Australian Information Security Association

Cyber-safety for Senior Australians

Inquiry Submission

The AISA Response to

the Parliament's Joint Select Committee's call for submissions

Date 23 March 2012

Executive Summary:

As Australia's leading organization of information security professionals, the Australian Information Security Association (AISA) is pleased to provide this submission based on a survey of our membership.

In our view, the current security of online services is demonstrably inadequate at a time when cyber threats continue to grow and spread. This exposes senior citizens as well as government and business in Australia to unacceptable risks impacting trade, development, and the personal enjoyment of the benefits of Cyberspace.

AISA urges the Joint Select Committee to take positive steps to improve the effectiveness of information security programs for Australia's private and community sectors. The benefits of positive action and investment in information security will be realised in reduced costs and incidence of security breaches and a safer, more efficient Cyberspace environment for individuals, commerce and national economic development.

Our members cite the availability of reasonable and effective security measures that are simply not deployed, or in some cases are, overlooked by organisations with a Cyber presence. The lack of adequate online Cyber Security directly impacts Cyber-Safety. This can be traced to many organizations not fully understanding or appreciating the security threats they face and placing other priorities ahead of effective Cyber Security – in the absence of any penalties or incentives to behave otherwise. The lack of effective organisational accountability for the impacts of security breaches also contributes to the mounting number of security breaches and failures. Our members agree that all participants in the online world must take a broader view of risks associated with online commerce and the effect their behaviour may have on others and place a higher priority on protecting online services, including responsibility for the security of their own and others' data and their on-line behaviour.

We also recognize that individuals now rely heavily on personal computing and smartphones in their daily lives, but current personal computing technology cannot adequately protect them against growing threats. The active encouragement by Government of the use of effective security technologies for individuals should be continued and enhanced.

Our membership is also clear in recommending broader and more effective data protection laws, including mandatory reporting of high risk security breaches and increased consumer protection. Better co-operation and transparency with trans-border law enforcement agencies would also make Australia a less appealing target for cyber criminals.

The Australian Information Security Association

The Australian Information Security Association (AISA) is a non-profit Australian representative industry body for the information security profession. Formed in 1999, AISA is focused on individual professional membership with a current membership of 1500 security specialists. AISA aims to foster and promote the development of information security professionals and the security of information.

Our broad membership base consists of information security professionals from all industries including education, finance, government, healthcare, manufacturing, mining, oil and gas, transportation, and utilities. Our members range from company directors and managers, lawyers, risk professionals, architects, highly skilled technical security specialists, professors and researchers.

AISA supports the Australian Government's Cyber Security initiatives, including the awareness programs for children and home users, the Cyber Security Strategy (2009), the creation of CERT Australia and the Cyber Security Operations Centre (CSOC), and the current whitepaper development process of the Department of Prime Minister and Cabinet.

AISA Submission Process

AISA developed the content of this submission via a working party and discussion at our national conference on 9 November 2011. Our recommendations are based on a survey of our membership conducted in October 2011 with 215 respondents. The survey report is available to the Joint Select Committee on request to submissions@aisa.org.au.

AISA Survey Highlights

- 90% of our respondents agreed that 'reasonable security strategies and measures were available' to secure our information systems, however, they acknowledged that for a number of reasons, these security controls have not been deployed
- 78% thought that their organisations did not fully appreciate the security threats they faced
- 61% of respondents agreed that 'External stakeholder interests were largely unimportant when planning online services'; the primary focus was on internal parties
- 77% agreed that Australia needs wider data protection laws, with 87% agreeing that there is not appropriate accountability for the impacts of security breaches
- A majority of respondents had experienced inadequate reporting of security incidents, with only 5% agreeing that current Government and law enforcement statistics were accurate. This corresponds with 45% of respondents reporting that the occurrence of security breaches and associated costs within their organisations were kept secret. As such, organisations and Government cannot revise security policies and controls to achieve a better control environment.
- 52% of respondents had experienced similar organisations deploying 'quite different levels of security'. This indicates the current approach does not consistently result in the adequate protection of information assets or online services.

Note: This content and AISA recommendations in this submission were endorsed at the AISA National Conference on 9th November, 2011 by its 700 attendees.

