SPECIAL REPORT

ASPI

December 2009 — Issue 26

Cyber security: threats and responses in the information age

by Alastair MacGibbon

Executive summary

Cyber security has emerged as a critical issue on the national security agenda. The threat to Australian interests, both strategic and economic, from the manipulation of electronic data and information systems means that cyber security is now a core national security priority. The risk is not yet fully understood by the public, and the current government policy response is less than ideal. This paper discusses the cyber threat environment and suggests several policy recommendations for consideration by government.

The paper approaches the issue of cyber security from a risk management perspective: understanding that in the online space absolute security is unachievable. Unlike some other national security concerns facing Australia, such as the possibility of conventional warfare between nation states, we are certain that there are criminal exploitation and state-sponsored computer network operations conducted against us now and that there will be in the future.

This paper seeks to assist in our ability to understand the risks, manage them better, mitigate them where possible, and thereby become a more resilient society.

There is a widening gap between the cyber security problem and our national capacity to deal with it, leaving a greater level of risk facing us as a nation. This is due mainly to the incremental nature of government policy-making which can't keep up with the speed of information and communications technology innovation, and more importantly, how such systems are abused.

We argue, too, that industry self-regulation has failed in the cyber security space. The paper calls for national leadership where prompt but considered decisions are arrived at in partnership with industry. We also recommend the establishment of an internet crime reporting and analysis centre to coordinate the national response. These decisions need to be carefully communicated to the public, and privacy must continue to be a central goal.

The global risk environment: the UK and US

In line with growing threat perceptions, both Washington and London have embarked on major policy reviews of the cyber security environment.

In October 2009, during cyber security month in the United States (US), President Barack Obama described the internet as offering both 'great promise and great peril', as being a key component of US 'military superiority and public safety', and that the 'internet and e-commerce are keys to our economic

Box 1: The National Security Statement

On 4 December 2008 the Prime Minister delivered Australia's inaugural National Security Statement in which he defined national security as, 'freedom from attack or the threat of attack; the maintenance of our territorial integrity; the maintenance of our political sovereignty; the preservation of our hard won freedoms; and the maintenance of our fundamental capacity to advance economic prosperity for all Australians.' [1]

The statement included references to cyber warfare, cyber attacks, electronic espionage, threats to critical infrastructure running on computer systems, and computers used by terrorists. As a result, bolstering e-Security efforts was listed as one of Australia's top national security priorities.

competitiveness'. The President described the victimisation of individual Americans as 'one of the most serious economic and national security challenges we face as a nation.' He concluded that while online safety and security requires cooperation at all levels of government and the private sector, including engagement of citizenry, 'government has the responsibility to lead'.[2]

In February 2009 the Obama Administration commissioned Melissa Hathaway to conduct a 60-day "clean slate" review of US cyber security policies and structures. Her *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* was presented in May 2009.[3] The report is strongly worded, saying that past policies had failed. The report recommended, and President Obama accepted, a 'ten step near term action plan':

1. Appoint a cyber security policy official responsible for coordinating the nation's cyber security policies and activities.
2. Sign off on an updated national strategy to secure the information and communications infrastructure.
3. Designate cyber security as one of the President's key management priorities.
4. Designate a privacy and civil liberties official to the National Security Council.
5. Formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cyber security-related activities across the federal government.
6. Initiate a national public awareness and education campaign to promote cyber security.
7. Develop US Government positions for an international cyber security policy framework and strengthen our international partnerships.
8. Prepare a cyber security incident response plan.
9. Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.
10. Build a cyber security-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the nation.

However, to date the White House cyber security policy official ('cyber tsar') has not been appointed, and since this role is vital to the delivery of the remaining nine steps, it would appear little progress is being made.

Indeed, with the number of US agencies involved in the cyber security space, and with significant jurisdictional overlap between them, it is unlikely Australia would benefit greatly from following current US practices (but could gain from some of the principles espoused in the review).

In June 2009 UK Prime Minister Gordon Brown delivered the UK's first Cyber Security Strategy. The strategy concluded with the following assessment:

> Just as in the nineteenth century we had to secure the seas for our national safety and prosperity, and in the twentieth century we had to secure the air, in the twenty first century we also have to secure our position in cyber space in order to give people and businesses the confidence they need to operate safely there.[4]

The strategy argues that economic considerations alone make cyber security a priority: 90 percent of offline purchases use credit or debit cards relying upon telecommunications systems; £50 billion in e-commerce transactions occur each year. As part of the strategy, the British Government has established an Office of Cyber Security and appointed a Cyber Security Minister.

UK government capabilities and policy developments have more in common with Australia than the US experience. In fact, the UK program of work is almost identical to that in Australia's Attorney–General's Department. A significant point of departure between the British and Australian responses has been the notion of privacy which receives less attention in current Australian thinking.

