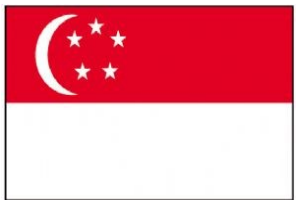

CYBERWELLNESS PROFILE SINGAPORE

BACKGROUND

Total Population: 5 256 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 73.00%
(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:
- Computer Misuse and Cybersecurity Act (Chapter 50A)

1.1.2 REGULATION AND COMPLIANCE

"Instruction Manual (IM) 8" specifies government policies, standards, regulations and codes of practice for IT security implemented by government agencies, that private vendors serving the government would also need to comply with. All IMs are mandatory for compliance by government agencies and subject to regular audit and assessment for enforcement purposes.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Singapore has an officially recognized national CIRT known as SingCERT. For the Government sector, the Government IT Security Incident Response (GITSIR) team co-ordinates with government agencies to perform investigations and supports agencies' response to the incident.

1.2.2 STANDARDS

Internationally recognised cybersecurity standards (such as ISO27000 series) are referenced in the development of Government security policies and standards. For the Telecommunications sector, internationally recognised cyber security standards (such as ISO27011) were referenced in the development of the Secure and Resilient Internet Infrastructure Code of Practice.

1.2.3 CERTIFICATION

Cybersecurity professionals are encouraged to obtain international certifications such as CISSP and the SANS series of certification. IDA's Critical Infocomm Technology Resource Programme (CITREP) provides support to offset the cost for people taking such certifications.
The Association of Information Security Professionals (AISP) aims to transform Infocomm security (IS) into a distinguished profession, with a recognised body, qualifications, established career paths and career development programmes.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Singapore has an officially recognized National Cyber Security Masterplan 2018 to further secure Singapore's cyber environment. As regulator of the financial services industry, the Monetary Authority of Singapore (MAS) uses a number of regulatory instruments to regulate and shape the conduct of financial institutions. While IDA does not have privileged access to MAS's cybersecurity strategy for the financial services industry, the publicly available 'Technology Risk Management Guidelines' and the Circular No. SRD TR01/2011: Information Technology Outsourcing sets out the risk management principles and standards to guide financial institutions in managing technology and IT outsourcing risks, including those relating to cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

The National Cyber Security Masterplan 2018 launched to further secure Singapore's cyber environment and developed through a multi-agency effort led by IDA provides an overarching strategic direction to help Government and organisations in strengthening resilience against cyber threats.

1.3.3 RESPONSIBLE AGENCY

National Infocomm Security Committee is the national-level committee responsible for steering cybersecurity strategy in Singapore. Secretariat support is provided by Infocomm Development Authority.

1.3.4 NATIONAL BENCHMARKING

IDA's Infocomm Security Health Scorecard put in place to measure the level of security readiness, assesses the state of info-security health of government agencies in areas such as policies, standards, the security knowledge of public officers, as well as physical and environmental security. The scorecard is aimed at helping government agencies to improve their info-security strategies and processes.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

One of the research and development (R&D) themes under the National Cybersecurity R&D Programme is on 'cyberspace governance & policy research'. The Programme is currently undergoing grant call phase. iTrust is a multidisciplinary research centre located at the Singapore University of Technology and Design (SUTD), established collaboratively by SUTD and the Ministry of Defence, Singapore which focus is on cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

Singapore has recognized various types of awareness programs on cybersecurity, for the general public as well as for public and private sector employees.

- National Infocomm Competency Framework (NICF) launched in 2008 serves as a reference for companies to use in their HR management of ICT professionals. Individuals (students and professionals) can also leverage on the framework to plan for their skills upgrading and career development.

-Critical Infocomm Technology Resource Programme (CITREP) established by the Infocomm Development Authority of Singapore (IDA) has the objective to accelerate the development of emerging, critical and specialised infocomm skills to meet Singapore's infocomm manpower needs.

-Company-Led training and Centres of Attachment aims to develop graduates and professionals through on-job-training and mentorship opportunities by leveraging local or overseas industry and education partners. These programs with focus on emerging skills will provide locals with structured quality learning and better career progression for the locals.

-Association of Information Security Professionals (AISP) aims to promote and enhance the information security profession in Singapore.
-National Cyber Security Masterplan 2018 aims to raise the awareness and adoption of cyber security best practices among the Public, Private and People sectors.
-There is collaboration between National Research Foundation (NRF) and IDA for Post-Grad Scholarship in Cybersecurity.

1.4.3 PROFESSIONAL CERTIFICATION

Singapore does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Singapore Prison service (SPS) has been certified for ISO/IEC 27001:2005 (Management and Operations of Data Centre Infrastructure Services). ISO/IEC 27001:2005 is a risk based information security standard and it is a requirement for organizations to have in place a risk management process based on the Plan-Do-Check-Act" (PDCA), Deming cycle approach. As part of maintaining the ISMS certification, organization needs to perform continual review on their information security program and ensuring effectiveness of security controls
Government Agencies comply with IM8 standards and ISD's Green book which has incorporated good practices but it is not an internationally recognised standard.
"Instruction Manual (IM) 8" specifies government policies, standards, regulations and codes of practice for IT security implemented by government agencies, that private vendors serving the government would also need to comply with.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Singapore, through SingCERT, actively engages international counterparts through platforms such as:
-APCERT - FIRST -ASEAN CERT Incident Drill (ACID)
Singapore is also a participant in Japan-led TSUBAME Working Group and PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) Project.

1.5.2 INTRA-AGENCY COOPERATION

The National Infocomm Security Committee draws its members for senior ranks of relevant public sector stakeholders. NISC is a platform where national cybersecurity policies are deliberated, information is shared, and inter-agency action is coordinated.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Singapore has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector. Cybersecurity Awareness Alliance amalgamates efforts from its members by bringing together different strengths and resources, to build a culture of cybersecurity in Singapore and to promote and enhance awareness and adoption of essential infocomm security (IS) practices for the private and people sectors.

1.5.4 INTERNATIONAL COOPERATION

Singapore participated in the following cybersecurity activities:
- ASEAN CERT Incident Drill (ACID) -APCERT Incident Drill -ASEAN Japan Comms Check Drill
-APEC-TEL -ASEAN-Japan activities
SingCERT is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
-Sections 293 and 376E of the Criminal Code.
-Section 32 of the Films Act.
-Sections 11 and 12 of the Publications Act.

2.2 UN CONVENTION AND PROTOCOL

Singapore has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Singapore 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

Singapore Computer Emergency Response Team (SingCERT) does not provide specific information on child online protection.

2.4 REPORTING MECHANISM

The CERT (SingCERT) provides an email to report incident: cert@singcert.org.sg and a hotline: 6211-0911

DISCLAIMER: Please refer to http://www.itu.int/en/Pages/copyright.aspx
More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 12th August 2014