CYBERWELLNESS PROFILE CROATIA

BACKGROUND

Total Population: 4 387 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 66.75%
(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:
- Croatian Criminal Law (January 2013)

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:
- Law on Information Security 2007
- Law on Protection of Personal Data 2003
- Law on Ratification of conventions on cybercrime 2002
- Law on Electronic Document
- Law on the Security and Intelligence System 2006
- Law on Security validation
- Ordinance on the manner and deadlines for the implementation of measures for protection safety and integrity of networks and services 2012
- Regulation on Information Security Measures 2008

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Croatia has an officially recognized national CERT in accordance with the Information security law and its main task is processing of incidents on the Internet. Croatia has also a government CERT ZSIS which is responsible for state authorities, local and territorial (regional) governments, legal personnel with public authorities and legal and physical person who have access to, or handle classified and unclassified information.

1.2.2 STANDARDS

Croatia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. They can be found under the guidelines set by Information Systems Security Bureau and by Office of the National Security Council.

1.2.3 CERTIFICATION

Croatia has officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. They can be found under the guidelines set by Information Systems Security Bureau and by Office of the National Security Council.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Croatia is currently in progress for adoption of a national strategy on cybersecurity. The Office of the National Security Council is responsible for the preparation of this document. Other bodies involved in the preparation of this document are: Information Systems Security Bureau, Croatian Regulatory Authority for Network Industries, Ministry

of Interior, Ministry of Foreign and European Affairs, Croatian national computer emergency response team, Croatian National Bank, Ministry of Maritime Affairs, Transport and Infrastructure, Ministry of Public Administration, Security and Intelligence Agency, Ministry of Defence of the Republic of Croatia.

1.3.2 ROADMAP FOR GOVERNANCE

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

1.3.3 RESPONSIBLE AGENCY

The Office of the National Security Council is the officially recognized institution responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING

Croatia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Croatia 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

Croatian national CERT provides a national or sector-specific research and development (R&D) program through many presentations and easily accessible documents. It also informs people about threats on Internet, gives them statistics about the most common problems concerning cybercrime and also give them advice about how to protect themselves. Center for Information Security (CIS) also creates documents on topics in information security that will be useful to the public, develops educational materials intended for the public, organizes events to raise awareness of information security for the public and for specific groups, cooperates with all the media to raise awareness about information security, brings together young people interested in information security and educates them and also prepares them for professional engagement in the field of information security.

1.4.3 PROFESSIONAL CERTIFICATION

The Information Systems Security Bureau (ZSIS) and the national CERT are public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

The Information Systems Security Bureau (ZSIS) is the central state authority responsible for the technical areas of information security of the state certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

The authorities in Croatia work closely with European Network and Information Security Agency (ENISA), as a body of expertise, whose main task is to help the European Commission, the Member States and the business community to address, respond and especially to prevent network and information security problems and thus Republic of Croatia works with other European countries regarding security incidents.

1.5.2 INTRA-AGENCY COOPERATION

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

1.5.3 PUBLIC SECTOR PARTNERSHIP

Croatia 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

Croatia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Croatia also participated at conference on Strategic Priorities on Cybercrime (Dubrovnik, February, 15th 2013) also participating were Albania, Bosnia and Herzegovina, Montenegro, Serbia, Macedonia, Turkey and Kosovo in cooperation with the Council of Europe and the European Union.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:
- Articles 163-165* of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Croatia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.
Croatia 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 Croatian national CERT provides specific information for parents in its guide about online safety.

2.4 REPORTING MECHANISM

The Croatian national CERT provides the following email address to report computer incidents: ncert@cert.hr
The Center for Missing and Exploited Children provides an online form to report illegal content.

More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 13th November 2014