It is also of note that in May 2009 Australia—and in June 2009 the US and the UK—announced the formation of operational cyber defence centres within their respective signals intelligence agencies: the Cyber Security Operations Centre as part of the Defence Signals Directorate (DSD) in Australia, Government Communications Headquarters in the UK, and the Cyber Command within the US National Security Agency.

Why e-Security matters in the Australian National Security context

According to the Australian Bureau of Statistics there's a continued rise in internet use and access (see Figure 1). As of June 2009 there were 8.4 million active internet subscribers in Australia.[5]

Consumer passion for the use of information and communications technologies (ICT), the internet and mobile telephones in particular, is matched by companies, and, to an almost equal extent, government agencies. Networked computer systems, laptops, removable storage media, mobile telephones with the power of many personal computers, have all made information less physical and thereby more susceptible to loss, redirection, and outright theft.

In the past decade the unauthorised exploitation of online systems by criminals has evolved from a cottage industry to a factory production line. Uptake of technologies has outpaced our capacity to deal with the unintended cyber security risks. Criminals break into computers to steal information like credit card details, email addresses, passwords, and economic secrets, and use or sell it. There are well developed global markets trading in this information.

Governments have realised the benefits too, developing computer network exploitation capabilities to gather information from economic, military and government systems offshore.

Bad actors can use a compromised computer to pretend to be the actual subscriber of a

Box 2: The government's policy today

Since 2001 the E-Security National Agenda (ESNA) has been the Australian Government's policy vehicle aimed at creating 'a secure and trusted electronic operating environment.'

ESNA has been the primary (but not only) source of funding for Australia's preparations against (criminal and state-sponsored) cyber attacks on Australia's National Information Infrastructure (NII). ESNA has also provided for broader cyber security initiatives, including specific funding for building operational agencies' capabilities in the areas of crime and intelligence, information sharing (under the auspices of the Trusted Information Sharing Network) between government and private companies owning and operating critical infrastructure (water, electricity, telecommunications, food, etc), as well as public and business education (including E-Security Awareness Week).

Throughout the life of ESNA the Attorney–General's Department has been the lead policy agency for cyber security.

One of the enduring arrangements of ESNA has been the Joint Operating Agreement between the Australian Federal Police, the Australian Security Intelligence Organisation, and the Defence Signals Directorate allowing for information sharing and investigations relating to NII incidents, threats and vulnerabilities.

The ESNA was first reviewed in 2006. One of the review's findings was 'that because the online environment is highly interconnected, e-security threats to different segments of the Australian economy cannot be addressed in isolation.'[6]

After its 2006 review, the ESNA priorities became to:

- reduce the e-security risk to Australian Government information and communications systems
- reduce the e-security risk to Australia's national critical infrastructure, and
- enhance the protection of home users and SMEs from electronic attacks and fraud.

In 2008 a further review of ESNA was conducted. The 'E-Security Review' recommended several new core capabilities and initiatives, including:

- the creation of a national Computer Emergency Response Team (CERT) utilising (and building on) the contracted services of AusCERT
- the establishment of a Cyber Security Operations Centre within the Department of Defence
- the creation of an e-security code of practice for Internet Service Providers (ISPs)
- the development of a whole-of-government international engagement strategy for e-security.

ESNA policy priorities talk about reducing risk and enhancing protection, but the initiatives over the past 8 years have largely been reactive, relating to information sharing and investigation—with the exception of the ISP code of practice—not attempting to change the structural settings in which cyber attacks occur. This is symptomatic of the "light touch", co-regulatory-based approach towards telecommunications of the era, which has relied upon industry self-regulation and, largely, failed.

service or can add the compromised machine to networks of other compromised computers called 'botnets'. Botnets are controlled remotely, and can be used to shut down the internet activities of businesses and governments through distributed denial of service (DDOS) attacks, as well as to deliver spam emails, crack passwords, and a growing number of other illegal activities.

In short, cyber security is a growing national security concern for three main reasons: the threat posed to Australia's economic interests; the integrity of Australian Government information and systems; and the wellbeing of the Australian public.

Most importantly, the pace of change, the scale of the problem and its extended geographic nature necessitates national leadership and robust action consistent with other national security interests.

