CYBERWELLNESS PROFILE
UNITED KINGDOM

BACKGROUND

Total Population: 62 798 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 89.84%
(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:

-Computer Misuse Act (1990)
-Data Protection Act (1998)
-Fraud Act

1.1.2 REGULATION AND COMPLIANCE

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

-OFCOM Telecom Regulation
-Info Commissioner Regulation

1.2 TECHNICAL MEASURES

1.2.1 CIRT

United Kingdom will be establishing a national CIRT by end of 2014. It has the 3 following governmental CIRTs:

-CSIRTUK (Critical Infrastructure)
- csirtuk@cpni.gsi.gov.uk

-GovCertUK (Govt Networks)
- enquiries@govcertuk.gov.uk

-MODCERT (Military Network)
-cert@cert.mod.uk

1.2.2 STANDARDS

United Kingdom is the leading member of the Common Criteria standardization group, which mandates standardization of cyber security in information technology solutions.

1.2.3 CERTIFICATION

The Institute of Information Security Professionals (IISP) is the leading UK professional certification body for the United Kingdom. The government promotes Information Assurance Professionalism. In particular, there is a certification scheme run by the ISSP.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

United Kingdom has an officially recognized national cybersecurity strategy which was published in 2011.

1.3.2 ROADMAP FOR GOVERNANCE

The national governance roadmap for cybersecurity is elaborated in the national cybersecurity strategy.

1.3.3 RESPONSIBLE AGENCY

The Office of Cybersecurity and Information Assurance (OCSIA), part of the Cabinet Office, is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

OCSIA is responsible for the benchmarking and measuring the progress of the National Cyber Security Programme.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

United Kingdom does not have any officially recognized national or sector-specific research and development (R&D) 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

Getsafeonline is a national program aimed at the general public and businesses to raise awareness about cybersecurity. In addition, the government published ten steps to cyber security for the private sector. Lastly, there is a certification scheme run by the ISSP.

1.4.3 PROFESSIONAL CERTIFICATION

United Kingdom has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

United Kingdom's National Technical Authority for Information Assurance (CESG) 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, United Kingdom has officially recognized partnerships with the following organizations:

-ITU
-European CERT Group
-ENISA
-NATO
-TRUSTED Introducer

1.5.2 INTRA-AGENCY COOPERATION

United Kingdom, through the OCSIA, has officially recognized a national program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The OCSIA manage the cyber information security partnership (CISP) with private sector. In addition, the Centre for the Protection of National Infrastructure runs a series of sector-based information exchanges for private sector running critical information infrastructure.

1.5.4 INTERNATIONAL COOPERATION

The UK Government participates fully in the cybersecurity debates within the UN, ITU, ENISA, NATO, and OSCE. This work is spread among many government departments and is coordinated by Cabinet Office and the Foreign Office. GovCertUK 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 instruments:

-§48-§50 of the Sexual Offences Act.
-§1 of the Protection of Children Act.
-§63 of the Criminal Justice and Immigration Act.
-§1 of the Malicious Communications Act.

2.2 UN CONVENTION AND PROTOCOL

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

United Kingdom 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

Child Exploitation and Online Protection (CEOP), under the UK Police, provides information on online safety for children and parents.

2.4 REPORTING MECHANISM

Inappropriate and offensive content can be reported in the website of CEOP. Online Criminal Content can be reported in the website of the Internet Watch Foundation. Computer Incidents can be reported by a filling a form found in the website of the UK Computer Emergency Response Team (GovCertUK) or by the phone number 01242 709311.

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 12th August 2014