CYBERWELLNESS PROFILE RUSSIAN FEDERATION

BACKGROUND

Total Population: 142 703 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 61.40%
(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:

- Criminal code (art. 271-273)

1.1.2 REGULATION AND COMPLIANCE

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

- Federal Law 152 on Personal Data Protection - regulated by Roscomnadzor (Telecommunications Regulator)

-Federal Law 139 on Blacklisting and ISP control - regulated by Roscomnadzor (Telecommunications Regulator)

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Russia has an officially recognized governmental CERT (GOV-CERT), a joint government project CIRT (RU-CERT) and one based on Group IB, the leading Russian company in incident response business CIRT (CERT-GIB).

1.2.2 STANDARDS

Russia does not have an officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Russia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Russia has officially recognized a National Security Concept of the Russian Federation (2000), a concept of the Foreign Policy of the Russian Federation (2013), an Information Security Doctrine of the Russian Federation (2000), basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013) and conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011) .

However the draft of Russia's Cyber Security Strategy is underway.

1.3.2 ROADMAP FOR GOVERNANCE

Russia does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Russian Federal Security Service (FSB), Federal Protection Service (FSO), Federal Service for Technical and Export Control (FSTEC), Ministry of Internal Affairs (MVD), Ministry of Defence (MoD) and the Foreign Intelligence Service (SVR) are the officially recognized institutions responsible for implementing a national cybersecurity strategy, policy and roadmap in Russia.

1.3.4 NATIONAL BENCHMARKING

Each government entity in Russia performs an annual audit of its own networks and systems depending on the requirements of the information.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Russia has 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 through the ITU-T study group question 17 on security.

1.4.2 MANPOWER DEVELOPMENT

Russia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Russia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information regarding any certified government and public sector agencies 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, the Russian company in incident response business CIRT (CERT-GIB) has officially recognized partnerships with the League of Safer Internet and the National Coordination Centre.

1.5.2 INTRA-AGENCY COOPERATION

Russian Federal Security Service (FSB) has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector with the following organizations:

Federal Service for Technical and Export Control (FSTEC)
Ministry of Internal Affairs (MVD)
Ministry of Defence (MoD)
Financial Crimes Unit in Federal Tax Services

1.5.3 PUBLIC SECTOR PARTNERSHIP

Russia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION

Russia does not have any officially recognized participation in regional and/or international cyber security platforms and forums.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:
- Article 242 of the Criminal Code – *does not criminalize simple possession*.

2.2 UN CONVENTION AND PROTOCOL

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

Russia has signed but not ratified (as of 14th December 2014), 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

Russia does not have ant officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM

Cyber Security and Incident Response Team for the governmental networks of the Russian Federation (GOV-CERT.RU (*)) provides space in its website to report a computer incident.

Safer Internet Centre for Russia (*) provides space in its website to report online illegal content.

The Friendly RUNET Foundation (*) provides space (*) in its website to report online illegal content.

More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 22th January 2015