The drivers for wrongful online activity

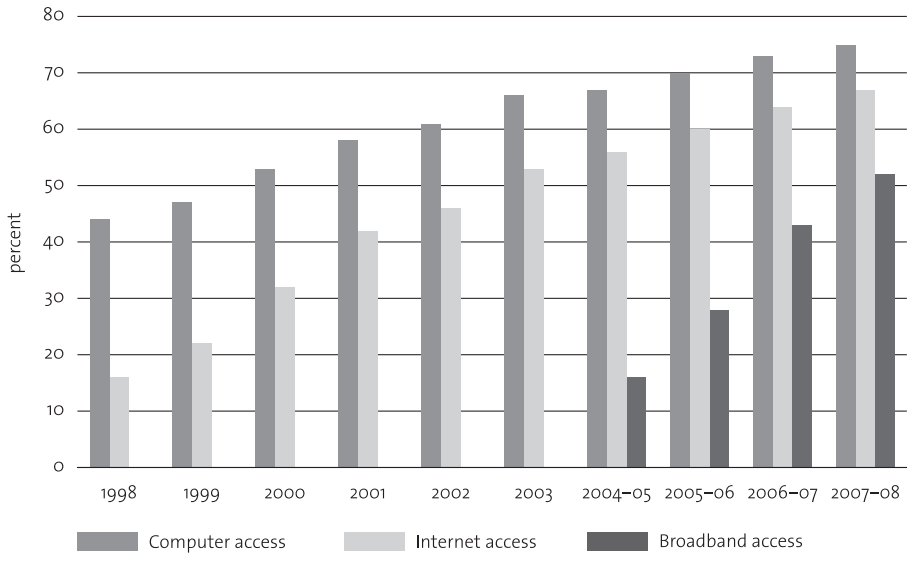
One of the key factors driving increased criminal behaviour online is that there is a presumption of anonymity—and a real difficulty in absolute attribution—in the online space that emboldens criminals.

The unfortunate reality of all types of online crime is that there is a very low likelihood of offenders being caught. This low risk of apprehension or conviction combined with the profitability of activities has ensured a steady supply of willing offenders and drives lucrative ongoing criminal innovation.

There is plenty of opportunity for online crime, with over a billion internet users globally, and millions of businesses and government agencies holding data in networked computer systems. Sometimes users lack experience and understanding of the consequences of their actions; other times the computer itself is vulnerable to exploitation. Often it is both.

It is easy to see how problems can keep occurring. A March 2009 report by the Australian Communications and Media Authority, *Australia in the Digital Economy Report 1: Trust and Confidence* highlights the complacency of the Australian internet population—less than 50 percent

Figure 1: Internet subscribers in Australia



Source: Australian Bureau of Statistics, Report on Household Use of Information Technology, Australia, 2007–08.

of survey respondents have installed anti-virus software, and even fewer had firewalls or other protective measures on home computers.

There is a strong link between bandwidth and computer use: more of one leads to more of the other. This holds true for misuse and victimisation. With the announcement of the National Broadband Network (NBN) to deliver 100 megabits of data per second to 90 percent of the Australian population, a step-change in safety and security must be developed.

Now is a unique opportunity for Australia to redress some of the structural and policy weaknesses of the past and to establish global leadership in this field.

Death by a thousand cuts

We have seen that malware—malicious criminal programs which perform functions not authorised by the user like leaving a "back door" open to the computer or transmitting passwords or sequences of keystrokes to online collection points—has proliferated.

All IT security companies can show charts indicating near exponential growth in criminal attacks and exploits against computer operating systems.

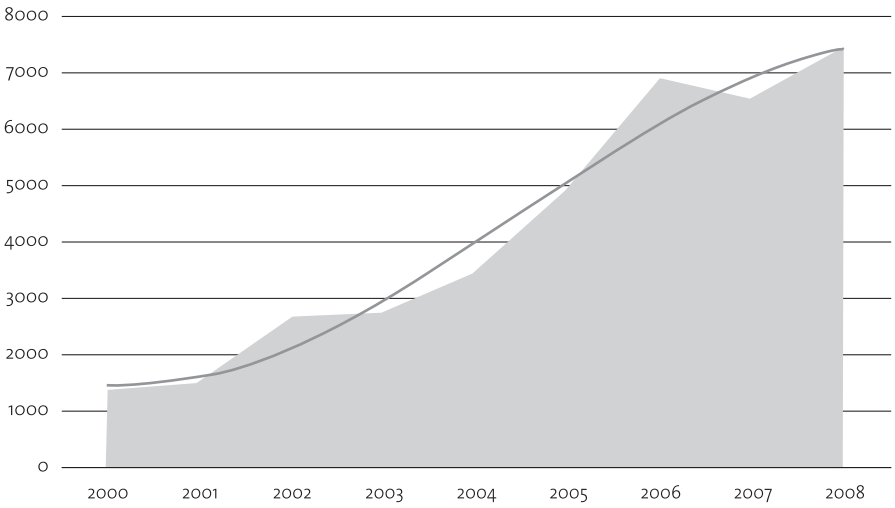
Below is a chart taken from the IBM Internet Security Systems *X Force 2008 Trend and Risk Report* published in January 2009 which shows the steady climb of vulnerability disclosures in software.[7] These vulnerabilities are potentially used by criminals and state actors to attack the computer systems and applications that we use.

The *McAfee Labs Blog*[8] (Figure 3) looks at the unique attack tools used by criminals, which, as with the chart above, shows a rapid growth in the threat.