AISA Recommendations

AISA supports the three objectives of the Government's 2009 Cyber Security Strategy. This submission contains several propositions that could progress the achievement of these objectives.

Objective One: All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online

Objective Two: Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers

Objective Three: The Australian government ensures its information and communications technologies are secure and resilient

The Government has a Role to help protect all Stakeholders

Recommendation:

The Government should act to encourage or to require all organisations to protect not only the organisation's interests, but also to consider and mitigate the risks to all stakeholders from information security failures resulting from the organisation's control regime.

Rationale: Relying upon the "market" to ensure that information is adequately protected for the benefit of whole community has had only partial success to date – and the existence of recognised market failures from an economic perspective would support the case for regulatory intervention in support of information protection.

Organisations clearly owe a duty of care to external stakeholders; including customers, creditors and other parties with which they do business, together with their internal shareholders. However, AISA members have noted that attention to this duty of care in so far as it relates to security of information is often a low priority for management.

Organisations owe a fiduciary duty to their shareholders which includes the appropriate protection of assets such as information and the supporting infrastructure. Unfortunately, in the current environment, security is often seen as a secondary consideration and a cost rather than a business enabler. Hence organisations often opt to minimise this cost.

While corporate directors have a clearly defined responsibility to protect the assets of their organisation, the responsibility to protect the information of other parties is often less clear and frequently afforded less weight, consideration, importance and action.

Furthermore, under most existing organisational governance regimes, little consideration is given to the interests of external parties. This is symptomatic of recognised economic failures in the information security market.

AISA submits that the Parliament should, recognise the failures inherent in the information security market and adopt an approach that supports the "right combination" of law and self- or co-regulatory rules and mechanisms to

support better information security practices by all participants in the on-line community. The European Commission is also considering this issue. [1]

AISA notes that this position is *not* proposing the Government defines specific technical requirements, but rather clarifies that an organisation's responsibility for information should extend beyond internal stakeholders.

Supports: Government Cyber Security Strategy Objectives 1 & 2

Data Protection Laws should be Expanded

Recommendation:

The scope of information protection should be expanded beyond personal information. Legislation should address the adequate protection of all information. Any information should be protected, if that information could lead to a gain by deception (fraud), or loss/impact to the others.

Rationale: The current legal regime, primarily based on the Privacy Act, is inadequate to motivate our businesses and other organisations to adequately protect information assets. This extends beyond the protection of personal data.

Supports: Government Cyber Security Strategy Objectives 2, 3

Guidance on "Reasonable Security"

Recommendation:

The Government should work with industry to provide guidance on what is meant by "reasonable security", particularly with regard to new and emerging technologies. This guidance should extend not just to the organisation's own data and systems but should also have regard to its role as a participant in the broader online world, which supports the economic prosperity and security of all Australians. It may include, for example, reference to accepted international standards as well as more specific guidance. The Government should work with Australian industry groups and subject matter experts from a broad range of disciplines including security professionals, social sciences, economists and technologists.

Secondly, organisations should be encouraged or required to protect information according to this guidance and appropriate accepted standards.

Rationale: Given the complexities of the internet, constantly emerging new technologies and business models and ever changing attacks and vulnerabilities, organisations and users such as Senior Australians participating in the digital

1 European Commission Final Report Executive Summary "New Challenges to Data Protection" issued January 20, 2010 available at http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm

economy require some guidance and expert support to effectively discharge their information security obligations.

This position is consistent with the introduction of a regulatory model to assist in addressing the market failures suggested in support of the preceding submission.

The AISA advocates 'outcome based' expectations and not a technical specification.

The above recommendation is also consistent with the recommendation from the Australian Law Reform Commission Report on its review of the Privacy Act 1988 (Cth)[2] that the then Office of the Privacy Commissioner should develop and publish guidance on the meaning of the term 'reasonable steps' and on the implementation of privacy-enhancing measures to support compliance[3]. This recommendation was accepted by the Government in its first stage response.[4]

It is not the position of this submission that the OPC or the OAIC should have regulatory oversight for information security issues – particularly in view of our subsequent recommendation that information security is a broader goal that information privacy. Protection should be extended to all types of data (not just personal data as required in the Privacy Act). However, we would like to draw the Joint Select Committee's attention to the fact that the absence of this guidance has been recognised and accepted as an issue and that it is timely to consider how it should be best addressed.

