CYBERWELLNESS PROFILE THAILAND

BACKGROUND

Total Population: 69 892 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 28.94%
(data source: ITU Statistics 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Thailand has a specific legislation pertaining to cybercrime. It is mandated through the following legal instrument:
- Act on Computer Crime B.E.2550 (2007)

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:
- Act on Computer Crime B.E.2550 (2007)

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Thailand has an officially recognized and legally mandated government CSIRT (ThaiCERT).

1.2.2 STANDARDS

Through the Office of the National Security Council and the Ministry of Information and Communication Technology Thailand has an officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

The approved national certification and accreditation body in Thailand is the IT Crime Prevention and Suppression Bureau, Ministry of Information and Communication Technology, Thailand and ThaiCERT.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Thailand has an officially approved national and sector specific cybersecurity strategy and/or policy through the IT Crime Prevention and Suppression Bureau, Ministry of Information and Communication Technology, Thailand and ThaiCERT.

1.3.2 ROADMAP FOR GOVERNANCE

There is an officially recognized national or sector-specific governance roadmap for cybersecurity through the IT Crime Prevention and Suppression Bureau, Ministry of Information and Communication Technology, Thailand.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Information and Communication Technology is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap in Thailand.

1.3.4 NATIONAL BENCHMARKING

The Ministry of Information and Communication Technology is responsible for national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Thailand's Ministry of Information and Communication Technology is officially answerable for national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors is the Ministry of Information and Communication Technology, Thailand.

1.4.3 PROFESSIONAL CERTIFICATION

Ministry of Information and Communication Technology, Thailand is responsible for educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector.

1.4.4 AGENCY CERTIFICATION

There are certified government and public sector agencies certified under internationally recognized standards in cybersecurity in Thailand: the Ministry of Information and Communication Technology and the Electronic Transaction Development Agency.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Thailand does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

Thailand does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Thailand does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Thailand is a member of the ITU-IMPACT initiatives and has access to relevant cybersecurity services.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instruments:

- Thailand Penal Code (Section 287)
-Computer Crime Act (Section 16)

2.2 UN CONVENTION AND PROTOCOL

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

Thailand 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

Thailand has a Computer Emergency Response Team (ThaiCERT) but does not provide specific information on child online protection.

2.4 REPORTING MECHANISM

Thailand allows for computer incident report using the email: report@thaicert.or.th. ; the website provides keys to encrypt reports.