Oftentimes such malware is combined with 'social engineering', aimed at convincing users to undertake activities they otherwise would not. It is this amalgam of devious software and human trickery which has compounded the problem, multiplying the vectors of attack and making it much harder to reduce risk.

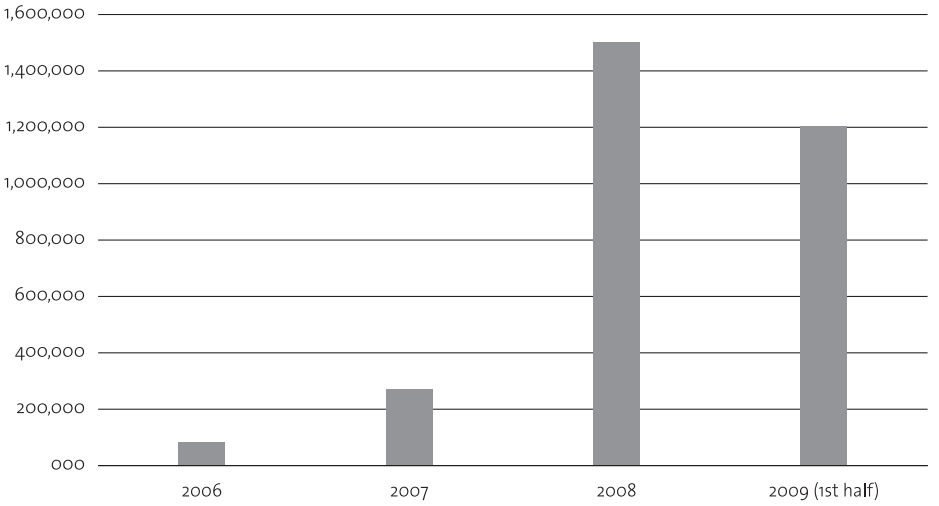
A tipping point occurred around 2003 with the advent of phishing, whereby criminals

Figure 2: Vulnerability disclosures, 2000–2008



Source: IBM Internet Security Systems X Force 2008 Trend and Risk Report.

Figure 3: Unique malware growth



Source: McAfee Labs Blog.

masquerade as reputable businesses, and use fake emails and websites to trick users out of their passwords and other identity credentials.

Criminals realised that the average consumer held information of value, like their password and identity information. It was at that point that the scale and jurisdiction of the threat moved beyond the capability of individual government agencies. Rather than attacking a centralised bank system that might have the details of five million account holders, criminals duped account holders directly, who are largely unprotected and therefore unaware of the risk to themselves or others. The criminal can get the same information in a scaled way, individual by individual, with a very low likelihood of detection and an even lower likelihood of prosecution.

Of course that is not to say central repositories are disregarded by cyber criminals. For example, in August 2009, Miami resident Albert Gonzalez was charged for his part in stealing 140 million credit card details after compromising US credit card processor Heartland Payment Systems, 7-Eleven, and Hannaford Brothers supermarkets.

Anywhere financial or identity information sits it is fair game. For example, in October 2009 the UK's *Guardian* newspaper admitted to losing up to 500,000 job applicant's details[9]. Similarly, the NSW Government's job site was hacked in early 2009, exposing the personal details of an undisclosed number of job applicants.

So far the best protection we have had against victimisation is criminal inefficiency. Criminals often get hold of data—but their capacity to exploit it can be limited. It is an important distinction.

Espionage—Computer Network Exploitation

Certain countries also have an interest in a range of sensitive Australian Government information. This is especially true for information which sits in the realm of traditional national security considerations: trade, defence, foreign affairs and intelligence. Australia's close intelligence partnership with

the US, UK, Canada and New Zealand make it a more obvious target for attack.

The Australian Security Intelligence Organisation (ASIO) acknowledges that Australian Government and business computers have been the target of foreign intelligence agencies.[10] The US Office of the National Counterintelligence Executive in its 2008 *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* gives more detail about attacks against the US Government, and specifically identifies mobile telephones, particularly the Blackberry and iPhone, as being of increasing importance and concomitant risk.[11] Open source reporting indicates just how pervasive and damaging attacks against mobile devices may become.[12]

As well, some of Australia's trading partners and commercial competitors show a keen interest in data held by Australian businesses. Economic espionage makes good sense: access to sensitive information, like the price a large exporting company will accept for wheat, coal, or iron could cost the nation billions of dollars in lost export revenue, either through purchasers driving a well-informed harder bargain, or being undercut by a rival seller. Yet—on the whole—such information is stored and accessed in corporate systems which have questionable defences, and often handled by staff unaware of the value of such information.

Under the Australian Government IT security arrangements, the Defence Signals Directorate has the lead information assurance function for government, providing advice to other agencies. The logic being that since DSD is Australia's signals intelligence agency, knowing how to attack and exploit can assist in defence.

