XAMAX
Consultancy
78 Sidaway St Chapman ACT 2611
AUSTRALIA
Tel: +61 2 6288 1472, 6288 6916
Email: Roger.Clarke@xamax.com.au
Web: http://www.xamax.com.au/

4 January 2013

Mr J. McMillan
The Information Commissioner
Office of the Australian Information Commissioner

Dear John

Re: Consultation Process re
OAIC Guide to Information Security

This Submission in relation to the above matter has been prepared in my role as an eBusiness consultant. (In addition, I'm aware of the Australian Privacy Foundation's Submission, and have participated in its preparation). This document is open for publication.

Given a somewhat tighter focus, the OAIC's Guide could be highly valuable to organisations.

Information is central to the operations of almost all business enterprises, government agencies and non-profit organisations. Computers, software and networks are inherently insecure. And threats to information security are substantial, and increasing.

As a result, every organisation needs to have at least a minimum set of information security safeguards in place – for its own sake, to protect the interests of the organisations it deals with, and to protect the personal data of its staff and other individuals whose data it holds.

I submit that the OAIC's Guide should declare a minimum set of safeguards; and then stress the need for risk analysis, and, depending on the findings, additional risk management measures above and beyond that minimum. Such a 'minimum safeguards' section would be of greatest use to organisations if it were expressed in a self-contained Appendix to the Guide.

By way of example, I attach a two-page brochure that proposes a set of safeguards that my IT security assignments lead me to believe is the minimum acceptable. (My intention is that a version of this document be distributed through various channels, possibly bearing the Xamax logo, but possibly not). Other consultants might prioritise the safeguards a little differently.

Yours sincerely

Roger Clarke, Director
Also: Visiting Professor in Cyberspace Law & Policy, UNSW
Visiting Professor in Computer Science, ANU

ACN: 002 360 456 ABN: 73 270 889 397

Information Security for Small and Medium-Sized Organisations

© Xamax Consultancy Pty Ltd
Version 1.0 of 4 January 2013

http://www.xamax.com.au/EC/ISInfo.pdf

Every organisation relies on information technology (IT) to some extent, and every organisation stores information of value. All IT contains weaknesses, and is vulnerable to acts of gods, accidents and attacks. Many laws and regulations require organisations to take appropriate care with information. So every organisation needs to invest at least some minimum amount of time, effort and money in information security.

Large organisations have specialist staff to manage these issues, but most small and even medium-sized organisations have to manage security along with all of their other activities.

This document briefly outlines what your organisation needs to do, in order to address information security. It first summarises the absolute-minimum safeguards – those that your organisation cannot afford not to have. It then outlines the additional measures involved in a more comprehensive approach, and the process whereby you can evaluate the extent to which such greater investment is warranted.

The Absolute-Minimum Information Security Safeguards (TAMISS)

1. **PHYSICAL SAFEGUARDS** for all processors, storage and access devices.
2. **ACCESS CONTROL**, including user-accounts allocated to individuals for their, and only their, personal use, with privileges limited to only the software, functions and data that are required for that person's work; and tight control over super-user accounts, to reduce the opportunity for abuse of access privileges.
3. **MALWARE DETECTION AND ERADICATION** on all inbound traffic, and periodically on all storage devices. (Malware includes viruses, worms, spyware, etc.).
4. **PATCHING PROCEDURES**, to ensure the frequent application of all security-relevant updates and patches to all systems software and application software.
5. **FIREWALLS**, in order to limit the scope for unauthorised individuals to gain access to and control over devices within the organisation.
6. **INCIDENT MANAGEMENT PROCESSES**, to receive reports, and ensure that they are addressed.
7. **LOGGING** of all changes and accesses to data and software, periodic audit of the logs, and the registration of anomalies with the incident management process.
8. **BACKUP AND RECOVERY** plans, procedures and training, and periodic exercise of the recovery procedures.
9. **TRAINING**, with clear instructions to staff and contractors concerning the transmission and storage of data, including access to it remotely and from mobile devices, reminders of their responsibilities, obligations expressed in the terms of employment and contract, and disciplinary processes to deal with malbehaviour by staff and contractors.
10. **RESPONSIBILITY** for the security of data by a sufficiently senior staff-member, who has the authority and resources to fulfil that responsibility.

