CYBERWELLNESS PROFILE
KINGDOM OF SAUDI ARABIA

BACKGROUND

Total Population: 28 705 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 60:50%
(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 instrument:
- Anti-Cyber Crime Law.

1.1.2   REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instrument:
- Electronic Transactions Law.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Saudi Arabia has an officially recognized national CIRT known as CERT SA.

1.2.2 STANDARDS

Saudi Arabia does not have an officially approved national or sector specific cybersecurity framework for Cybersecurity.

1.2.3 CERTIFICATION

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

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no national or sector-specific cybersecurity policy in Saudi Arabia.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Saudi Arabia.

1.3.3 RESPONSIBLE AGENCY

CERT SA is the agency responsible for cybersecurity in Saudi Arabia.

1.3.4 NATIONAL BENCHMARKING

Saudi Arabia does not have an official national benchmarking and referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no officially recognized national or sector-specific research and development program or project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

CERT SA security quality management is responsible for awareness building and education/training.

1.4.3 PROFESSIONAL CERTIFICATION

There is a certified professional statistics database where this information is stored.

1.4.4 AGENCY CERTIFICATION

Saudi Arabia 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

There is no framework for sharing cybersecurity assets across borders with other nation states in Saudi Arabia.

1.5.2 INTRA-AGENCY COOPERATION

Saudi Arabia does not have an officially recognized national or sector-specific program for sharing cybersecurity assets.

1.5.3 PUBLIC SECTOR PARTNERSHIP

There is no officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector in Saudi Arabia.

1.5.4 INTERNATIONAL COOPERATION

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

Saudi Arabia participates in the following cybersecurity activities:

- APWG   - OIC-CERT   - The Honeynet Project.

2.   CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

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

- Articles 6 and 8(3) of the Anti-Cybercrime Law (*).

2.2 UN CONVENTION AND PROTOCOL

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

Saudi Arabia 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 Computer Emergency Response Team of Saudi Arabia CERT.SA (*) provides specific information (*) on child online protection.

2.4 REPORTING MECHANISM

The website of CERT.SA provides space in its website for reporting a computer incident but requires a login to do so. It is still possible to contact the CERT through an online form or the mail: info@cert.gov.sa.