The establishment of a Cyber Security Operations Centre within DSD, which will provide a 24/7 watch and warning role, with staff from AFP, ASIO and CERT Australia, will serve to solidify DSD's information assurance capacity and broaden its ability to assist other agencies.

Although some progress is being made in improving resilience of government systems and the practices of staff, there is still significant discretion granted in the Australian Government Information Security Manual (formerly ASCI 33) to chief executives of government departments to issue waivers and to diverge from security best practices provided by DSD. Though it is interesting to note in certain circumstances discretion is being eroded, evidenced by the Australian Government Information Management Office *Instructions on the Allocation and Use of Blackberry in the Australian Government*.[13]

If the Australian Government expects strategic businesses to improve their IT systems and practices, which are not progressing at the pace of government efforts, it must lead by example and further reduce the discretionary powers of individual departmental chief executives within the Information Security Manual, while increasing the authority of DSD. A controversial, but necessary, change.

There is no current capacity to measure and report on the cyber health of government networks, and such a system needs to be introduced, based on self assessment against criteria established by DSD, and monitored by the Cyber Security and Coordination Committee chaired by the Attorney–General's Department.

The government must endeavour to provide a cohesive and comprehensive set of information assurance policies, recommendations, and guidelines to Australian businesses to ensure that reasonable best practices are encouraged and poor practices are never rewarded.

In an effort to speed up private sector change, the government must increase the scope and frequency of intelligence briefings to Australian businesses on the types of activities and threats they may encounter, as well as expand ongoing communications channels. CERT Australia and DSD will play significant roles in this endeavour.

Cyber Warfare—Computer Network Attack

The notion of cyber warfare has remained attractive to military commentators over several years mainly because of the asymmetric nature of the attack, the supposed 'clean' nature of the attack, and the deniability associated with the attack.

Two significant examples are the distributed denial of service (DDOS) attacks conducted against Estonia in 2007, and Georgia during the South Ossetia War in 2008, both carried out by Russian interests. Most evidence would point to Russian nationalists who may have acted on behalf of Russian authorities.

We have seen examples in Australia where issue-motivated groups have used website defacement as a means of disruption and spreading propaganda, but they pose no greater security risk than the embarrassment to governments: the equivalent of an electronic poke in the eye.[14] So do most of the denial of service attacks launched against government websites, as there is little if any impairment to non-public systems.

But the July 2009 attacks launched out of South Korea against US Government (and other) websites shows how such attacks could have more significant implications. It seems that the attackers had been careful to use mostly computers from South Korea whereas in other DDOS attacks computers would generally be more geographically dispersed.

Much legitimate internet traffic emanating out of South Korea was dropped by the US in an attempt to stem the attacks, hampering the activities of innocent South Korean citizens, business and government. This highlights the collateral damage that can occur with such attacks, helping dispel the 'clean' or surgical notion suggested by some. A *New York Times* report suggested that concerns over lack of ability to contain the effects of an attack led to the Bush Administration shelving a plan to launch a cyber attack on Iraq's financial system before their invasion in 2003.[15]

Most commentators agree though, that such attacks are more annoying than damaging, and the most successful cyber efforts will operate in the realm of less overtly visible compromise of computer systems.

A report on *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* prepared for the US–China Economic and Security Review Commission highlights conventional and irregular forces being developed for war fighting, but devotes most of its effort to the espionage side.[16]

There are, of course, offensive cyber capabilities being developed by various militaries, and China is most often cited. The concept of developing computer network attack capabilities to work alongside other military assets is a rational one for all militaries; it is a reasonable extension of the role that electronic warfare plays in modern conflicts. The US National Research Council of the National Academies has published a thoughtful document on the various considerations that need to be taken into account when developing a cyber attack capacity: legal training, command and control, political fallout and a range of other issues.[17]

Australia has announced the formation of a Joint Electronic Warfare Centre and it will be

important to work through Australia's own cyber warfare concepts, to understand the less-than-surgical nature of such activities, to understand what collateral damage may be inflicted, and to determine what thresholds of attack justify responses, as well as dealing with the issues raised in the US National Research Council report.

Terrorist use of the internet

Terrorist groups increasingly use the internet for communications, propaganda, recruitment and radicalisation. As a previous ASPI publication has noted, the problem in Southeast Asia is growing.[18]

The online motivations and methods of terrorist groups are similar to those of other criminals: they benefit from the relative anonymity of online transactions, including establishing websites and peer-to-peer channels for communications. They benefit from the ease of conducting online fraud and there have been publicised examples where terrorist groups have raised funds through internet fraud.[19]

The internet has allowed terrorists and other issue-motivated groups to get their message—uncensored—to the world in a real-time way. This is possibly where the internet has been of greatest benefit to them. Those messages are then often re-broadcast by mainstream media. While serving to erode public confidence in Western government actions and to influence public debate, the biggest danger is that potential recruits and sympathisers may find succour in the message, and be emboldened to greater radicalism and violence.

