CYBERWELLNESS PROFILE AUSTRALIA

BACKGROUND

Total Population: 22 919 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 83.00%
(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Cybercrime Legislation Amendment Act 2012

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- National Plan to Combat Cybercrime
- Australian Cybercrime Online Reporting Network
- Australian Communications and Media Authority (ACMA)
- Data breach notification
enforces the Spam Act.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

CERT Australia is the officially recognized national computer emergency response team (CERT). In addition the Cyber Security Operations Centre (CSOC) is also responsible for coordinating and assisting operational responses to cyber events of national importance across government and systems of national importance.

1.2.2 STANDARDS

The ASD is responsible for producing ICT security policy and standards for the government and publishes these in the Australian Government Information Security Manual.

1.2.3 CERTIFICATION

The Emanation Security Program is responsible for the framework for certification and accreditation of national agencies and public sector professionals, and sets out the requirements for government and industry agencies to be formally recognised by the national authority. ASD conducts emanation security practices to national standards.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Australia has officially recognized the National Plan to Combat Cybercrime and the Cyber Security Strategy as the national strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The national governance roadmap for cybersecurity is elaborated in the National Security Information Environment Roadmap: 2020 Vision.

1.3.3 RESPONSIBLE AGENCY

The following are the officially recognized agencies responsible for cybersecurity in Australia:

- The Cyber Policy and Intelligence Division
- The Attorney-General's Department

- The Department of Prime Minister and Cabinet   - The Australian Signals Directorate.

1.3.4 NATIONAL BENCHMARKING

In Australia the Federal Government entities subject to the Public Governance, Performance and Accountability Act 2013 participate in annual benchmarking of their ICT activities.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Currently Australia does not have any national or sector-specific recognized body or framework responsible for Research and development (R&D) of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

The following programs have been put in place fostering educational and professional programs for raising awareness, higher education:

- Cybersmart   - Stay Smart Online   - Budd:e Cybersecurity builder

1.4.3 PROFESSIONAL CERTIFICATION

Australia does not have a recognized national or sector-specific body for certifying professionals in cybersecurity. Currently there is no record showing the number of public sector professionals who are certified in the area of cybersecurity.

1.4.4 AGENCY CERTIFICATION

In Australia there is no recognized national or sector-specific body for certifying agencies in the area of cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Australia has officially recognized the following partnerships:
- Statement of Intent regarding the Cooperation on Cybersecurity and Cyber Incident Response between the United States Department of Homeland Security (DHS) and the Attorney-General's Department (AGD) of the Commonwealth of Australia.
- CERT Australia has direct working relationships and a range of bilateral and multilateral agreements with government and business computer emergency response teams around the world.

1.5.2 INTRA-AGENCY COOPERATION

Through the Govdex and Govshare platforms, agencies are encouraged and supported to share knowledge, skills, and resources in the pursuit of more effective, efficient and innovative solutions. These are the nationally recognized platforms for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Trusted Information Sharing Network (TISN) is the framework for sharing cybersecurity assets between the public and private sectors in Australia.

1.5.4 INTERNATIONAL COOPERATION

Australia participates in the following:
- UN GGE   - ASEAN
CERT Australia is a member of APCERT and FIRST.

2   CHILD ONLINE PROTECTION

2.1   NATIONAL LEGISLATION
Specific legislation on child online protection has been enacted through the following instrument:
-Divisions 273 and 474 (subdivisions D-F) of the Criminal code.

2.2   UN CONVENTION AND PROTOCOL
Australia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Australia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3   INSTITUTIONAL SUPPORT
The Australian Communications and Media Authority ACMA and Stay smart online are the institutions responsible for child online protection.

2.4   REPORTING MECHANISM
Inappropriate and offensive content can be reported directly to the CERT Australia on the number: 1300 172 499 (24 hours) and by the e-mail info@cert.gov.au. Also online content complaints can be directed to ACMA.