Deliverable 3.1

Cross-matching of organizations with EU standards - draft

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 Contents

• 1. Introduction

To make of Montenegro a cyber secure nation means not only to increase the cyber security awareness of its citizens at all levels, as we did in WP2, but to fully secure, protect, and defend the Montenegrin information systems from all types of cyber threats. To this end, it is fundamental to concurrently address two main goals: (i) the development of an advanced ICT infrastructure, and (ii) the formation of an agile, highly skilled professional cyber security workforce. WP3 was designed exactly to achieve the latter requirement, *i.e*, to pave the way for the improvement of the cyber security knowledge maturity of the governmental, public and private Montenegrin institutions. ICT related organizations demand a globally competitive, up-to-date cyber security workforce, able to foresee and prevent cyber risks (when possible), and to promptly tackle ongoing cyber attacks. The process of educating a national cyber security workforce consists in three main complementary components: workforce planning, professional development, and identification of core professional competencies.

Workforce planning means to analyze the functional capabilities needed to achieve the current mission, forecast future capabilities, and identify specific knowledge, skills, and abilities for cyber security professionals. Professional development incorporates formal training and education to maintain the technical health of the cyber security workforce. Professionalization of cyber security identifies core occupational competencies, sets objective standards for skills development, accreditation, and job performance of cyber security practitioners, and develops career ladders within the various cyber security disciplines.

All the aforementioned activities need to be performed in accordance with EU recognized best-practices and principles. For this reason, the first step is a careful cross-matching of the current scenario of Montenegrin organizations with respect to EU standards and guidelines for cyber security enforcement. This report summarizes the joint work of staff from the Montenegrin institutions involved in the project and of representatives from the EU partners, to explore the deficiencies of Montenegrin organizations in order to schedule training activities and produce recommendations for implementation of well-defined corrective actions.

Unfortunately, assessing the responsiveness of organizations to cyber threats, and the general cyber security competence of their staff, is a very hard task: most companies are not willing to share confidential information concerning the countermeasures to cyber risks they put in practice and the training of their employees, preferring to claim their readiness to face any possible

eventuality. As a consequence, the best way to assess the current situation of Montenegrin organizations consists in identifying relevant training topics based on EU cyber security standards, and to measure the interest that Montenegrin organizations exhibit with respet to such topics, arguing that the interest is in direct proportion with their need for specific education in that field. More specifically, we proceeded in the following way:

- We collected EU standards, guidelines and best-practices for cyber security in public and private organizations, discussed them and pinpointed the aspects of cyber security enforcement that emerge as the most important ones
- We consequently identified a set of cyber security requirements for organizations and their staff to meet EU standards
- Based on such requirements, we elaborated a set of fundamental cyber security training topics
- We contacted all main Montenegrin public and private organizations to measure their interest for all identified training topics
- Based on the interest scores collected from such organizations, we assessed the needs of Montenegrin institutions and companies compared to EU standards

Summing up, we were able to analyze existing level of cyber security knowledge (focusing on specialized knowledge related to work position) in Montenegrin governmental, public and private organizations through inquiries for employers within different works and positions, and to cross-match the results with European standards and practices, using the results to define realistic needs and basic structure of the future sustainable framework.

• 2. EU standards for cyber security in public and private organizations

2.1 EU standards, guidelines and best-practices

2.2 Cyber security requirements for organizations and their staff

2.3 Relevant cyber security training topics

• 3. Cross-matching with Montenegrin organizations

3.1 Current scenario of Montenegrin public and private organizations

3.2 Cross-matching Montenegrin organizations with EU standards

• 4. Conclusions