



CYBERWELLNESS PROFILE UNITED ARAB EMIRATES



BACKGROUND

Total Population:

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

Internet users, percentage of population: 88.00%

(data source: [ITU Statistics](#), December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

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

- [Federal Law by Decree No. 5 of 2012 regarding Cyber Crimes](#)
- The Federal Law No. (2) Of 2006 on the Prevention of Information Technology Crimes.

1.1.2 REGULATION AND COMPLIANCE

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

- [Federal Law No. \(1\) of 2006 on Electronic Commerce and Transactions](#).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

The UAE has an officially recognized national CIRT known as [aeCERT](#).

1.2.2 STANDARDS

There are no officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards in the UAE.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in the UAE.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

The UAE has officially recognised the [General Policy for the Telecommunications Sector](#) and the [Cabinet Resolution No. 21 of 2013 regarding Information Security Regulation in Government Entities](#) as the national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in the UAE.

1.3.3 RESPONSIBLE AGENCY

The Telecommunications Regulatory Authority ([TRA](#)) is the body responsible for the implementation of a national cybersecurity strategy and policy in the UAE.

1.3.4 NATIONAL BENCHMARKING

There is no national benching marking or referential to measure cybersecurity development in the UAE.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

[aeCERT](#) is the officially recognized national body responsible for research and analysis 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

[TRA](#) and the [aeCERT](#) launched its awareness campaign [Towards a Safe Cyber Culture](#) with Salim, a cyber-security advisor. The [aeCERT](#) is also responsible for Advisory, Education and Awareness.

1.4.3 PROFESSIONAL CERTIFICATION

There is a Certified Professional Statistics Database that holds this record of public sector professionals certified under the [aeCERT](#).

1.4.4 AGENCY CERTIFICATION

There is no information on any certified government and public sector agencies certified under internationally recognized standards in cybersecurity in the UAE.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

There is no information on any framework for sharing cybersecurity assets across borders with other nation states.

1.5.2 INTRA-AGENCY COOPERATION

There is no information on any framework for sharing cybersecurity assets within the public sector in the UAE.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no information on any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector in the UAE.

1.5.4 INTERNATIONAL COOPERATION

The UAE is a member of the [ITU-IMPACT](#) initiative and has access to relevant cybersecurity services.

The UAE participates in the following cybersecurity activities:

- [APWG](#) - [The Honeynet Project](#).

[aeCERT](#) 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 instrument:

- Article 12 of the prevention of Information Technology Crimes.

2.2 UN CONVENTION AND PROTOCOL

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

The UAE 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 [aeCERT](#) has no current project on child online protection. There is no information on any agency responsible for the online protection of children.

2.4 REPORTING MECHANISM

The website of [TRA](#) provides an online form for [complaints](#) and another one for [contacting](#) them. The [aeCERT](#) can be contacted by email: info@aecert.ae; the communication can be encrypted using the key available on the website.

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 19th February 2015