusCERT has provided substantial assistance to UK financial institutions, via APACS, for cyber attacks targeting UK banking customers and hence impacting UK banks, until these organisations were able to develop their own capacity in this regard, in the absence of any UK national CERT or equivalent.

¹⁰ <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf>

¹¹ <http://www.state.gov/t/pm/rls/othr/misc/78657.htm>

¹² <http://www.oecd.org/dataoecd/53/34/40724457.pdf>, page 52

¹³ <http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/itu-summary-and-wrap-up-brisbane-july-08.pdf>, page 3

¹⁴ APEC Project TEL01/2006 – Strengthening Effective Response Capabilities among APEC Member Economies - Final Report, May 2008, available: www.apec.org

¹⁵ *Ibid*, page 50

¹⁶ <http://www.cert.org/csirts/national/contact.html>

¹⁷ http://www.govcertuk.gov.uk/about_us.shtml

¹⁸ APACS oral submission to House of Lords Paper on “Internet Security”, <http://www.parliament.the-stationery-office.co.uk/pa/ld200708/ldselect/ldsctech/131/131we03.htm>

This example is provided to demonstrate that the role is important and a government focused CERT alone is not enough to address current threats/vulnerabilities affecting our respective information/digital economies in general.

What models exist for national CERTs?

35. With the exception of AusCERT, generally national CERTs are government funded entities, but they are not always government employees or government agencies. Many support a level of independence from government, which some argue, when dealing with many industry groups (as national CERTs frequently do), is likely to result in increased trust, including when dealing with other government funded CERTs. Regrettably some industry groups are distrustful of government and some government CERTs are distrustful of some foreign governments, including government CERTs.
36. In Malaysia, MyCERT, is the national CERT and part of a Malaysian government business enterprise called Cyber Security Malaysia. In the USA, US-CERT is the national CERT but a large part of US-CERT's technical capability and services is provided by CERT/CC which is based at Carnegie Mellon University in Pittsburgh with US government funding.
37. In Brazil, the national CERT, CERT.br, is centrally funded by the Brazilian government from the proceeds of domain registration and other Internet delivery revenues as a service to the Internet community of Brazil. Governance for CERT.br is overseen by a board comprising government, industry (general and telecommunications) and academic representatives. The choice of this governance model was a reflection of the government's desire to ensure CERT.br was independent and perceived to be independent and able to respond in the best interests of the whole Brazilian digital economy. CERT.br is a mature CERT in terms of its experience, capability and contribution to Internet security within Brazil and highly regarded by the international national CERT community.
38. The national CERT function does not need to be housed within any government agency. In fact, many overseas governments, such as Japan and Malaysia have gone to significant lengths to establish their national CERTs as fully funded government enterprises. This approach allows the government to retain oversight and control over the activities of the national CERT consistent with the policy outcomes and objectives it wishes to achieve. Such control and oversight is not possible without formalising the relationship between the national CERT and government through adequate funding arrangements. However, it is important that such arrangements are put into place without reducing the flexibility and speed of independent action that is critical to successful CERT operation.

Recommendation

R5 *AusCERT supports funding by government of its national CERT role, as part of a new e-security framework, while allowing AusCERT to conduct other services on a fee-for-service basis and remaining part of the University of Queensland.*

What roles, functions and services are provided by national CERTs?

39. While the concept and requirement to establish a national CERT/CSIRT has been broadly recognised and accepted, there is currently no authoritative list of agreed national CERT functions and services. While national CERTs can and do conduct a variety of services and programs to help reduce e-security risks within their country (jurisdiction) there are generally three primary roles that are common among all national CERTs. These are:

- a) Situational awareness – monitoring and analysing computer network threats (attacks) and vulnerabilities for the national CERT's constituents. In AusCERT's case this is for anything that affects the .au namespace and Australian organisations using gTLDs;¹⁹
- b) Incident response by providing assistance to networks facing cyber attack sourced from within the national CERT's country or, more often, outside their own country jurisdiction. Such assistance generally involves a range of potential actions designed to stop a current attack and/or minimise harm arising from the attack such as:
 - i. requesting action from ISPs or domain registrars and/or CERTs in relation to attacking hosts and/or compromised hosts;
 - ii. analysing malware to identify related web based attack sources and taking action against each one as per (i) above;
 - iii. submitting malware to anti-virus vendors to develop new signatures to mitigate a current cyber attack;
 - iv. analysing malware to understand functionality and capability of the attack for threat assessment and attack mitigation/recovery purposes; and/or
 - v. requesting log data from affected servers.
- c) Providing advice in various forms – security bulletins, papers, media comments, government submissions, participation in government and law enforcement meetings, presentations, awareness raising programs – based on AusCERT's specific knowledge of the threats and vulnerabilities. Coupled with information relating to incident response, the national CERT is uniquely placed to analyse

¹⁹ This includes Australian entities that use generic Top Level Domains (gTLDs).

these incidents and to provide practical advice to the community. This can be done on a one to one basis or on a one to many basis in the form of alerts, advisories and assessments.

