Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

7 January 2013

Office of the Australian Information Commissioner
G.P.O Box 5218
Sydney NSW 2001
consultation@oaic.gov.au

Dear Sir / Madam

Re: OAIC Guide to Information Security
Consultation Draft – December 2012

The Australian Privacy Foundation's Submission on this matter is attached.

Thank you for your consideration.

Yours sincerely

Vice-Chair, for the Board of the APF
0414 731 249, vicechair1@privacy.org.au

Australian Privacy Foundation

OAIC Guide to Information Security
Consultation Draft – December 2012

SUBMISSION

4 January 2013

Introduction

The APF's Policy Statement on Information Security forms an integral part of this Submission. A copy is attached and the original is at http://www.privacy.org.au/Papers/PS-Secy.html.

Briefly, the APF argues that all organisations have moral and legal obligations to apply the available knowledge about information security in order to ensure privacy protection. Obligations are identified in the area of security governance and security safeguards.

The Board is generally quite positive about the current draft of the OAIC Guide.

The APF submits, however, that it falls short of the current need on several key aspects, and that it will be of far greater value to organisations and individuals alike if it is enhanced in the following ways.

More Direct Guidance Is Needed

On page, 1, the document declares as a Key Message that "This guide provides guidance on information security, specifically the reasonable steps entities are required to take ...".

But in fact it does not require trhat any steps be taken. The key passages on p. 14 merely say "Appropriate security safeguards and measures for personal information need to be considered ... This could include [list of safeguards] ... This section outlines examples ... ".

It is untenable for any organisation to not provide minimum levels of safeguards for data of value, including personal data. It is essential that the OAIC communicate that to organisations.

APF submits that:

(1) The document needs to be revised to provide more direct guidance relating to the minimum safeguards that are required, together with references to documents that contain more detailed advice on specific security safeguards.

(2) The document needs to be revised to make very clear that privacy-sensitive personal information must be subject to additional safeguards, well beyond the minimum safeguards, that address risks that arise in the particular context.

Direct Statements Are Needed About Enforcement

The document contains very little about enforcement actions and penalties.

The public understands the benefits of adopting a primarily positive approach, encouraging good organisational practices, and guiding organisations towards them.

However, the public also knows that many organisations fail to respond to positive approaches. The public accordingly expects the OAIC to exercise all enforcement powers at its disposal, and to put organisations on notice that it does so. The document fails to communicate a forceful message to organisations about enforcement of the requirements. Worse, nothing in the document provides the reader with any confidence that the OAIC will take the action necessary to achieve change.

The APF submits that:

(3) The document needs to be revised to project the following additional Key Messages, and provide supporting information:

- security safeguards are a mandatory requirement of the law, not optional;
- organisations that fail to implement the basic set of well-known safeguards for personal data are *prima facie* in breach of the Privacy Act, and are subject to enforcement actions; and
- organisations that handle privacy-sensitive personal information but fail to implement additional safeguards appropriate to the risks involved, are in breach of the Privacy Act, and are subject to enforcement actions.

Complementary Activities Are Needed

The Guide has existed since 2001. Yet there are continual breaches of the law. It is clear that, by itself, even an updated Guide is not sufficient to achieve the necessary substantial improvements in organisational practices.

The APF submits that:

(4) The OAIC needs to reinforce the messages in the Guide with complementary activities, including:

- reminders through industry associations and the media that inadequate personal data security has adverse consequences, including:
  - breaches of the Privacy Act, harm to individuals, and consequential enforcement actions by the OAIC and the courts, including financial penalties
  - breaches of other laws, and consequential enforcement actions by other regulatory agencies, including financial penalties
  - reputational harm among the general public and through the media
- reminders through industry associations and the media that all organisations must implement well-known information security safeguards
- statements through industry associations, professional associations and the media that audits need to include, as a core focus, compliance with privacy laws and norms
- much more active use of all processes and sanctions available to the Commissioner, including 'naming and shaming' of organisations that fall short of the requirements
- public warnings of the likelihood of greatly increased public concern arising from such factors as continual data breaches, abuse of personal data by social media services, the risks involved in cloud computing, and the looming threat of 'big data'

Australian Privacy Foundation

Information Security

APF Policy Statement on Information Security

Organisations hold a great deal of personal data. All of it is at least to some degree sensitive, and some of it highly so. Inappropriate handling of personal data represents a threat variously to the safety, wellbeing and peace of mind of the people it relates to. Primary privacy concerns are in the areas of unauthorised use and disclosure of data, with other issues including loss of data and threats to data integrity. Personal data needs the same level of care as financial information.