It is worth noting that cyber terrorism—whereby terrorists conduct computer network attacks—has largely failed to materialise. This is most likely explained by the greater publicity and impact derived from traditional physical attacks.

Critical Infrastructure

With the pervasiveness of information and communications technologies across industries, it is logical that an increasing amount of Australia's critical infrastructure is either directly or indirectly supported by those technologies. Critical areas include food production and supply, electricity, water, transport, telecommunications and banking. Of course many federal and state government systems are essential too, like the police and emergency services.

Security vulnerabilities in these systems could be exploited to subvert or impair networks, although there have been very few open source references to such actions.

In the area of critical information protection, the Australian Government, via its Trusted Information Sharing Network, has done a good job in sharing threat information, and engaging private sector partners. This capacity will expand with CERT Australia and the insights available from the Cyber Security Operations Centre.

And Australia continues to participate in global exercises with our allies to simulate attacks on this type of infrastructure. However, there is a diminishing ability to distinguish between a critical infrastructure network and end users, whether businesses or households. In fact, to focus on one without the other is to address only half the problem.

A problem without borders

The inherently multi-jurisdictional nature of the internet hampers efforts to fight its abuse. The law enforcement, domestic intelligence and regulatory agencies of nation states are jurisdictionally bound, and criminals exploit the inefficiencies of jurisdiction to their own advantage. Even where there are good intentions for mutual assistance between countries, mechanisms designed

for offline cooperation are not suited to the online environment. And there remain many countries where legal regimes are weak, or where there is a lack of will to impose the rule of law on criminal actors operating online.

The 2008 e-Security Review recommended enhancing Australia's international efforts. Current efforts should be commended, but they can go further. Just as the Australian Federal Police have deployed liaison officers to international drug crime hubs, and other locations to take the counter terrorism fight offshore, appropriately skilled officers need to be deployed to internet crime troublespots: East Africa, Russia, and some of the more active former Soviet republics at the least. They should also seek to have officers embedded in allied high-tech crime investigative agencies, particularly in the United Kingdom, Canada and the United States, to assist in information sharing and joint operations.

Additionally, the efforts of AusAID need to be harnessed to build cyber crime fighting and cyber security capacity in weaker regional states to reduce their ability to provide safe harbour for network abuse.

The small nature of many individual online incidents means that much of the time they go unnoticed even if reported. One individual act may be spread across many jurisdictions and be replayed against thousands of victims, all of whom have a small loss that combined becomes something of much greater magnitude. The fragmented and often opaque nature of incident reporting prevents law enforcement, regulatory and security agencies from seeing a true picture. Often it is unclear if there is a logical place for reports to be made; agencies accept reports only when they fall into (sometimes narrow) interpretations of jurisdiction, reducing the likelihood of successful intervention and identification of perpetrators.

Should the onus be on victims to know the bureaucratic processes of government, or the physical location of their internet attacker to report an incident? On the whole, businesses and consumers have been left to protect themselves and to clean up the mess when things go wrong.

A national response: establishing an internet crime reporting and analysis centre

Australia needs an internet crime reporting and analysis centre for homes and businesses. The relevant federal law enforcement and consumer protection agencies are not constituted, staffed, or able to deal with the often small and seemingly inconsequential incidents of fraud, spam, scams, data loss, inappropriate content, or sometimes IT security incidents. We need an internet 'shopfront' approach. A place for people to report matters, and to seek advice: a single, consumer-orientated destination, scaled for the internet, which takes a national whole-of-government approach.

This would not just bring Australia into line with the UK, which has announced the formation of the National Fraud Reporting Centre to tackle all fraud and online crime complaints, but would go to the next logical step of delivering services covering safety and security for the end user in one place.

An internet crime reporting and analysis centre would be most successful as a public-private-partnership which could allow real-time information flow between the government's CERT Australia and the Cyber Security Operations Centre, giving Australia a more holistic view of Australia's internet health, and improving our ability to respond to threats and rebound.

An internet crime reporting and analysis centre would deliver significant benefits, including an ability to:

- aggregate complaints to better determine the scope of crime, and to pass on that information to relevant agencies to investigate those responsible
- gather intelligence and trends on scams, illegal content, crime, and IT security attacks from Australian households and businesses
- provide a single point of education and remediation for Australians
- give a sense of redress to victims, reducing feelings of helplessness and frustration
- pass on relevant information to other countries for their action
- reduce individual victimisation and losses
- provide information back to industry to reduce further victimisation.

Importantly, a rationalisation of existing resources within individual agencies already tasked with such reports should make this a relatively inexpensive exercise, with significant upside in terms of output.

A time for shared responsibility

Internet Service Providers (ISPs) play a crucial role in connecting Australians to the internet, as do others in the internet industry such as registrars (who issue domain names), and they could play a much greater role in protecting us. But for a long time many of them have argued that as providers of a commercial service, they are unable to assist.