40. In outlining the roles and functions of the national CERT, it is not enough to simply describe the type of services it provides. Rather, the national CERT as a national resource and centre of expertise into cyber attacks and vulnerabilities, should have the following characteristics:
- a) Be generally available and responsive to enquiries made by the Internet-using community and provide public resources to assist them further, within certain guidelines;
 - b) Provide assistance where it is not readily possible for an organisation or entity to assist themselves in relation to a cyber attack, ie is unlikely to have the resources or skill level to do so;
 - c) Provide assistance where it is not readily possible for an organisation or entity to assist themselves because they need to rely on unknown parties (such as domain registrars, ISPs or other organisations) to help mitigate the attack;
 - d) Provide assistance in response to an attack on an Australian-based entity where the attack is likely to result in further harm to many more people and their systems who otherwise are not able to readily prevent the attack. (For example, a web site belonging to a legitimate well-known Australian brand that has been compromised and is serving malware to unwitting members of the public that connect to the site);
 - e) The agility, backed with the technical capability, to respond in 'Internet time' to evolving threats, vulnerabilities and broader changes on the Internet generally.
41. In developing a national cyber-security framework, it should be noted that the combination of these three primary roles consumes considerable resources; and in the case of the latter, require staff to be on-call after hours for emergencies.
42. Given, the level of cyber attack activity and vulnerabilities present, it is also necessary to develop tools and systems that automate the detection, response and mitigation processes.
43. CERT/CC²⁰ and ITU²¹ have resources available that provide guidance on the national CERT function and services. AusCERT also provides CERT training including for building national CERT capabilities.

²⁰

<http://www.cert.org/csirts/national/>

What AusCERT does to fulfil and support its role as the national CERT

44. The national CERT has a role to play in helping users and participants of all sectors of the information economy prevent, detect and respond to cyber security issues to help reduce e-security risks that, without the assistance of the national CERT, would be difficult for them to do themselves.
45. In this regard AusCERT devotes considerable resources and expertise to the following activities and functions which provide broad based benefit to Australia's e-security interests:
- a) *monitors, analyses and provides advice in relation to ICT and in particular Internet based threats and vulnerabilities;
 - b) *proactively detects and helps Australian organisations mitigate Internet based attacks for their direct benefit and for the benefit of the broader Internet using community who also have the potential to be affected by the attack/vulnerability;
 - c) *provides a single point of contact (POC) for Australian entities, overseas CERTs (and other parties) to report and gain assistance to stop attacks sourced from and targeted to Australian systems;
 - d) *provides assistance to Australian law enforcement – state and federal, including technical support for investigations;
 - e) *participates in government meetings nationally and internationally relating to cyber security at the request of government;
 - f) *provides information sharing infrastructure (such as mailing lists) and information to various closed and trusted industry groups in order to share new threat/attack information and/or facilitate greater response capability among participants of these various groups;
 - g) *participates in CERT related events nationally and internationally to build and maintain important CERT relationships;
 - h) *actively contributes to government planning and preparations for serious, large scale cyber security incidents, such as CyberStorm as well as smaller exercise events with other CERT counterparts such as APCERT;

²¹ <http://www.cert.org/csirts/services.html>
<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf>
<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>

- i) *in conjunction with other CERTs, develops policies and procedures to facilitate greater efficiencies and cooperation between national CERTs. For example, involvement with APCERT;
- j) *provides 'clean' data feeds vendors for inclusion in anti-phishing tool bars to mitigate attacks prior to their removal;
- k) *provides malware to anti-virus vendors to enable them to update signature files; Prior to sending to a trusted list of security contacts, AusCERT tests the malware to determine the level of detection and potential impact.²²
- l) *writes papers and assessments on common forms of cyber attack threats and vulnerabilities and their impact on victims²³ to help policy makers and industry develop appropriate strategies to better mitigate the risks;
- m) *contributes to public awareness raising campaigns about cyber security through the provision of publications, resource materials, surveys and presentations; and
- n) through its submissions to government and industry regulators, advocates the adoption of specific strategies to help cyber security based on AusCERT's experience monitoring and responding to cyber threats and vulnerabilities for the benefit of all participants/users of the information economy within Australia.

AusCERT statistics on its handling of incidents to mitigate threats and vulnerabilities as part of its national CERT role

46. In order to better gauge the extent, volume and value of the work that AusCERT does as part of its national CERT role, we have provided some figures. These figures demonstrate a number of points worth noting:
- a) The online cyber threat environment is active and aggressive – there is no shortage of Internet based attacks targeting Australian interests from criminals (interested in illicit financial gain) and other elements and vulnerable systems are being quickly exploited. The need for a national CERT function within Australia (as in other countries) to deal with the range of threats and vulnerabilities in the online environment is undisputed and is acknowledged by various government and international government forums;

²² Only malware with a low detection rate and high impact is provided by AusCERT. This makes AusCERT a high value source which has high priority within the AV community.

