Deliverable 2.2

Development of a draft cyber security framework

Tempus

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

Deliverable 2.2

Development of a draft cyber security framework

European Commission Tempus Project:

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of content

1. Introduction and preliminaries

According to actual state recorded in Montenegro, regarding cyber security education Roadmap for new Cyber security Education in Montenegro is created as one of previously established results of the Tempus project »Enhancement of Cyber Educational System of Montenegro - ECESM«. Since we are taking initial steps in the area of cyber education, all aspects of cyber education should be considered, analysed and addressed.

To this end, the Cyber Security Framework drafted in this document, is focused on raising awareness about cyber security at national level. Having in mind importance of establishing sustainable framework for continual provision of cyber security education at basic levels for the whole nation, this Framework identifies short term goals (that are expected to be achieved during project duration, 2014- 2016) and long term goals (for period 2014-2020, which will ensure further development of cyber educational system at national level).

The aim of the Framework is, based on previous research, to show proper steps needed to be taken for proper education among citizens, identify key stakeholders and their roles and responsibilities. They are identified by focusing on target groups of ICT users previously defined based on common EU practice and indicators of ICT literacy in Montenegro. Finally, the whole set of trainings and other promotional campaigns are planned to be organised as a part of ECESM project (in period 2015-2016), direct insights from both, identified stakeholders, and several target groups among citizens, will be evaluated and naturally, they might have impact on proposed Framework in revising defined goals and planned activities (and revised Framework is published in Section IV).

2. Goals of the Framework

This Framework builds on existing analysis of current educational system at all levels in the field of cyber security, the efforts to improve the awareness among citizens and establish the bases for creation of enhanced and empowered nation in cyber security. Its intent is to help plan, organise and guide related educational elements in cyber security such as child education, education of youth and adults with different ICT literacy, and academic institutes supporting the research and development in cyber security. This Framework:

- Presents a vision, along with a supporting short-term and long-term goals, to improve the cybersecurity awareness at national level
- Defines an action plan with identified stakeholders and their roles and responsibilities that addresses the specific cybersecurity needs of different groups of ICT users
- Proposes a comprehensive plan for improving the availability, organisational complexity and functionality of educational initiatives, measures and activities - Proposes methods and programs that encourage compliance of educational programs at different levels
- Promotes continuous improvement in the security posture within educational sectors, allowing them to establish baselines to measure security awareness and make changes accordingly.

2.1 Short term goals (2014-2016)

The Roadmap for new Cybersecurity Education in ME (Dev. 1.4), defines the following priorities regarding rising awareness about the risk of online activities:

(p1) Rise awareness about cyber security over Montenegrin population in general. Target should be to educate all population about possible threats over Internet and make them familiar with basic rules about using online accounts, safe surfing and using online services.

(p2) Create core elements of formal educational system in cyber security (graduate and post-graduate studies). In order to ensure sustainable education in cyber security, educational system should be established, including both, formal and informal education. In accordance with the above priorities, its core elements should include literacy of cyber security at lowest levels in educational system and specialised HE such as post-graduate and master studies. All other elements of educational system may be established later in full coherence with those core elements.

In order to achieve defined priorities in short term period (2014-2016) of project duration, the following more specific goals are identified:

(p1.1) Improve Knowledge of Risks and Vulnerabilities in Cyberspace among children (elementary schools), youth (high schools and faculty education) and adults

(p1.2) Promote the Use of Cybersecurity Resources and Tools

(p1.3) Promote Interest in Computer Science and Cybersecurity

(p2.1) Create a plan for updating existing study programs at all educational levels and promote to relevant authorities at both, national and institutional levels

(p2.2) Create and establish multidisciplinary master study program in cyber security

2.2 Long term goals (2014-2020)

The Roadmap for new Cybersecurity Education in ME (Dev. 1.4) recognises the main goal of establishing integral cyber security educational system at national level, and thus the following priorities are defined, related to the scope of this Roadmap:

(pl1) Create R&D environment in the field of cyber security. R&D activities are essential in order to prepare own forces to face a challenge on dynamic and constantly evolving and growing cyber space. To this end, PhD studies should be established with simultaneous preparation at institutional and individual (already proven researchers with expressed willingness and readiness for R&D in cyber security filed) levels to lead those activities at national and/or regional level.