Security Safeguards Needed for More Sensitive Data

Many organisations hold information that is particularly sensitive, due to its value for industrial espionage, commercial confidentiality, personal privacy, government sensitivities, or national sovereignty or diplomatic concerns. Security measures need to be commensurate with the sensitivity of the information being protected. Which of the following additional safeguards need to be implemented depends on the circumstances.

11. **DATA COMMUNICATIONS ENCRYPTION**, to protect information in transit.
12. **DATA STORAGE ENCRYPTION**, to protect information in storage, particularly in high-risk contexts such as portables, handhelds and thumbdrives.
13. **VULNERABILITY TESTING** of all devices, on a periodic basis, to identify known weaknesses that have not yet been addressed.
14. **STANDARD OPERATING ENVIRONMENTS**, to ensure that safeguards are implemented in a reliable and efficient manner.
15. **APPLICATION WHITELISTING**, to ensure that the organisation's devices only run approved software.
16. **DEVICE AUTHENTICATION AND AUTHORISATION**, to ensure that only approved devices can connect to the organisation's networks.
17. **USE OF A VIRTUAL PRIVATE NETWORK** for access from remote locations.
18. **INTRUSION DETECTION AND PREVENTION**, to identify attempts to break into the organisation's devices and enable countermeasures to be planned.
19. **USER AUTHENTICATION** utilising means that are stronger than passwords.
20. **FIREWALL CONFIGURATIONS**, to prevent inappropriate outbound traffic.

Risk Assessment and Risk Management Processes

Your organisation needs to know whether any of the more advanced safeguards are needed, and, if so, which of them are the appropriate ones to invest in. The way to find this out is to conduct an assessment of the risks associated with the information that your organisation holds, and then develop a plan for managing those risks.

A Risk Assessment identifies, analyses and evaluates the risks to information security that arise in the organisation's current context. The analysis focusses on the organisation's assets, the natural, accidental and intentional threats to them, the vulnerabilities that those threats may impinge on, the harm that may result, and the existing safeguards already in place.

A Risk Management Plan identifies the specific safeguards that are to be deployed, and the processes whereby they are to be implemented, tested, and reviewed.

Next Steps

An experienced business analyst should be able to assist your organisation in conducting an Information Security Risk Assessment. It is likely, however, that specialist skills will need to be contracted in to establish the safeguards, and to review and adjust them from time to time.

Resources

Security specialists know where to find documents about specific security processes and safeguards. The following are general guidance documents intended for managers and non-specialist professionals.

Andress J. (2011) 'The Basics of Information Security' Syngress, www.syngress.com, 208 pp.

DBCDE (2011) 'Stay Smart Online – Small & Medium Business' Dept of Broadband Communications and the Digital Economy, 2011, at http://www.staysmartonline.gov.au/small_and_medium_business

ISO 27005:2011 'Information technology—Security techniques—Information security risk management' International Standards Organisation, 2011, especially pp. 7-17 and 33-49

NIST (2012) 'Guide for Conducting Risk Assessments' US National Institute for Standards and Technology, SP 800-30 Rev. 1 Sept. 2012, pp. 23-36

PCI-DSS (2010) 'Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures' Version 2.0, PCI Security Standards Council LLC, October 2010, at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

RACGP (2011) 'Computer and Information Security Standards' Royal Australian College of General Practitioners, October 2011, at http://www.racgp.org.au/your-practice/standards/ciss/

VAG (2004) 'Managing Internet Security' Auditor-General of Victoria, 2004, at http://www.articsoft.com/whitepapers/internet_security.pdf