²³ This also includes contributing substantial content and expertise to the OECD's paper, *Malicious Software (Malware) – A Security Threat to the Internet Economy*, to ensure that the paper accurately represented the severity and complex technical aspects of the threat for the benefit of policy makers. <http://www.oecd.org/dataoecd/53/34/40724457.pdf>

- b) AusCERT's contribution to detecting, responding and mitigating threats and vulnerabilities for the benefit of the Australian information and digital economy is substantial. A large part of this assistance is proactive, as a result of reports received by third parties or through AusCERT's own monitoring activities. In almost all cases, until AusCERT has contacted the affected parties, the compromises were not known to them. AusCERT's established name, role and reputation backed up by sound technical expertise is often a major reason why affected third parties respond positively and agree to fix their systems.
- c) Without AusCERT's assistance in mitigating these attacks, it is safe to estimate that many thousands of victims would remain compromised and many more would be compromised. 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. Without AusCERT's assistance to notify and help affected parties recover and mitigate further harm, 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.
- d) The figures demonstrate that sometimes efforts to prevent cyber attacks fail. Whether prevention fails due to ignorance, negligence, lack of resources and capabilities or through the sophistication of the attack vectors, a cyber security response capability that provides early detection, mitigation and recovery assistance is vital to help recovery and allow all parties to continue to use, participate and benefit from the online information and digital economies. Hence AusCERT's activities in providing substantial levels of incident response for the benefit of users and participants in the information/digital economy as part of its national CERT role, should be included as part of the government's new e-security framework including under the terms of reference:

incident response and crisis management arrangements for e-security, including the recommendations from Australia's participation in Exercise Cyber Storm II, and

- e) A national cyber incident response capability is needed to address the daily high level of cyber attacks targeting the Australian information/digital economy, just as much as it is needed for less common, more serious and widespread cyber attacks, such as that which Cyber Storm is helping to prepare for. Failing to take action to mitigate the more commonplace (but still harmful) cyber attacks of the type that AusCERT currently responds to on a daily basis, increases the chances of a more serious widespread, concerted cyber attack against Australian interests. Notably, AusCERT has been heavily involved in the CyberStorm

exercises to date, providing specialist advice in the planning, execution and review phases of the exercises.

Recommendation

R6 AusCERT recommends these services be funded by the Australian government to provide an integrated approach to cyber security accessible by all users/participants in the digital information economy.*

Funding the national CERT role, and incorporating the functions as part of a new e-security framework will allow the government to better monitor the threat environment and evaluate response preparedness capabilities and mitigation strategies that make up part of the e-security framework.

With dedicated government funding, there is also scope to improve and augment these services further in line with international expectations and the changing threat environment.

47. The *AusCERT Home Users Computer Security Survey 2008* provides an example of the type of data that can be captured from a compromised computer and its associated impact on the individuals concerned.²⁴

48. In this regard, under the following terms of reference :

Examine current programs, arrangements and agency capabilities and capacities that contribute to e-security, including [...] relevant information and communications technologies (ICT) initiatives being undertaken by the Commonwealth and by state and territory governments to establish their suitability and effectiveness to achieve the policy objectives of the new Framework.

it should be noted that the various local, state and federal e-government programs, including the various important state and federal e-health programs need to take into consideration prevention and response mitigation to address these types of threats which is impacting on the security of e-government service delivery and the privacy of Australian citizens. AusCERT has identified threats to e-government services since 2005²⁵ and again more recently.²⁶

Notification of compromised computers and web sites with exploitable vulnerabilities

²⁴ <http://www.auscert.org.au/usersurvey>, page 25

²⁵ Managing Risk Associated with Online ID Theft for Government and Providers of e-Government Services, <https://www.auscert.org.au/5777>

²⁶ Submission to the Privacy Act review, <https://www.auscert.org.au/8510>

49. Through a range of trusted sources within the information security community, AusCERT receives feeds of data providing information about compromised hosts (clients and servers)²⁷ within Australia. AusCERT supplements this feed by using a number of its own purpose-built tools to detect compromised web servers in Australia. The following figures also include cases where AusCERT has identified web sites within Australian with easily exploitable vulnerabilities.
50. Consistent with global trends, it is important to note that in the last 18 months the number of legitimate web sites that have been compromised and are also serving malware to the public have increased substantially and a high proportion of these cases include compromised Australian web sites and client computers²⁸ that are serving malware to members of the public (including customers and clients of the business or entity) that connects to the infected web site.
51. The following figures represent the number of notification messages AusCERT sent relating to compromised client and server computers, including web servers serving malware or web servers with easy to exploit vulnerabilities, each year since 2005. Typically each message contains information about at least one compromised host.