More specifically, the following sub-goals should be achieved for long time period 2014-2020:

(pl1.1) Establish Standards and Guidance for Cybersecurity Training and Professional Development

(pl1.2) Establish updated study programs at all levels in accordance with suggested plan in (p2.1)

(pl1.3) Establish R&D Network at national level and make connections at regional and international levels

3. Action Plan

Since each action at national level requires coordinated and joined forces of identified stakeholders and actors, this section is focused on their identification with preciously defined roles, responsibilities and expected measures to be taken by their side.

3.1 Key stakeholders

The Roadmap is focused on raising awareness among at national level, and analysis conducted in Report – »Analysis of the ME cyber security public awareness« (DEV 2.1) identified the following target groups of ICT users:

- Students (<=18)
- Young adults (19-45)
- Adults (46-64)
- Elderly (65+)

By taking into consideration their primary occupation (e.g. pupils, students, workers, parents, teachers, grandparents, etc.) the following key stakeholders can be identified:

- Elementary schools
- High schools
- Universities
- Ministry of education
- Chamber of Economy
- Other relevant institutions with activities related to those listed below.

3.2 Roles and responsibilities

3.2.1. Elementary school education

Cyber security education in elementary schools should be included into existing subjects about computer science. Children are living with new technologies and they use them every day. Through basic education children will be introduced to technical, law, and sociological aspect of technology they use.

> **Objective 1.** ***Improve Knowledge of Risks and Vulnerabilities in Cyberspace - basic level.*** Children need to learn about responsibilities of using cyberspace. They need to know what is proper way of using Internet, how to be active on net and how to know what is private and what is public on net. It is psychologically new for children and they do not have real

image of their presence on the net and they often have more confidence than they should have. Also it is very important to know how to protect themselves and the others online. To learn about bad praxis and principles of using Internet.

Objective 2. ***Promote the Use of Cybersecurity Resources and Tools – basic level***. Children should be introduced to resources and tools use to enhance their online security. They need to be teach about basic usage of antivirus software, about malware and spam and also about existing and usage of firewall. Children at least have to know about that types of software and hot to enable them on their personal computers.

Objective 3. ***Increase Exposure to Cybersecurity in elementary education.*** Through the existing subjects improve children comprehension about cybersecurity.
Work more on technical, legal and sociological aspects of cybersecurity.

3.2.2. High school education

Objective 1. ***Improve Knowledge of Risks and Vulnerabilities in Cyberspace*** - advanced level. Students need to learn about responsibilities of using cyberspace. They need to know what is proper way of using Internet, how to be active on net and how to know what is private and what is public on net. It is psychologically new for students and they do not have real image of their presence on the net and they often have more confidence than they should have. Also it is very important to know how to protect themselves and the others online. To learn about bad praxis and principles of using Internet.

Objective 2. ***Promote the Use of Cybersecurity Resources and Tools - advanced level***. Students should be introduced to resources and tools use to enhance their online security. They need to be teach about advanced usage of antivirus software, about malware and spam and also about existing and usage of firewall. Students have to know about that types of software and hot to enable and configure them on their personal computers.

Objective 3. ***Increase Exposure to Cybersecurity in high school education.*** Through the existing subjects improve students comprehension about cybersecurity. Work more on technical, legal and sociological aspects of cybersecurity. Also create possibility for students to choose one subject that is specially form the area of cybersecurity.

Objective 4. Promote Interest in Computer Science and Cybersecurity by Increasing the Diversity and Quantity of Course Offerings and Research Opportunities. Ensure to students possibility to choose subjects related to various areas of cybersecurity and to improve their knowledge which will also be connected with other areas and sciences. It should enable students to study cybersecurity from technical, law or sociological aspect.

