



CYBERWELLNESS PROFILE

EGYPT



BACKGROUND

Total Population: 83 958 000

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

Internet users, percentage of population: 49.56%

(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:

[-The Penal Code](#)

[-Intellectual Property Law](#)

[-Telecomm Act](#)

[-E-Signature Law](#)

[-Child Act](#)

1.1.2 REGULATION AND COMPLIANCE

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

[-E-Signature Regulation](#)

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Egypt has an officially recognized National CIRT ([EG-CERT](#)). EG-CERT has expanded to reach 26 cybersecurity professionals working in four departments: incident handling, cyber forensics, malware analysis and reverse engineering, and penetration testing. EG-CERT has moved to a separate facility and is currently upgrading its labs in the four key operational departments. Additional labs are being planned for mobile cyber security and Industrial control systems cyber security.

1.2.2 STANDARDS

Egypt is currently drafting an officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

Cybersecurity-based regulations for the banking sector are issued by the Central Bank of Egypt (CBE), in relation to internet banking and mobile money (www.cbe.org.eg); and by the [Egyptian Financial Supervisory Authority](#) (EFSA) in relation to electronic stock trading.

1.2.3 CERTIFICATION

The e-Signature Law requires ISO 27000 certification for (private sector) Digital Certificates Service Providers (CSPs). The ISO 27000 certification is a prerequisite for CSPs licensing by IT Industry Development Agency ([ITIDA](#)).

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

An joint expert group from Government and (private) Industry were commissioned by the Minister of Communications and Information Technology to prepare a Cybersecurity Strategic Business Plan (SBP) at the

national level. The 6 month effort resulted in an SBP that has become part of the national ICT strategic plan from 2014 to 2020.

1.3.2 ROADMAP FOR GOVERNANCE

A national committee headed by the minister of Communications and Information Technology with participation from key governmental stakeholders prepared a roadmap for cybersecurity governance and high level strategic policy and operational recommendations that was forwarded to the Cabinet of Ministers in September 2014.

1.3.3 RESPONSIBLE AGENCY

The [Ministry of Communications and Information Technology \(MCIT\)](#) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

EG-CERT participates regularly in regional and international cyber drills. EG-CERT successfully participated in (Asia Pacific - APCERT) cyber drill (2012 & 2013), (Organization of Islamic Countries - OIC-CERT) cyber drill (2012 & 2013), and ITU/Impact Arab region cyber drill (2012). In 2014, EG-CERT participated both in APCERT cyberdrills as well as the OIC-CERT cyberdrills.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The IT Academia Collaboration (ITAC) Program at ITIDA recognizes cybersecurity as a priority R&D domain. Since 2005, ITAC has provided several grants for cybersecurity related R&D projects carried out jointly by partners from the academic sector and ICT companies. ITAC R&D grants are valued between \$15K and \$280K each. (An example of the ITAC funded R&D cybersecurity related projects is a project that successfully developed a smart PKI token for e-signature.)

In addition, EG-CERT has on-going R&D activities in the area of cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

In 2009 and 2010, the [National Telecommunications Regulatory Authority](#) (NTRA) organized and sponsored an advanced cybersecurity training program for professionals, training 220 professionals in 38 organizations within the governmental/public sector, banking sector, education sector, as well as from ICT private sector companies (Telecom companies, mobile operators, CSPs, etc.). As a result, 179 of those professionals obtained international certificates from SANS.

In 2008, MCIT established a national Child Online Protection (COP) Committee, and launched a program called [Amanak](#) for public awareness, especially targeting youth, educators, and families. In 2013, the national COP Committee was given the mandate to develop a comprehensive national COP strategy.

1.4.3 PROFESSIONAL CERTIFICATION

Egypt has over 1000 certified professionals (public and private sector) with international certificates from SANS (through SANS-EGYPT) and EC Council (through 16 EC Council certified centers that are based and operating in Egypt).