Year	2005	2006	2007	2008	Projected end of 2008
Notifications	404	1,488	1,864	1,515	2,508

52. These include the web sites of popular well-known Australian brands that have been compromised for the purposes of serving malware to the public. Sometimes, federal, state and local government web sites have also been detected serving malware to unsuspecting members of the public. Hence it is not a problem isolated to small business with lack of staff or resources to address the problem.
53. In all cases, but especially when a web site is serving malware to the public, timely detection and mitigation is critical to help prevent further harm being done to potentially thousands of new unwitting victims. Currently the only way to do this is by contacting the relevant web site owner and seeking their assistance to fix the affected web site.
54. Often the malware being served is of the type that logs captured password and other sensitive data outlined in the previous example.

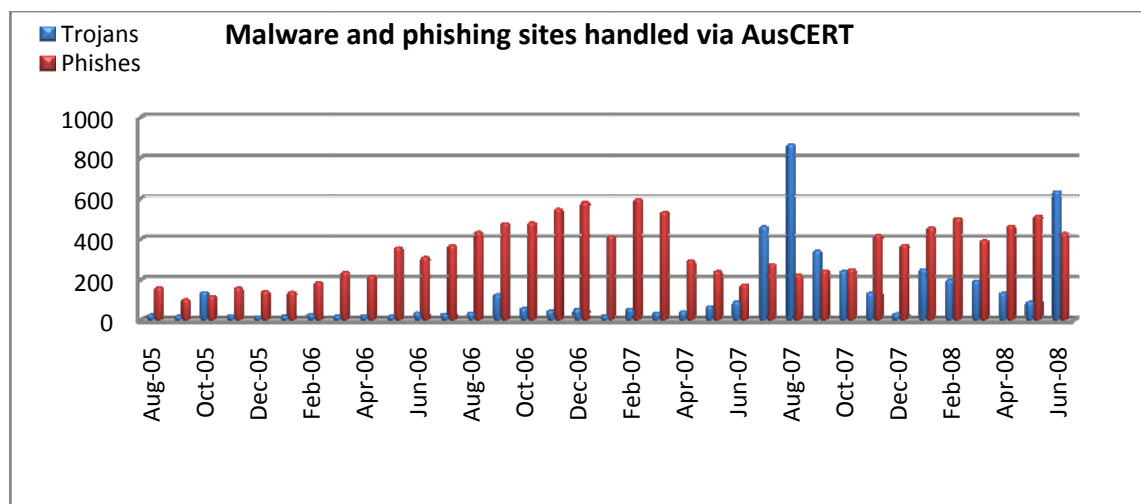
²⁷ If it is a client host, AusCERT will pass the information to the relevant Australian ISP, if it is a server then there is usually a contact for the web site which can be contacted directly. In the case of advice to ISPs, it is sometimes the case that a single message will relate to multiple compromised hosts belonging to various customers of the ISP.

²⁸ Client computers that serve malware, typically include storm worm infected hosts.

55. Once a new compromised web site is detected serving malware, AusCERT monitors the web site to ensure that the malware is removed. Unfortunately some owners of private and government sector web sites that serve malware are not always quick to take action and remove the infection. The same delays have been noted in those cases with known cross-site scripting vulnerabilities. The reality is that if AusCERT is able to find these vulnerabilities, so too can criminals and their presence allows attackers to use vulnerable web sites to facilitate attacks launched via the web site.
56. More recently, AusCERT has established a pilot project which is providing its list of malware hosting servers in a data feed to trusted network contacts. Many large networks pass Internet traffic through a central gateway and are able to use the AusCERT feed at the gateway to block internal access to these sites. This feed has also shown itself to be a valuable means of locating compromised internal hosts (ie have been logged as connecting to the malware server. The details of the malware infection and the time and date of likely infection is also seen as valuable information for network owners who are seeking to undertake damage assessments resulting from the malware infection. This pilot approach developed by AusCERT is yet another good example of practical and effective mitigation strategies that can reduce the exposure and impact of malware related attacks and add value to the role of the national CERT.

Phishing and malware sites

57. Since 2003, AusCERT has responded and provided assistance to a range of organisations to help remove phishing sites designed to steal access credentials or personal information or funds from their customers. As the volume of attacks has increased beyond levels able to be handled by AusCERT, financial institutions have increasingly relied on other third parties to help mitigate phishing attacks. AusCERT continues to provide triage assistance, when normal channels fail or for small institutions that don't have the resources to respond themselves. Phishing attacks target a range of other entities including universities, government agencies, ISPs and other e-commerce entities.
58. For malware sites targeting Australian users, AusCERT takes a range of mitigation action, ranging from site closure (either via ISP or domain registrar), malware analysis, submission of URLs and malware samples to vendors,.