Supports: Government Cyber Security Strategy Objective 2

There is a Cyber Security Skills Crisis in Australia

Recommendation:

The Government should require all Universities and colleges to include and integrate security principles and skills in their IT courses; both within existing modules and as standalone electives.

Rationale: Security is often misunderstood by business, and is frequently left to technologists to deploy tactical solutions. Moreover, this speciality is seen as a separate skillset and the majority of the ICT workforce doesn't know enough about incorporating security into ICT life cycles, roles and responsibilities and linking business objectives to ICT operations. Security should be an integral part of all information systems procurement, design and development and not perceived purely as a separate discipline. This is unlikely to happen until security is a part of the training for all ICT professionals, and endorsed by business management.

Supports: Government Cyber Security Strategy Objectives 1, 2 & 3

[2] ALRC Report 108: For Your Information: Australian Privacy Law and Practice http://www.austlii.edu.au/au/other/alrc/publications/reports/108/

[3] ALRC Report 108 Volume 2 at p950

[4] Australian Government "Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice'* October 2009 at 62. Available for download at http://www.dpmc.gov.au/privacy/reforms.cfm

Data Breach Notification Legislation Should be Introduced

Recommendation:

The Australian Parliament should legislate to require notification to information stakeholders potentially impacted by security breaches.

Rationale: Based on experiences in parts of the USA and within the Payment Card Industry, the threat and cost (both financial and the impact on brand and reputation) of potential stakeholder notifications appears to have led service providers to improve security levels.

AISA submits that:

- Data breach notification regulations should be introduced incorporating the lessons learned from the USA and EU experiences.
- Any data breach notification scheme be part of a broader and "more responsive" regulatory approach supporting information security

Supports: Government Cyber Security Strategy Objectives 1, 2 & 3

Support of Standards Development

Recommendation:

The Government should provide additional resources for Standards Australia to participate in international efforts to develop better security standards. Support of other de facto standards bodies should also be considered – such as the efforts by the Open Web Application Security Project (OWASP) in the web application security domain.

Furthermore, the core principles (and mandates) of the standards should be set out in a technology agnostic manner that maintains the high-level goals despite the changes in the underlying technologies.

Rationale: There are 90 security related standards under development in the ISO and ITU organisations. It is difficult to represent Australia's interests in this large development effort with a volunteer committee.

Supports: Government Cyber Security Strategy 1, 2 & 3

There is a need for better Prevention and Early Detection of Incidents

Recommendation:

The frequency and severity of incidents is too high for the deterrent effect of law enforcement to decisively reduce the impact of cyber security incidents on the Australian community.

The Government should plan or require Australian organisations processing, storing or outsourcing handling of information to significantly improve security levels. The objective should be to reduce the frequency and impact of security breaches.

Rationale: The number and impact of incidents are alarming, particularly when information security professionals report that the publicly known incidents are only "the tip of the iceberg".

A combination of both prevention and early detection of security breaches must be incorporated into the management of each online service. The aim is to reduce the number and impact of security breaches.

The Government's Cyber-security discussion paper floated an option of increasing the resources available to law enforcement bodies. While that is a worthwhile endeavour, the major aspect to reducing the number and impact of security breaches is better protection of online services and the earlier detection of incidents.

Supports: Government Cyber Security Strategy Objectives 1, 2

The Lack of Cyber Security Awareness is not just in SMEs

Recommendation:

Cyber Security awareness programs should be targeted to different sizes and types of public and private organisations.

Rationale: A lack either of cyber security awareness or willingness to mitigate the risks exists in organisations large and small and is not limited just to SMEs. The majority of home users, as well as corporate and government employees, are often unaware of the threats they face when using online resources.

The most notable public security breaches in 2011 have either been triggered by or exacerbated by insufficient security awareness of staff (for example: the Sony Play Station Network and "RSA Security" security breaches).