1.4.4 AGENCY CERTIFICATION

Egypt has 17 entities certified under internationally recognized standards in cybersecurity precisely ISO/IEC 27001 certification in 2013.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Egypt has officially recognized partnerships with the following organizations:

- | | | |
|-----------------------------------|---|-------------------------------|
| -ITU | -OMAN CERT | -TUNISIA CERT |
| -FIRST | -CyberSecurity Malaysia | -Indian CERT |
| -South Korea KISA | -Uganda CERT | |

In addition to the listed partnerships, [EG CERT](#) has partnership with [US CERT](#) and Tanzania CERT ([TZ-CERT](#)).

1.5.2 INTRA-AGENCY COOPERATION

EG-CERT organizes workshops and disseminates cybersecurity related reports within the ICT sector, governmental sector, public sector, and with the banking and financial sectors.

1.5.3 PUBLIC SECTOR PARTNERSHIP

EG-CERT organizes workshops and disseminates cybersecurity related reports within the ICT sector, governmental sector, public sector, and with the banking and financial sectors.

1.5.4 INTERNATIONAL COOPERATION

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

Egypt is a member of the United Nations Group of Government Experts (UN GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security (Aug'12-Jun'13). The UN GGE is a high level group of 15 international experts who prepared a report that addresses emerging cybersecurity threats, forwarded to the UN General Assembly in Oct 2013.

The UNGGE report that Egyptian Expert participated in preparing (the only expert from Africa and Middle East) was adopted by United Nations' General Assembly in October/November 2013. A new UN GGE has been formed to follow up on the work of the 2012/13 UN GGE, and Egypt continues to be a member of that Group in 2014/15.

Egypt has led the efforts to establish and currently chairs the ITU's Council Working Group for Child Online Protection (CWG-COP) since 2010.

Egypt is a member of MERIDIAN conference since 2009.

Egypt is an observer of the **OECD's [Committee for Information, Computer and Communications Policy \(ICCP\)](#)**, including the working party on Information Security and Privacy (WPISP).

EG-CERT is a full member of [FIRST](#) (2012), has participated in its annual conference since 2009, and has served on the program committee of the annual FIRST Conference in 2012 and 2013.

EG-CERT is a member of the Organization of Islamic Countries-CERT (OIC-CERT), and has participated in OIC-CERT annual general meeting since 2009.

NTRA (EG-CERT) hosted an ITU Arab Regional cybersecurity Forum attended by over 120 professionals from 8 countries, in Dec 2011, and an Egypt-US R&D cybersecurity Workshop attended by over 200 professionals, in May 2013.

Egypt participated in the 2012 ITU-IMPACT Workshop on cyber Drill in Jordan and in the ITU RCC Regional cybersecurity Forum cyber Drill 2013 in Oman.

Egypt was the chair of the Program Committee of the Annual meeting of the national CERTs held in Boston – June 2014.

Egypt is also supporting Africa CERT and participated in its annual meeting in Djibouti – May 2014.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

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

[Child Act \(Article 96 and 116\)](#)

2.2 UN CONVENTION AND PROTOCOL

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

Egypt 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

[TEDate \(*\)](#) was established in 2001 by [Egypt Telecom \(*\)](#) and is Egypt's largest IP based data communications vehicle. Its service is supervised by the [National Telecommunication Regulatory Agency \(NTRA\)](#). TEdData launched the "[Family Internet](#)" service to protect children from inappropriate content exposure on the web.

Egypt has led efforts to establish and currently chairs the ITU's Council Working Group for Child Online Protection (CWG-COP) since 2010. At the national level, a national COP Committee was established in May 2013, with representatives from key stakeholders from governmental entities, private sector, academia and professional associations. Three national COP competitions were organized in 2013/14, in addition to several awareness workshops, seminars, and training of trainers sessions.

2.4 REPORTING MECHANISM

Complaints can be addresses to the [Child helpline](#) using the number: 16000.

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 07th November 2014