59. Each site represents a single unique URL or domain name that is hosted by one or more compromised computers for the purpose of stealing sensitive information and access credentials from other computers. Multiple sites can be associated with each attack, which is the set of compromised computers needed to launch the attack and collect the stolen data. The number of IP addresses associated in a single incident and a single attack is variable but can range from 1 to over 5,000.
60. This graph does not include specific compromised hosts involved in any single attack or incident - only URLs and domain names. Nor does this depict the number of computer infections (compromised hosts) that occur arising each malware attack of which there is generally many hundreds or thousands.
61. In recent years with the explosive growth of Internet related cybercrime, many national and government CERTs are investing significant funds towards ways to detect and respond to the increasing level of malicious activity. While AusCERT has demonstrated its ability to respond quickly with creative and innovative approaches, this is no long term substitute for a properly funded and comprehensive research and development program. At present, despite AusCERT's considerable efforts, Australia is still lacking the fundamental capabilities and processes to detect compromises of Australian, including government web sites serving malware to the public, and the ability to respond quickly to notifications of this nature.

Recommendation

- R7 Adequate government funding for the national CERT role would also allow AusCERT to upgrade many of its internal systems and processes to provide better granularity of the nature of cyber attacks AusCERT handles affecting Australian information/digital economy to allow better e-security planning, threat analysis and mitigation to occur.*

Risk of failing to fund AusCERT for its national CERT services/role

62. Given the case in support of Australia continuing to have a national CERT as a vital component of any country's cyber security framework, the related issues that need to be considered by the Australian government in this review are whether to:
- a) Keep the status quo and hope that AusCERT can continue to support its national CERT function on the presumption that it can continue to generate sufficient and increasing funds;
 - b) Fund AusCERT to do the national CERT work as it is currently doing or with small modifications on how it is done, including governance control issues; or
 - c) Provide funding to the government itself to do it instead, for example through GovCERT.au.
63. Option (a) carries considerable risks for the government and the broader digital economy. It cannot guarantee the University of Queensland will always be willing to take on this function even though it does not currently consume direct cash funds doing so. Nor can the government guarantee that the revenue AusCERT is able to generate through its commercial offerings will be sustainable and/or be sufficient to cover the increasing costs of providing an effective national CERT role in the medium to long term. There are a number of factors which erode the funds available to AusCERT to cover these services,
64. Similarly, as the threat environment continues to worsen and the cost of responding escalates, it is not certain that AusCERT can continue to generate sufficient revenue to fund the national CERT function. Already AusCERT has had to adapt on many occasions by developing new tools and processes to handle the workloads and new requirements which are becoming increasingly complex and expensive. Without adequate and sustainable ongoing funding, it is entirely possible the national CERT services being supplied by AusCERT will erode to the detriment of Australia's information/digital economy.
65. To allow the status quo to continue, particularly in light of the current threat environment and the increasing costs and demands, is a risky option for the maintenance of the national CERT. Many factors that can influence the status quo are beyond the direct control of the government and the University of Queensland. Ultimately, is the Australian government prepared to accept this level of risk which is actually increasing over time?
66. Option (c) also carries some risk for the government in terms of whether it is feasible or even possible for the government to develop an equivalent capability within an acceptable timeframe. Given AusCERT's development and expansion of the national CERT role over many years, we do not believe it is possible to achieve this outcome

without significant damage to the role and without a prolonged break in continuity and effectiveness. AusCERT's preferred outcome is the adoption of option (b), with the resulting action being to fund AusCERT to enable it continue to undertake the national CERT role.

67. In support of option (b), AusCERT has provided significant evidence in this submission to show that it is providing considerable resources, expertise, experience and dedication to support its national CERT role and for all accounts receives positive feedback for the assistance we provide – not only to directly affected parties but more generally, in terms of some of the other awareness raising and intelligence sharing work we are involved with. It is important not just to have an operational role but to share with others what is learnt about cyber attacks, threats, vulnerabilities and mitigation in order to deal with the cyber threats more effectively.

Why would it be difficult for the Australian government to quickly and readily develop a national CERT capability?

68. In proceeding with option (c) there are a number of reasons why this cannot readily be achieved by a simple increase in government funding.
69. The vast majority of users and participants of the information and digital economy are in the private sector. When working at the operational level in providing incident response assistance and advice and notifying them of compromises to their systems, it is generally accepted as being better for them to have an independent trusted party that is one-step removed from government.
70. It would be a costly exercise and would take the government at least two to three years to build a basic national CERT capability. It would also be difficult for the government to recruit and attract sufficient numbers of experienced staff at a time when there is a severe skills shortage in IT skills and in particular IT security. The absence of an effective national CERT role for the period of establishment of a new national CERT would seriously degrade the security of the Australian information and digital economy for this period.
71. AusCERT has 15 years experience and developed contacts off shore with ISPs, domain registrars, anti-virus vendors, major product vendors and many closed professional security groups (associated with large ISPs internationally and other bodies – not necessarily available to governments), which are able to provide practical incident response assistance and expertise in analysing malware and other security incidents to augment AusCERT's own capabilities. Such reach is vital to respond quickly and globally to numerous and varied online threats affecting Australian interests.

