



CYBERWELLNESS PROFILE PHILIPPINES



BACKGROUND

Total Population: 96 471 000

(data source: [United Nations Statistics Division](#), December 2012)

Internet users, percentage of population: 37.00%

(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 instruments:

- [Cyber Crime Prevention Act - RA 10175](#)

1.1.2 REGULATION AND COMPLIANCE

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

- [Data privacy Act of 2012 RA 10173](#)

- [Electronic Act of 2000 RA 8792](#)

- [Anti-Child Pornography Act of 2009 RA 9775](#)

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Philippines has an officially recognized national CERT ([PHCert](#)).

1.2.2 STANDARDS

Philippines has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through iGovPhil services which include a single sign-on facility, a Public Key Infrastructure for secured online transactions.

1.2.3 CERTIFICATION

Philippines does not have an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Philippine has an officially recognized national [cybersecurity plan 2005](#).

1.3.2 ROADMAP FOR GOVERNANCE

Philippines does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Philippines has officially recognized the following agencies responsible for implementing a national cybersecurity strategy, policy and roadmap:

- Cyber Crime Unit and Cyber Crime Unit

- Zamboanga City Zamboanga City

- Davao City Davao City

- Computer Forensic Labs Computer Forensic Labs

- General Santos City General Santos City

- DOST-ICTO Cyber Security Section

1.3.4 NATIONAL BENCHMARKING

DOST-ICTO Cyber Security Section is responsible for benchmarking and measuring cybersecurity development in Philippines.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Philippines does not have any officially recognized 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

Philippines has officially recognized through ISACA a sector-specific educational and professional training program 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. ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. It provides practical guidance and other effective tools for all enterprises that use information systems.

1.4.3 PROFESSIONAL CERTIFICATION

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

1.4.4 AGENCY CERTIFICATION

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.2 INTRA-AGENCY COOPERATION

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Philippines does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5.4 INTERNATIONAL COOPERATION

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

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

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

- [Articles 201 and 355](#) of the Criminal Code.
- [Section 4\(c\)\(1\)](#) of the Cybercrime Act.

2.2 UN CONVENTION AND PROTOCOL

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

Philippines 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

Philippines does not have an officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Philippines does not have any officially recognized agency that offers an avenue for the reporting of incidents related to child online protection.

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 23th October 2014