Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:11
Received 9 May 2003
Mr Mark Bezzina
Director - Business Standards Management and Business Communication, IT and eCommerce
Standards Australia International Ltd
286 Sussex Street
SYDNEY NSW 2000
☎02 8206 6730
E-mail:

Standards Australia

Standards Australia International Limited is an independent, non-government organisation that is recognised as the peak standards writing body in Australia through a memorandum of understanding with the Commonwealth Government. Standards Australia aims to excel in meeting national needs for contemporary, internationally aligned standards and related services, which enhance the nation's economic efficiency and international competitiveness, and fulfil the community's demand for a safe and sustainable environment. We represent Australia's interest in the two peak International Standards Organisations, ISO and IEC, representing Australian industry's perspective in an international arena.

Standards Australia has a rich history of providing documents to the market based on an inclusive, transparent and consensus based methodology. Standards are written by volunteers participating in committees; and reflect the needs of industry, producing relevant, workable documents. We work and consult with a wide spectrum of interest from the community to publish consensus-based standards that are practical and contemporary in nature. The committee structure has provided Standards Australia with an abundance of knowledge and ties to professional organisations that has spanned decades. Standards Australia has an ongoing and involved relationship with a variety of government agencies through committee involvement.

Standards Australia is at the forefront of development in information and knowledge management and technology. The attached document provides details of existing standards in information security management, metadata, risk management, current development work in the areas of IT governance and management, IT forensics and a proposed project to develop an Australian ebXML Registry. These areas of standardisation provide a basis for information protection, management, storage and transmission that is relevant to all Commonwealth agencies.

Standards Australia appreciates the value of Commonwealth Government representation on its committees, and supports the involvement of agencies in all its information technology committees. We welcome suggestions for development of future standards in areas where particular needs are identified, and are willing to engage in new work, including the development of government specific handbooks, to support the management and integrity of electronic information in the Commonwealth.

Standards Australia submission to the Parliamentary Joint Committee on the Australian Crime Commission

Information security management standards have become an integral and essential element to organisations in the present business environment. Standards Australia is acutely aware of trends in the market place and the changing needs of industry. Accordingly, we have increased the profile and are constantly monitoring and developing standards nationally and internationally standards in the information security management area. Current Australian Standards allow for a management system to be put in place along with a governance structure allowing for the efficient treatment and prevention of security incidents.

The documents detailed below will assist law enforcement agencies and other government bodies involved in the reduction of cybercrime activities by ensuring baseline procedures are put in place for the handling of incidents related to:

1) Child pornography and associated paedophile activity

2) Banking, including credit card fraud and money laundering; and

3) Threats to national critical infrastructure.

Standards Australia has a very keen interest in working closely with any government committee established to address matters of critical infrastructure protection and banking security. We welcome an opportunity to be able to assist in the development of handbooks and guides for consumers, government agencies and industry to use to ensure the safety and welfare of all Australians.

Information Security Management Standards

Information security management standards have become an integral and essential element to organisations in the present business environment. Standards Australia is acutely aware of trends in the market place and the changing needs of industry. Accordingly, we have increased the profile and are constantly monitoring standards in the information security management area.

AS/NZS ISO/IEC 17799:2001, *Information technology - Code of practice for information security management*

This comprehensive Standard provides recommendations for information security management for those who are responsible for initiating, implementing or maintaining security in their organsiationorganisation. It provides a common basis for developing effective security management practice and to provide confidence in inter-organsiationalorganisational dealings.

The standard addresesaddresses areas such as:

- Organisational security
- Asset classification and control
- Personnel Security
- Physical and environmental security

- Communications and operations management
- Access Control
- Systems development and maintenance
- Business continuity management
- Compliance

AS/NZS 7799.2:2003, *Information Security Management Part 2: Specification for information security management systems*

This standard specifies the requirements for establishing, implementing and documenting information security management systems (ISMSs) and security for individual organisations. It forms the basis for an assessment of the ISMS of organisation, and may be used as a foundation for a formal certification scheme. It covers:

- ISMS requirements – such as implementation and documentation
- Detailed controls – such as security organisation and asset control.

This standard supercedessupersedes the previous version AS/NZS 7799.2:2000. The new version is backwards compatible with the previous version, but has been expanded and improved based on experience, especially in Europe, with the previous BS 7799.2:1999 version. The new version has had input not only from Australia, New Zealand and the UK, but also from Japan, Hong Kong, Malaysia, Singapore, India, United Arab Emirates, Netherlands, Sweden, Norway, and Germany.

Key features of the revision are:

- more comprehensive coverage of implementation, operation and review to complement the current emphasis on planning;
- increased flexibility, so that security management system requirements can be integrated into other management systems that an organization might have;
- Alignment with the 'Plan, Do, Check, Act' model used in other ISO management standards as shown in figure 1.