72. It is not in itself enough for a national CERT to have a range of useful contacts but it must have developed a level of trust and confidence with these contacts. This is also based on the ability to provide reciprocal benefits to these contacts in either the sharing of information, methodologies and approaches or responding to requests for advice and assistance. This would take a considerable period of time for the Australian government to build this network of contacts from scratch, particularly as a replacement for AusCERT.
73. In keeping with its earned trust relationships, AusCERT has developed and facilitated a number of online forums for sharing tactical and technical cyber attack threat intelligence with various industry groups such as the education sector and finance sector. In some cases, this exchange has occurred with industry groups in other countries. These information sharing arrangements have benefited AusCERT's ability to provide effective response within Australia and helped Australian industry to better help themselves; and in turn AusCERT has contributed value to these information sharing arrangements through its own contributions. This level of information exchange and sharing for mutual benefit is unlikely to be replicated in a time critical way by government.²⁹
74. AusCERT has developed the experience and level of trust required to perform this function over 15 years of operation. There are still a number of sensitivities across the national and international security community and AusCERT is well placed to address these. It is impractical to iterate all of these sensitivities here, however there are a few "case in point" examples that are worthy of consideration. For example, some sections of Australian industry show a degree of discomfort in reporting or discussing issues with the Australian government. The reasons for this are complex, but issues such as fear of regulation, concern over reporting to existing regulators and uncertainty over potential legal issues are amongst those of concern to business.
75. By contrast, some of these organisations feel more comfortable in reporting to AusCERT as AusCERT is able to take a truly independent view and work in the best interest of the affected parties. In these matters, AusCERT operates with a freedom of interaction that it is unlikely that an Australian government agency can enjoy in the near future particularly in dealing with a range of foreign government counterparts.
76. AusCERT also has a great deal of flexibility in outreach with foreign governments on operational security matters and can add value to the Australian response arrangements that cannot be easily replicated by government.

²⁹ Despite TISN's value, its information exchange arrangements are more formal, at a higher level, slower and infrequent and of a different nature to the technical and tactical intelligence exchanged in the operational context mentioned here.

77. Unlike government agencies and in keeping with the freedoms and resources that come with working in the academic and research sector, AusCERT has the ability to rapidly develop new tools to provide automated responses to deal with new vulnerabilities and threats on a large scale. By contrast, many government agencies have various policy and role based constraints. By operating outside of core government, and largely unencumbered by inter-agency jurisdiction concerns, AusCERT is able to react in time-frames measured in minutes and days to threats that adapt in a similar timeframe.
78. Without the ability to adapt and respond rapidly by develop new tools, systems and processes to respond to the cyber threat environment, no national CERT will be able to effectively respond to the volume or speed of attacks that occur. This allows AusCERT to also be more proactive and able to detect new attacks and vulnerabilities before they are reported to us and prevent further attacks to vulnerable systems.
79. A benefit of its long standing experience in incident response is that AusCERT is able to dynamically and rapidly respond to new threats and vulnerabilities to mitigate risks in the Australian context. AusCERT's relationships, coupled with its agility, would be difficult to replicate within the less dynamic and more hierarchical and structured nature within government agencies.

Advantages of retaining the national CERT role within UQ

80. AusCERT has already outlined a number of challenges the Australian government would face and need to overcome in order to develop a national CERT with AusCERT's level of experience, expertise, tools and trust relationships.
81. The following paragraphs outline particular advantages that exist by funding AusCERT as part of the University of Queensland to continue this role.
 - a) It provides practical experience from an organisational perspective of issues surrounding in managing network security for a large complex network environment.
 - b) As part of UQ, AusCERT is very close to the academic and research sector including through its work with the Australian Access Federation, a PKI infrastructure being built for the benefit of Australian universities. This enables AusCERT to share information in a trusted way with Australian universities in ways that are unlikely to be achieved to the same degree by the government. The close trusted relationship can help strengthen and secure nationally critical parts of the digital information economy/ infrastructure belonging to the higher education sector.

AusCERT's current funding model

82. AusCERT is the national CERT (computer emergency response team) for Australia and is an independent, non-government, not-for-profit organisation based at the University of Queensland. Its staff are employees of the University.
83. AusCERT's roles and functions can be broadly divided into those services it provides on a fee-for-service basis and those which are not funded but are carried out as part of its national CERT role. In this role, AusCERT actively supports the Australian public interest by helping to protect the security of the Australian Internet using community, through the national CERT role outlined above.
84. AusCERT provides a range of services on a fee-for-service basis, including subscription services, training and education and conference registration fees, which generate income to cover the services associated with its national CERT role for which it receives no direct funding or income.