The government-backed draft Internet Industry ISP Code of Conduct for e-security is a good first step in recognising how ISPs can help reduce e-security threats.

The draft code covers issues such as detection and removal of 'zombie' computers on networks (by building on the existing Australian Communications and Media Authority (ACMA)-managed Australian Internet Security Initiative). It also highlights the role of consumer education.

But because it will be an industry code created under the co-regulatory regime of the *Broadcasting Services Act 1992*, it notes 'the measures recommended in the Code should not adversely affect the commercial viability of the parties and the services they make available'.[20] Even when the code is finally registered with ACMA, and therefore enforceable, it is unlikely ACMA will proactively check for compliance across ISPs: all part of industry self-regulation.

It is time for Australia to consider whether the current 'light touch' approach towards the internet has served its use-by date. It allowed Australia to develop its internet capacity in a relatively unfettered and competitive way, but at the cost of safety and security, which may now be inhibiting future growth.

A final—and more prescriptive—code needs to be registered with ACMA, and enforced. It is inappropriate that backyard ISPs—providing such essential services to the community—should be allowed to provide limited safety and security measures to their customers.

As the NBN begins to roll out next year the government-owned NBN Company will eventually become the dominant wholesale broadband ISP for Australia. Proper consideration must be given to policies that enhance the end-point security of users so that computers connecting to the network have adequate IT security protection, are patched, and pose a lesser threat to other internet users and themselves. Even Microsoft has realised that it is better for the internet at large to allow security updates to install even on pirated copies of Windows,[21] a marked change of policy for the company.

Registrars are those who issue internet addresses (domain names) that we rely upon for a healthy internet. We need to have some comfort that we are visiting the website we think we are. The registrar business is a volume business, not one which spends a great deal of time determining if an applicant for a domain name is who they claim to be. It is about time that Australia instituted a 'know your customer' regime for registrars, just as we have for financial and other services.

But it isn't just ISPs and registrars who need to shoulder more of the burden. There is a greater role for those whom we entrust with our information: business and government. They need to have strong incentive to collect and store less information and better protect the information they do collect. Some of this change can be brought about by the government acting on the data disclosure changes suggested by the Australian Law Reform Commission in its review of the *Privacy Act 1988*. In particular, the need for businesses to notify individuals if data is lost, the Privacy Commissioner, and—perhaps—the proposed new internet crime reporting and analysis centre. Real cyber security for individuals will not be possible without strict adherence to these privacy considerations.

End user responsibility

Individual end users will need to be more responsible in reducing their own e-security risk. We have failed as a society in how we actualise that responsibility. The mantra of end user responsibility has often been taken as an opportunity for governments and businesses to play a minimalist role. If nothing else, it has allowed both to invest very little in preventative risk management.

What is needed is governments and business partnering with home users to help them understand how they can help themselves.

And online businesses need to offer safer services, where education, security and encryption are built into the product, rather than—sometimes—added as an afterthought. In fact, any organisation which collects information and stores it electronically has to build security in, as they are not immune from compromise.

While the Department of Broadband, Communications and the Digital Economy (DBCDE) has the responsibility under ESNA for educating home users and SMEs in e-security, ACMA has funding and responsibility for online safety education. It is time to consolidate these efforts. It is time to build greater resilience into the Australian internet population through an effective 'public health' style campaign designed to change user behaviour.

It is time to weave internet citizenship education seamlessly into the school system. Children should not just be taught how to use technology, they must be taught how to use it wisely, safely and securely.

Key recommendations for government

- Establish an internet crime reporting and analysis centre for homes and businesses.
- Enact data disclosure changes suggested by the Australian Law Reform Commission in its review of the *Privacy Act 1988*.
- Consolidate the online safety and security education efforts of DBCDE and ACMA and undertake 'public health' style campaigns designed to change user behaviour.
- Partner with home users and SMEs to help them understand how they can help themselves.
- Provide internet citizenship education in schools.

- Deploy appropriately skilled AFP officers to internet crime troublespots as well as embedded in allied nations' high-tech crime investigative agencies.
- Build cyber crime fighting capacity in weaker regional states.
- Develop policies that enhance the end-point security of users connecting to the NBN.
- Enforce a 'know your customer' regime for internet registrars.
- Reduce the discretionary powers of individual departmental chief executives within the Information Security Manual, while increasing the authority of DSD.
- Introduce a mechanism to measure and report on Australian Government agencies' cyber security health.
- Provide a cohesive and comprehensible set of information assurance policies, recommendations, and guidelines to Australian businesses to ensure that reasonable best practices are encouraged in businesses.
- Increase the scope and frequency of intelligence briefings to Australian businesses on the types of activities and threats they may encounter.
- Develop cyber warfare doctrine and concepts for the military.