Supports: Government Cyber Security Strategy Objectives 1, 2 & 3

Cyber-related Issues Indicate Offline weaknesses

Position: Many organisations need to improve offline security practices in the light of "Identity Fraud" and the compromise of "online data".

Rationale: Only partial responsibility can be attributed to the security of the online environment, and some responsibility should be attributed to the lax authentication and identification processes relied upon by both offline and online service providers.

Some security practices (such as authenticating people via their mother's maiden name) have been outdated by the rise of "social media" and online databases. The ubiquitous computer network connections of all businesses, not for profit organisations and many governments, many of them experiencing cyber intrusions, has reduced the effectiveness of controls designed in the "pre-online" era. Many organisations need to reassess the effectiveness of security precautions in their business processes.

Where the costs corresponding to poor security practices are externalised, there is a role for the Government to set or co-ordinate the establishment of benchmarks of acceptable practices.

Supports: Government Cyber Security Strategy Objectives 2 & 3

Other AISA Comments

Senior Citizens and Home Users:

The increasing threats to home users, associated with the compromise of their computers, cannot be solved solely by the current strategies and technologies (education and anti-virus) and a new approach is required.

This may involve upstream mitigation (for example at the ISP level), revised education or partnership with software providers (such as free provision of security software by some banks).

Enforcement of Existing Legislation

Although this submission supports regulatory (or co-regulatory) measures to assist in providing incentives for improved information security practices, we also submit that the Government should support increased enforcement of existing regulation to the same effect.

As an example, the Government has indicated that it believes that there is adequate existing protection under current consumer protection law in relation to the sale of insecure IT products.[5] However, to date there has been no action by the ACCC or its successor supporting enforcement of any breach of the Australian Consumer Law based on information security failure. By contrast, the Federal Trade Commission in the United States has taken action in over 29 different cases over the last 10 years for either breach of privacy or "false and deceptive conduct" relating to the adequacy of

[5] See the Government Response to recommendation 26 in the House of Representatives Standing Committee on Communications' Cybercrime report that the Australian consumer law be amended to provide a cause of action for compensation against a manufacturer who releases an IT product onto the Australian market with known vulnerabilities

information security controls, pursuant to a provision of the Federal Trade Commission Act which is in almost identical terms to the provision in the Australian Consumer Law. The presence of the FTC as an enforcement authority has added significantly to the general acceptance of a duty of care in regard to provision of reasonable security measures by American organisations.

While we accept that there may in some cases already be legislative protections in place, without those being properly enforced, they act a little incentive to support improved information protection.

In addition, there has been little movement on some important information security issues that have been long identified as requiring resolution. For example, the Cybercrime report argued for increased powers for the Australian Communications and Media Authority to direct service providers to remove malicious content. The Government responded that this should be the responsibility of its new agency CERT Australia and that "any further regulation" should await "a holistic approach" for Australian individuals and businesses. To date, there has been no further formal advances to address this major source of security weaknesses.

AISA submits that where the Government wishes to rely on existing legal and regulatory instruments, it should adequately resource and empower the relevant regulatory authorities to act. This action should be expedited.

Trusted Information Sharing

The reluctance to report or share information on data breaches is evidenced by the responses to the AISA survey – with a large majority responding that data breaches were under reported. Without proper information sharing, the size and extent of the information security problem in Australia remains difficult to determine – and hard to address.

Another problem for information security from the inadequacy of information sharing is the information asymmetry this causes, particularly for those without any links to experts in the field. Although the Attorney General's Department has worked on developing the Trusted Information Sharing Network (TISN) and other programs in regard to critical infrastructure protection – some of the organisations most needing to improve their security did not actively participate. Nor is it clear that the information sharing model should be limited to the particular industry sectors identified as part of the critical infrastructure – particularly given the interdependencies across all connected entities forming part of the digital economy.

We submit:

1. The Government should revisit and enhance its information sharing scheme for the business and not for profit sectors
2. Consideration be given to any mechanisms required to develop trusted information sharing – such as indemnities and confidentiality provisions

Contacts and Further Information

Gary Gaskell
AISA Information Security Policy Committee
gary.gaskell@aisa.org.au

Benn Dullard
AISA National Director
benn.dullard@aisa.org.au