National Broadband Network and Next Generation Network

85. The terms of references invites comments on:

emerging e-security issues including those resulting from technological change, including roll-out of the National Broadband Network the new broadband network.

86. It is generally recognised that the level of malicious Internet activity and cybercrime increases in proportion to the availability of, high speed broadband services.³⁰ This is because cybercriminals are attracted to compromise and control computers on networks with powerful broadband capabilities because this provides them with the greatest versatility and reliability in how they may use their compromised "bot" hosts.
87. AusCERT has noticed a rapid growth in the level of online threat since 2003. This in itself provides substantial justification for the funding the role of the national CERT within the government's e-security framework for the whole information/digital economy. When the government's new fibre to the node, National Broadband Network (NBN) is available, the level of interest of interest in targeting Australian computers will significantly increase.
88. A similar compounding effect will be further exacerbated with the development of Telstra's (and other carriers) new Next Generation Network (NGN). Under the NGN, the backbone architecture of the majority telecommunications system will be

³⁰ OECD, *Malicious Software (Malware) – A Security Threat to the Internet Economy*. <http://www.oecd.org/dataoecd/53/34/40724457.pdf>, page 26

modified and public switched telephone network, mobile networks and IP networks will converge to allow a vast arrange of services (such as voice, video and data, inter alia) to be carried more quickly and effectively across the network backbone.

89. A key concern with the new NGN is that there will be little or no security built into the NGN backbone architecture. Rather it will be increasingly important for the end points (nodes) to bear responsibility and the major burden of security, which even today is proving increasingly difficult. The combination of both these technological changes to the digital landscape in Australia will significantly exacerbate the current threat environment and provide even more reason to support and continue to develop, the national CERT function through AusCERT.
90. The expected delays and difficulties in attempting to develop a government operated national CERT would set back e-security arrangements significantly in Australia at a time when, due to the worsening threat environment and technological changes to the digital landscape, this capability needs to be augmented. It makes good sense, and will be more efficient, to fund and augment the already effective capability that exists through AusCERT than start from scratch.
91. As noted in paragraph 40, a key feature of a national CERT is to provide services and capabilities that *would otherwise be difficult for individuals or organisations, be they government or business to provide themselves in a timely manner*. Hence, with the imminent approach of the NGN and the NBN, when it is more likely end points will be attacked, there will be greater need for services that organisations and individuals cannot readily provide themselves, through the national CERT function.
92. This point was made in part by the UK House of Lords in its enquiry into Internet Security. It noted that:

The current emphasis of [UK] 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.
(paragraph 3.34)

The current assumption that end-users should be responsible for security is inefficient and unrealistic. (paragraph 3.67)³¹

93. As noted in paragraph 46 (d), it is incumbent on the government to provide assistance when – for whatever reasons – protective counter-measures fail in order to help individuals, businesses and other organisations recover and continue to participate without harming others in the online information economy. With the advent of the NBN and NGN, this is even more imperative.

³¹ House of Lords, Personal Internet Security, Volume 1,
<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>

94. Funding the national CERT role provided by AusCERT will ensure general users/participants in the information economy and CIIs are better placed to prevent, detect and respond to cyber security risks associated with increased availability, affordability and bandwidth associated with a new NBN and the new and/or increased use of online services it will bring.
95. In addition to a funded national CERT role, the NBN and NGN would benefit from improved national arrangements for:
- a) Network monitoring (layer 3) to assist in the early detection of widespread cyber attacks, inter alia. Details of this strategy have been provided in previous submissions to government.³²
 - b) Better industry policies for domain name registrars and ISPs for dealing with compromises on their networks or the de-registration of fraudulent domains. Details have been provided in a previous submission to auDA.³³
 - c) Better adherence to standards on securing domain name servers within Australia.

Roles and responsibilities of government, business, education sector and home users

96. The terms of references invites view on:

the respective roles and responsibilities of these different sectors, and how they can best be integrated within the national framework.

Australian government

97. There are a number of things that are difficult for each of these groups to do by themselves and this is where the government – through AusCERT – can add significant value and assist. The Australian government has the responsibility to ensure the national CERT function is maintained for the benefit of the digital

³² Submission to DCITA, Review of the e-Security National Agenda, <http://www.auscert.org.au/7037> (2006)

³³ See AusCERT submission relating to .auDA review of the .au domain name policy framework, <http://www.auscert.org.au/8396> (2007)

economy in an efficient and cost effective manner. It can achieve this by funding AusCERT in this role.

e-Government service providers

98. All federal and state e-government (including e-health) programs have responsibility to fully consider risks to the entire channel (not just government systems and data) including to personal identifying information and provide accurate information about those risks to the public.³⁴ This issue is both a privacy issue and data security issue. E-government services providers, as part of the e-security framework, need to outline how they will effectively manage risks to mitigate current and future threats before they roll out services.
99. Better support is needed to audit and mandate better security for government web sites and e-government services than currently exists. This will help reduce compromises and harm to other computers within the Australian digital economy that connect to these sites.