Conclusions

It is clear that information and communications technologies have brought great benefit to society. It is also clear that threats to individual—and national—safety and security have grown as well due to the following factors, which need to be addressed in order to improve Australia's cyber security:

1. The scale of the problem, with targets ranging from individual home computers, phones, and mobile devices to corporate networks and government departments, all of whom contain useful information or may be used as springboards to carry out further attacks.
2. The pace at which the attacks have multiplied and evolved in line with society's increased use of technology and bandwidth.
3. The jurisdictional conundrum that these activities present to nations, where criminals and foreign countries can attack systems using computers from a third, or even within the target country, and where the perpetrators can reside outside the geographic region and reasonable legal reach of the nation.
4. The problem of identity, which means malicious actions can be passed off as committed by others.
5. The indivisible link between individual vulnerabilities and our national security interests: where seemingly trivial annoyances mix with malignant actions of nation states.
6. The pervasiveness of the information which may be compromised, or misused.

The 2008 recommendations of the E-Security Review are logical next steps in capacity building and reflect a recognition that critical information is spreading further into the community.

But the current initiatives lack scale and are—largely—reactive in nature and slow to develop. They tend not to address the root cause of the problem, primarily because of the 'light touch' regime which has dominated internet regulation up until now.

Cyber security will be enhanced if the government approaches the problem from a range of non-traditional angles: the safety and security of end users, increasing protection from businesses and ISPs, enhanced law enforcement, intelligence

and CERT capacities, right through to the development of cyber warfare doctrines.

There needs to be a greenfields review to determine a platform upon which Australia can build the cyber security framework for a new generation.

Endnotes

1 http://www.pm.gov.au/sites/default/files/file/documents/20081204_national_security_statement.pdf Transcript of the Prime Minister's National Security Statement, The First National Security Statement to the Australian Parliament, p.7

2 http://www.whitehouse.gov/blog/Protecting-yourself-online/

3 http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

4 http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf

5 http://www.abs.gov.au/AUSSTATS/abs@.nsf/mf/8146.0

6 eSecurity National Agenda Policy Statement, Department of Broadband, Communications and the Digital Economy, http://www.dbcde.gov.au/__data/assets/pdf_file/0011/71201/ESNA_Public_Policy_Statement.pdf

7 http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf p.18

8 http://www.avertlabs.com/research/blog/index.php/2009/07/22/malware-is-their-businessand-business-is-good/

9 http://www.theregister.co.uk/2009/10/26/guardian_jobs_data/

10 ASIO Annual Report to Parliament 2008—2009, p.12

11 http://www.ncix.gov/publications/reports/fecie_all/fecie_2008/2008_FECIE_Blue.pdf

12 See for example http://www.theregister.co.uk/2009/10/23/iphone_voip_sniffing_made_easy/ and http://www.theregister.co.uk/2009/10/22/rim_blackberry_bugging_software/

13 http://www.finance.gov.au/e-government/security-and-authentication/docs/Instructions.pdf

14 See for example http://news.bbc.co.uk/2/hi/uk_news/england/wear/8350039.stm and http://www.abc.net.au/news/stories/2009/07/16/2628167.htm

15 John Markoff and Thom Shanker, Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk, New York Times, 1 August 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html

16 http://online.wsj.com/public/resources/documents/chinaspy20091022.pdf p.8

17 http://books.nap.edu/openbook.php?record_id=12651&page=R1

18 Countering Internet radicalisation in Southeast Asia, ASPI Special Report Issue 22, March 2009.

19 http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html

20 http://iia.net.au/images/resources/pdf/esecurity_code_consultation_version.pdf

21 http://windowsteamblog.com/blogs/windowssecurity/archive/2009/04/27/who-gets-windows-security-updates.aspx

Acronyms and abbreviations

ACMA	Australian Communications and Media Authority
AFP	Australian Federal Police
AHTCC	Australian High Tech Crime Centre
ASIO	Australian Security Intelligence Organisation
AusAID	Australian Government Overseas Aid Agency
CERT	Computer Emergency Response Team
DBCDE	Department of Broadband, Communications and the Digital Economy
DDOS	distributed denial of service
DSD	Defence Signals Directorate
ESNA	E-Security National Agenda
ICT	information and communications technologies
ISP	Internet Service Provider
NBN	National Broadband Network
NII	National Information Infrastructure
SME	small and medium enterprises

About the author

Alastair MacGibbon is an internationally respected authority on high-tech crime including internet fraud, consumer victimisation and a range of internet security issues. Now Managing Partner of Surete Group and founder of the Internet Safety Institute, he advises companies on online trust, and provides thought leadership on internet safety issues. Prior to that, Alastair headed Trust & Safety at eBay Australia and later eBay Asia Pacific. Previously he was the founding Director of the Australian High Tech Crime Centre (AHTCC) and a Federal Agent with the Australian Federal Police.

Important disclaimer

About Special Reports

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au