3.2.3. Faculty education

Objective 1. ***Improve Knowledge of Risks and Vulnerabilities in Cyberspace*****.** Teach students about all aspects of existence in cyberspace. Depending on the faculty students can be teach more or less about cybersecurity depending on the area of the faculty. It is very important to highlight that cybersecurity is not only technical issue but it is also law and sociological issue.

Objective 2. ***Promote the Use of Cybersecurity Resources and Tools*****.** Students should be introduced to resources and tools use to enhance their online security. They need to be teach about advanced usage of antivirus software, about malware and spam and also about existing and usage of firewall. Students have to know about that types of software and hot to enable and configure them on their personal computers.

Objective 3. ***Increase Exposure to Cybersecurity***. Through the existing subjects improve students comprehension about cybersecurity. Work more on technical, legal and sociological aspects of cybersecurity. Also create possibility for students to choose one subject that is specially form the area of cybersecurity.

Objective 4. Promote Interest in Computer Science and Cybersecurity by Increasing the Diversity and Quantity of Course Offerings and Research Opportunities. Ensure to students possibility to choose subjects related to various areas of cybersecurity and to improve their knowledge which will also be connected with other areas and sciences. It should enable students to study cybersecurity from technical, law or sociological aspect.

Master studies

Creation of master studies on HEI that will provide obtaining of special knowledge about cyber security. As area of cyber security is very wide master studies should provide obtaining of very high level of specialized knowledge about cyber security.

PhD Studies

PhD studies at HEI should provide education for next generation of cyber security researcher and education staff. Studies should be base for creating group of scientist that will be capable to educate in area of cyber security and to do research in theoretical and practical aspects of cyber security.

3.2.4. Lifelong education

Since there is no formally established any lifelong educational program, raising awareness among adults should be implemented in conjunction with other promotional activities and campaigns.

Objective 1. Encourage the Development and Adoption of the National Cybersecurity Workforce Framework
Objective 2. Develop Cybersecurity Workforce Forecasting Tools
Objective 3. Establish Standards and Guidance for Cybersecurity Training and Professional Development
Objective 4. Analyse and Identify Best Practices to Help Organizations Recruit and Retain Cybersecurity Professionals
Objective 5. Evaluate the Professionalization of the Cybersecurity Workforce

4. Updated cyber security framework- v2 (after project implementation)

After organizing all training events and conducting evaluation analyses of their impact, as well as after implementing actions aimed on ensuring Sustainability and visibility at national level, few changes are made in drafted short-term and long-term goals, which are presented in Section 2.

4.1 Short term goals (2016-2018)

In order to continue with building cyber nation in Montenegro, continuation and spreading the training events are essential among all identified target groups (even some of them were not directly reached by the project). Thus, the following goals are defined for short term period (2016-2018) after project duration:

(p1) Continue with improving knowledge of risks and vulnerabilities in cyber space among youth (high schools and faculty education) and staff members at schools

(p2) Start with programs aimed improving knowledge of risks and vulnerabilities in cyber space among children (elementary schools) and adults

(p3) Promote the Use of Cybersecurity Resources and Tools

(p4) Promote Interest in Computer Science and Cybersecurity

(p5) Continue with promoting Montenegrin Cyber Education Centre as a core unit for both, raising awareness, education and training in cyber security at national level in Montenegro

(p6) Create a plan for updating existing study programs at all educational levels (form elementary schools to university level) and promote to relevant authorities at both, national and institutional levels

4.2 Long term goals (2018-2022)

The main long-term goal is already identified in Section 2.2, which still remains the same with few more detailed directions how to be achieved:

(pl1) Create R&D environment in the field of cyber security.

More specifically, the following sub-goals should be achieved for long time period 2018-2022:

(pl1.1) Establish Standards and Guidance for Cyber security Training and Professional Development, all in close cooperation with the Ministry of education and Ministry of science of Montenegro

(pl1.2) Establish PhD study program in multidisciplinary fields of cyber security **(pl1.3)** Establish R&D Network at national level and make connections at regional and international levels