Business and government web site owners

100. Many businesses and some government agencies are failing to secure their web sites. The current trend to compromise legitimate web sites to serve malware to the public creates a difficult situation. Many businesses are reluctant to remove the affected parts of their web site, or if outsourced, may have difficulty doing so quickly.
101. It is not enough for government to tell home users to patch and secure their systems when business and government are failing to secure their own web sites resulting in their web sites being used to compromise home users' computers. Government and business owners have a higher onus of responsibility to make sure their web sites, which are generally trusted by the public, are not used to serve malware and compromise unsuspecting visitors' computers.
102. Prevention is better than response. Government needs to provide incentives for organisations to build and maintain secure web sites. This may be achieved by providing more opportunities for training courses, web audits and 'secure web site' certifications, etc.
103. The seriousness of this situation requires that more needs to be done to prevent generally trusted web sites serving malware to members of the public; this includes both prevention and response capabilities.

³⁴ For further details see AusCERT's submission to the Australian Law Reform Commission, available at: <http://www.auscert.org.au/> 8510

Small business and home users

104. Small business and home users will benefit from the government's new Stay Smart Online Alert Service (and associated Stay Smart Online resources). However, there are limits as to what can be achieved through the resources available via the web site alone. This group in particular would benefit from the ability to contact a national CERT and enquire about security issues.
105. At present, while AusCERT currently provides this assistance to those who seek us out, without dedicated funding, this service is not one that is actively encouraged for fear of being over-whelmed by time consuming public enquiries.

Recommendations

The following is a list of the recommendations that appear throughout the submission.

- R1 The new e-security framework should formally recognise the status, role and function of the national CERT including the key aspect of acting as a single Point of Contact (POC) for Australia in the global IT community (as was intended by creation of the national CERT function within AusCERT) and more clearly defined set of complementary roles for AusCERT and GovCERT.au. Through its national coordination role, AusCERT can then triage information and redirect or call upon the participation of GovCERT.au as appropriate. This would be wholly consistent with the existing MOU between AusCERT and the Australian Government.*
- R2 As part of the government's framework to protect the CII, AusCERT should be formally identified within the framework as a source of reliable and unique expertise about cyber threats and vulnerabilities affecting the Australian information and digital economy, including the CII.*
- R3 As part of the government's framework to protect the CII, AusCERT as the national CERT should be included in the JOAs.*
- R4 To develop a more effective and integrated national approach to e-security for all interests (critical and non-critical, business, government and home users) within the Australian information and digital economy, the new policy framework should recognise and articulate the role of AusCERT as the national CERT and, together with GovCERT.au, clearly delineate complementary roles and functions.*

In doing so, it should be recognised that AusCERT has a long standing history and reputation of helping to protect Internet security in Australia and, through its actions here, abroad. As such it would be counter-productive to pursue the government's e-security policy goals without better utilising, in a coordinated manner, the services, expertise and capability provided by AusCERT.

The best way to achieve the latter is through a formal integration of AusCERT into a truly national e-security framework including a funding relationship which binds funding to fulfilling particular role/functions and achieving outcomes.

The ESPaC would benefit from substantial involvement by AusCERT and it is difficult to see how it could operate effectively without such involvement.

- R5 AusCERT supports funding by government of its national CERT role, as part of a new e-security framework, while allowing AusCERT to conduct other services on a fee-for-service basis and remaining part of the University of Queensland.*
- R6 AusCERT recommends these services* be funded by the Australian government to provide an integrated approach to cyber security accessible by all users/participants in the digital information economy.*

Funding the national CERT role, and incorporating the functions as part of a new e-security framework will allow the government to better monitor the threat environment and evaluate response preparedness capabilities and mitigation strategies that make up part of the e-security framework.

With dedicated government funding, there is also scope to improve and augment these services further in line with international expectations and the changing threat environment.

- R7 Adequate government funding for the national CERT role would also allow AusCERT to upgrade many of its internal systems and processes to provide better granularity of the nature of cyber attacks AusCERT handles affecting Australian information/digital economy to allow better e-security planning, threat analysis and mitigation to occur.*

References

OECD, *Malicious Software (Malware) – A Security Threat to the Internet Economy*, <http://www.oecd.org/dataoecd/53/34/40724457.pdf> (2008)

House of Lords, *Personal Internet Security*, Volume 1, <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf> (2007)

Submission to the Australian Law Reform Commission, Review of the Privacy Act 1988, <http://www.auscert.org.au/8510> (2007)

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

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

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

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

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

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