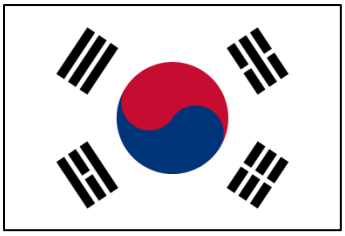

CYBERWELLNESS PROFILE REPUBLIC OF KOREA

BACKROUND

Total Population: 48 588 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 84.77%
(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

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

- Criminal Act (Art. 316(2), Art. 366, Art, 314(2), Art. 347(2), Art. 227(2), Art. 323(2), Art. 140(3), Art 141(1))
- Act on Promotion of Information and Communications Network Utilization and Information Protection
- Personal Information Protection Act
- Act on the Protection of Information and communications Infrastructure

1.1.2 REGULATION AND COMPLIANCE

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

- Act on Promotion of Information and Communications Network Utilization and Information Protection
- Personal Information Protection Act
- Use and Protection of Credit Information Act
- Electronic Financial Transactions Act

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Republic of Korea has an officially recognized national CIRT (KrCERT/CC) and a private CERT (CONCERT) that is promoting secure operation of information and communications network by preventing incidents in the domestic information and communications network.

1.2.2 STANDARDS

The Information Security Management system (ISMS) is the officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

The Korea Internet Security Agency (KISA) provides cybersecurity frameworks in order to foster professionals equipped with information security technology and practical abilities, national qualification. Also SIS (Specialist for Information Security), an accredited private qualification, was promoted to national technical qualification (information security engineer/ industrial information security engineer) in 2013.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Republic of Korea has an officially recognized national cybersecurity strategy (National cybersecurity measures) in order to ensure a systematic government-level response to various cyber threats to national security.

1.3.2 ROADMAP FOR GOVERNANCE

The Personal information protection normalization plan (five plans) provides a national governance roadmap for cybersecurity in Republic of Korea.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Science, ICT and Future Planning establishes, supervises, adjusts and evaluates scientific and technological policies, such as on information security, information culture, ICT convergence promotion and radio wave management. It also monitors and coordinates the implementation of a national cybersecurity strategy, policy and roadmap in Republic of Korea.

1.3.4 NATIONAL BENCHMARKING

The National Information Security Index is a measure for assessing the information security level of the private sector (enterprises and individual internet users) in Republic of Korea and is the officially recognized national benchmarking referential to measure cybersecurity development. The Ministry of Science, ICT and Future Planning also organizes joint workshops and shares information with countries, agencies and companies holding excellent technologies by concluding MoU with them .

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Korea Internet Security Agency (KISA) provides various guidelines regarding personal information protection on Internet, VOIP information security and biometric information. It is also the officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The ICIS (International Conference on Information Security) share latest information about information security, such as domestic and international advanced security technologies, success cases and government policies, and to highlight the importance of security industry as the next-generation growth power.

The Korea Internet Security Agency (KISA) also provides various educational and professional training programs in order to raise awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in both public and private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Republic of Korea has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity such as CISA, CISSP etc. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

The Korea Internet Security Agency (KISA) is the only public agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Korea Internet Security Agency (KISA) has signed MoU and has officially recognized partnerships with the following organizations:

- Office of cybersecurity and Information Assurance (OCSIA UK)
- Checkpoint Israel
- Microsoft
- Israel National Cyber Bureau (INCB)
- MacAfee
- CERT Australia

- CERT Romania (CERT-RO)
- Chinese CERT (CN CERT)
- Japan CERT (JP CERT)
- Cybersecurity Institute (STS) of Kazakhstan

1.5.2 INTRA-AGENCY COOPERATION

Republic of Korea has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the Information Communication Infrastructure Protection Committee which is part of Ministry of Science, ICT and Future Planning and which aims to coordinate policies on critical ICT infrastructure and improve institution on protection of critical ICT infrastructure.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The National Cyber Security Conference is held on a regular basis in order to share information about key cyber security threats occurring in public and private sector in which governmental departments, key CERTs, security companies (vaccine, monitoring) and ISP are the participating organizations.
Republic of Korea has also has a Private – Public – Military Joint Response Team created by the Ministry of Science, ICT and Future Planning organized and operated for decision-making on cyber threats, situation monitoring, analysing of threats and joint investigation.

1.5.4 INTERNATIONAL COOPERATION

Republic of Korea participated in several cybersecurity activities with APCERT and FIRST, of which the Korean CERT KrCERT/CC is a member.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:
- Articles 243-245 o the Criminal Code.
- Article 8 of the Act on the Protection of Children and Juveniles from Sexual Abuse.

2.2 UN CONVENTION AND PROTOCOL

Republic of Korea has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.
Republic of Korea 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 Illegal and Harmful Information Report Center (*), under the Korean Communications Standards Commission (KCSC (*)), works on the protection of internet users with the Korean National Police Agency, the Commission on Youth Protection, NGOs and ISPs.
The SafeNet (*) website, under KCSC (*) introduced a rating system that allows content providers to rate and filter content according a selection made by parents and educators.
The Korean Computer Emergency Response Team (KrCERT/CC*) provides information on general cyber-threats.

2.4 REPORTING MECHANISM

The Illegal and Harmful Information Report Center, a channel of the Korean Internet Safety Commission, receives report on illegal and harmful information.

More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 1st December 2014