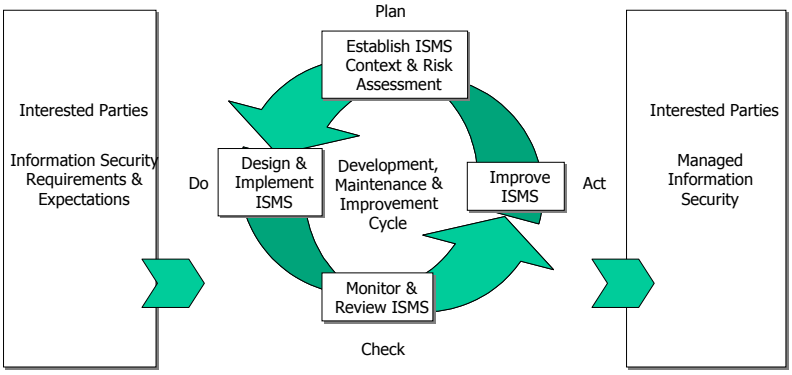

Figure 1: Model for Information Security Management Systems

A number of editorial improvements have also been made, notably that it is now much simpler to find the related control clauses in AS/NZS ISO/IEC 17799:2001 and AS/NZS 7799.2:2003. The revision will also include an appendix showing the relationship between clauses in the current and new versions of AS/NZS7799.2.

HB 231, *Information security risk management*

This handbook provides a generic guide to the establishment and implementation of a risk management process for information security risks. It serves as a reference point describing an information security risk management process for most situations in industry and commerce, and can be applied by a wide range of organisations. It covers the following topics:

- Risk Management framework, overview and process
- Documentation

HB 248, *Organisational experiences in implementing information security management systems*

This handbook provides an insight into how some of Australia's leading organisations have implemented Information Security Management Systems. Its objective is to assist organisations and individuals to develop their own approaches to the implementation of an Information Security management System. HB 248 includes input from the ANZ Bank, Telstra, LINK, BSI and many more. ITt includes information on:

- Key elements of ISMSs
- Australian Case Studies
- International Case Study

- Key elements of ISMSs
- Australian Case Studies
- International Case Study

Risk Management Standards

Risk management has become an integral component of contemporary business practises and Standards Australia has been in the forefront in producing risk management standards that are being utilised by organisation globally. These standards have provided a pragmatic and accessible methodology to implement risk management tools within organisations.

- AS/NZS 4360:1999 *Risk Management*

  Provides a generic guide for evaluating and implementing the risk management process, which involves establishing context, identification, analysis, evaluation, treatment, monitoring, review, consultation and communication. The standard can be applied at every stage in the life of an activity, function, project or asset generated by any public, private or community enterprise or group.

- HB 231:2000 *Information Security Risk Management Guidelines*

  Provides information on how to establish and implement a risk management process for information security risks.

Guidelines for the Management of IT Evidence

A working group has completed the preliminary draft on standardisation in the field of cyber forensics and evidence collection. The current business climate, where security issues have altered priorities and policies within organisations has precipitated the need to expand on standards in the IT security area. The document has been produced through extensive consultation with industry and government agencies.

Information security has been attracting much attention since the events of 11 September however it is very easy to focus on the wrong aspects of information security. The standards currently developed allow for a management system to be put in place along with a governance structure allowing for the efficient treatment and prevention of security incidents.

The documents detailed above will be able to assist law enforcement agencies and other government bodies involved in the reduction of cyber crime activities by ensuring baseline procedures are put in place for the handling of incidents related to:

4) Child pornography and associated paedophile activity

5) Banking, including credit card fraud and money laundering; and

6) Threats to national critical infrastructure.

Much of the criminal activity associated with the above mentioned areas occurs using digital technologies, it is important that information collected as evidence is obtained using proper means and is treated appropriately. Often evidence is collected however is not admissible in a court of law. The Guidelines for the Management of IT evidence provides a set of best practices for professionals in the field to collect and store information that may be called upon at a future date as evidence in a criminal or civil case in a court of law.

Electronic In the area of banking, Standards Australia has developed a multi part standard AS 2805 which covers all aspects of banking transactions. This includes security for ATM and EFT terminals to backend processing and transactions between banks. Though not mandated by law all major banks are using the standard in some form or another to secure their online transaction processing systems and other infrastructure.

Standards Australia has a very keen interest in working closely with any government committee established to address matters of critical infrastructure protection and banking security. We will welcome an opportunity to be able to assist in the development of handbooks and guides for consumers and the industry to use to ensure the safety and welfare of all Australians.

Banking Standards

In the area of banking, Standards Australia has developed a multi part standard AS 2805, which covers all aspects of banking transactions. This includes security for ATM and EFT terminals to backend processing and transactions between banks. Although not mandated by law, all major banks are using the standard in some form or another to secure their online transaction processing systems and other infrastructure.