CYBERWELLNESS PROFILE
TURKEY

BACKGROUND

Total Population: 74 509 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 46.25%
(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:

-Law on Regulation of the publications on the Internet and Combating against committed crimes by these publications

-Turkish Criminal Law

1.1.2 REGULATION AND COMPLIANCE

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

-Law on Security of Electronic Communications

-Regulation Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Turkey has an officially recognized national CIRT (TR-CERT).

1.2.2 STANDARDS

Turkey has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the National Cyber Security Strategy and Action plan 2013-2014 and the Law on Security of Electronic Communications.

1.2.3 CERTIFICATION

Turkish Standards Institution provides system, personnel and product certification services according to many international standards including ISO IEC 27001, ISO IEC 15408, ISO IEC 12207.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Turkey has an officially recognized national cybersecurity strategy (National Cyber Security Strategy and Action plan 2013-2014). The strategy is based on the principal of securing the information systems used in critical infrastructures and taking necessary measures to provide national cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

The National Cybersecurity Strategy and Action Plan allows for 29 main actions and 95 sub actions and assigns responsibilities about legislation, capacity building, development of technical infrastructure. This in turn provides a national governance roadmap for cybersecurity in Turkey.

1.3.3 RESPONSIBLE AGENCY

The Cybersecurity Board is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. It was established, in order to determine the measures regarding cyber security, to approve the prepared plans, programs, reports, procedures, principles and standards and ensure the application and coordination of them.

1.3.4 NATIONAL BENCHMARKING

In last three years Turkey organized three cyber security exercises at the national level. Participants from both public and private sector have experienced real cyber-attacks and also worked on scenarios. These exercises played a big role in raising awareness of cybersecurity and also were a great tool for measuring the development of cybersecurity. Additionally the By-Law on Security of Electronic Communications obliges electronic communications service providers to comply with ISO IEC 27001. The audits performed by the NRA (ICTA) play a big role in measuring the cybersecurity development level of electronic communications sector.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Turkish Standards Institution is the institution that is responsible for standardization activities. Internationally recognized cybersecurity standards are adopted as Turkish standards as part of harmonization process. The institution provides also standardization services considering the country and sector specific needs.

1.4.2 MANPOWER DEVELOPMENT

Turkish Scientific and Technologic Research Agency and Turkish Standards Institution provide cyber security related training programs including CEH, ISO IEC 27001 lead auditor, internet governance, ICT law etc. There are also graduate programs like information security engineering, cybersecurity, ICT law in several universities like Bahçeşehir University and Şehir University. The graduate programs cover both technical and legal aspects of cybersecurity. Besides, several websites such as www.bilgiguvenligi.gov.tr, www.bilgimikoruyorum.org.tr, www.guvenliweb.org.tr have been established to raise awareness among the people.

1.4.3 PROFESSIONAL CERTIFICATION

Turkey has about 400 public sector professionals certified under internationally recognized certification programs in cybersecurity

1.4.4 AGENCY CERTIFICATION

There are 106 electronic communications service providers that have ISO IEC 27001 certification. The certification agencies include both accredited national (like Turkish Standards Institution, Kalitest etc) and international certification agencies (like BSI, Bureau Veritas, and DAS etc). There are nearly 15 governmental and public sector institutions that have certifications like ISO IEC 27001, ISO IEC 17025, ISO/IEC 18045. The certification agencies are generally accredited national certification agencies (like Turkish Standards Institution, Kalitest etc).

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

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

-Albania, Azerbaijan, Bosnia, Herzegovina, Bulgaria, Kosovo, Kyrgyzstan, Macedonia, -Montenegro, Morocco, Niger, Republic of Sudan, Senegal, Serbia, Tunisia, Iran, Thailand, Egypt and Ukraine

-NATO

1.5.2 INTRA-AGENCY COOPERATION

The National Cyber Security Strategy and Action Plan 2013-2014 encourages the efficient use and sharing of resources between governmental institutions in cybersecurity related activities.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The National Cyber Security Strategy and Action Plan 2013-2014 encourages the efficient use and sharing of resources between public and private sector in cybersecurity related activities.

1.5.4 INTERNATIONAL COOPERATION

Turkey is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Turkey is also actively involved in the standardization work on cybersecurity within ITU-T. TR-CERT (USOM) is also candidate for FIRST and Trusted Introducer Membership. Turkey has co-organized with the collaboration of IMPACT and ITU, the International Cyber Shield Exercise 2014 (ICSE 2014), in May 2014 Istanbul, Turkey. Turkey participated in Applied Learning for Emergency Response Team (ALERT) 2012 during the ITU Regional Forum on Cybersecurity for Europe and CIS, in October 2012, in Bulgaria.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

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

-The Criminal Code (Article 26)

-Law on Regulation of the publications on the Internet and Combating against committed crimes by these publications (Article 8)

2.2 UN CONVENTION AND PROTOCOL

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

Turkey 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 Turkish Information and Communication Technologies Authority, Telecommunications Presidency (*), provides information and makes awareness raising activities about online safety and children online protection to the Turkish public.

2.4 REPORTING MECHANISM

Online illegal material (according to Law 5651) can be reported at the website of Turkish Internet Hotline which is a member of INHOPE.