The privacy interest shares a great deal of common ground with organisations' own needs for protection of data of financial and competitive value, with commercial confidentiality, and with government and national sovereignty desires for the protection of sensitive data.

Information and Information Technology Security are well-established fields of professional endeavour, supported by a substantial array of products and services and a busy industry.

Organisations have moral and legal obligations to apply the available knowledge and to thereby ensure privacy protection. This applies to:

- all government agencies at federal, State and Territory, and local levels
- large and medium-sized business enterprises and not-for-profit organisations
- small business enterprises and not-for-profit organisations that handle personal data
- service-providers, including to small organisations and consumers, where the services provided involve personal data that is under the control of the service-provider's customer (particularly personal health records and credit-card data, but also, for example, records of goods and services purchased, social media, dating services and business-contact lists)

The following, specific obligations exist, must be recognised by organisations throughout the public and private sectors, and must be enforced by regulatory agencies.

Security Governance

All organisations have obligations to:

- conduct Information Security Risk Assessment (SRA), which identifies and evaluates threats, vulnerabilities and potential harm, including a focus on risks to the privacy of individuals whose data the organisation handles
- establish an Information Security Risk Management Plan (SRMP), which specifies the information security safeguards that are to be established and maintained, including safeguards against risks to the privacy of individuals whose data the organisation handles
- establish and maintain business processes to ensure the implementation, maintenance, review and audit of those information security safeguards

Resources to guide and support these activities include:

- ISO/IEC 27005:2008 'Information technology – Security techniques – Information security risk management'
- NIST (2012) 'Guide for Conducting Risk Assessments' US National Institute for Standards and Technology, SP 800-30 Rev. 1 Sept. 2012, pp. 23-36

Security Safeguards

All organisations have obligations to establish and maintain a sufficiently comprehensive set of information security safeguards in the following areas, commensurate with the sensitivity of the data:

- Physical Access Controls, such as locks, and authorisation processes for entry to premises
- Logical Access Controls, such as user account management, privilege assignment, and user authentication
- Data Protection in Transit, such as channel encryption and authentication of devices
- Data Protection in Storage, such as access logs, backup and recovery procedures, and encryption
- Perimeter Security, such as firewalls, malware detection, and intrusion detection
- Internal Security, such as vulnerability testing, patch management, software whitelisting, malware detection, and automated detection of security incidents
- Software Security, such as pre-release testing, change control and configuration management
- Organisational Measures, such as staff training, staff supervision, separation of duties, security incident management, log monitoring and audits
- Legal Measures, such as terms of use for employees, and terms of contract for suppliers
- Data Breach Notification Processes
- Formal Audit of data protection measures

Resources to guide and support the design and implementation of effective safeguards include:

- Andress J. (2011) 'The Basics of Information Security' Syngress, www.syngress.com, 208 pp.
- Clarke R. (2013) 'Information Security for Small and Medium-Sized Organisations' Xamax Consultancy Pty Ltd, 2013
- PCI-DSS (2010) 'Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures' Version 2.0, PCI Security Standards Council, October 2010
- ISM (2012) 'Information Security Manual – Controls' Defence Signals Directorate, 2012
- ISO/IEC 27001:2006 'Information technology — Security techniques – Information security management systems – Requirements', Annex A, pp. 13-29
- Goodrich M. & Tamassia R. (2011) 'Introduction to Computer Security' Addison-Wesley, 2011, 576 pp.

Sanctions

All organisations, and individuals within organisations, must be subject to sanctions where they fail to fulfil their information security obligations.

Sanctions must exist, and must be applied, at all of the following levels:

- civil liability by organisations
- civil liability by directors
- staff disciplinary action, up to and including dismissal in serious cases
- criminal liability for serious and repeated cases

Created: 20 December 2012 - Last Amended: 4 January 2013 by Roger Clarke - Site Last Verified: 11 January 2009