Deliverable 3.2

Usable cyber security competency 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

Both public and private organizations increasingly rely on data networks for business, commerce and protection of sensitive information, and the frequency, sophistication and impact of cyber attacks are continuously rising. In 2014, crime involving computers and networks has cost the world economy more than $445 billion. No organization is immune to cyber security threats: in recent years successful attacks struck leading companies in retailing (Target and Neiman Marcus), finance (JPMorgan Chase), and technology (eBay, Adobe and Snapchat), just to name a few[1]. The nature of a cyber attack may substantially vary, but it is possible to identify seven major causes of cyber security breaches[2] (reported in casual order):

- Users not keeping up with new tactics
- Underestimating cyber criminals
- Loss of mobile devices
- Mobile devices as ideal entry points
- Naive end-users and disgruntled employees
- No perimeter to protection
- Lack of a layered defense

Investing in wide-scale cyber security is nowadays a priority for all companies, but this list makes perfectly clear that most (not to say all) vulnerabilities could be easily addressed by a proper and systematic approach to cyber security. However, as managers and boards increasingly realize, this is only possible relying on a highly skilled and trained cyber security workforce.

Technological solutions, in fact, are completely useless and unreliable in absence of cyber security professionals capable of putting them in practice effectively and of keeping users and less qualified employees aware of cyber threats. The cyber security field is on the rise and the demand for IT specialists (especially security experts) often exceeds the supply. To clearly identify the scope of cyber security and the competencies that employees at different level must demonstrate is therefore fundamental both to allow better hiring strategies and to implement proper internal training.

The purpose of Dev. 3.2 is to create an usable cyber security competency framework that, based on the outcome of Dev. 3.1, defines proper actions to provide highly skilled workers and specialists for cyber security at adequate places within organizations. To this end, it is critical to identify guidelines for definitions and standards in order to measure and assess the cyber security workforce with any consistency. The competency framework will facilitate the identification of training needs and guide the design of a professional development program, that will be fully developed in Dev. 3.3.

Defining and measuring effectiveness, especially the performance of workers, is a critical part of managing an organization. The problem is to understand what to measure exactly: the main

1 http://fortune.com/2014/06/17/is-a-cybersecurity-bubble-brewing/

2 http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_2014_breachreport.pdf

issue is to find proper ways to define the skills, behaviours, and attitudes that workers and applicants need to perform their roles effectively, to comprehend whether they are qualified for the job.

Formal education, on-the-job training, years of experience, personal characteristics are all important factors to determine the expertise and competence of an employee. Nevertheless, none of them seems sufficient to describe an ideal set of behaviours and traits needed for any particular role. Nor do they guarantee that individuals will perform to the standards and levels required by the organization.

To approach this problem in a systematic way, we need to link individual performance to the goals of the business, that is, to identify integrated knowledge and skills that an employee need to perform a job effectively. More precisely, we need to formally identify a list of "tasks", "roles", "competencies" and "competency levels", and to map each role in the organization with the tasks it is responsible for, and with the competencies such tasks require, identifying the level of familiarity required for each of such competencies. This way, organizations have a powerful instrument to evaluate the readiness of a worker for a specific role, to delineate customized training activities to fill possible educational gaps, and to recruit and select new staff more effectively.

2. Cyber security competency framework

Aiming at building a highly skilled and competitive cyber security workforce for Montenegrin public and private organizations, first of all we need to provide them with instruments to identify clear and universally recognized core competencies for cyber security professionals. A competency is defined as "a group of related skills and abilities that influence a major job function, indicate successful job performance, are measurable against standards, and are subject to improvement through training and experience"[3]. To establish a cyber security competency framework we therefore need to:

- Define cyber security knowledge and skills required for each managerial and technological task in public and private organizations that need to deal with data and assets possibly exposed to cyber threats
- Identify specific cyber security competencies, in the form of sets of cyber security topics
- List several competency levels, going from knowledge and comprehension, to application and evaluation
- Map roles to tasks and competencies, with corresponding required competency levels
- Synthesized the mapping into a clear and detailed competency framework table
- Finally, propose courses and delineates courses structure to implement such framework

Overall, this process allows us to provide a fundamental instrument for organizations to manage cyber security efficiently and effectively within their employees, and for the project consortium to identify suitable training activities to guarantee a globally competitive cyber security workforce.

3 http://www.careeronestop.org/competencymodel/userguide_competency.aspx

Of course, a similar work follows other remarkable examples, especially in EU and other western countries. Probably, the most relevant effort in this direction was put in practice by the US government that through the National Initiative for Cybersecurity Education (NICE) and the Department of Labor (DOL) developed standardized professional requirements for cyber security.

Significantly, we observe that only national governments are in a position to lead national cyber security efforts that involve all national stakeholders. In addition to putting in place functional measures to counter cyber security threats, governments have the central task of establishing, among all stakeholders, a common awareness and understanding of cyber security as well as a common recognition of each stakeholder's roles and responsibilities.

This is a further proof that the role and responsibility of governments in cyber security is extensive, and is not limited to well known aspects such as (i) policy making, (ii) organizational structures (including institutional organization and coordination, incident management, cyber security readiness assessment, etc.), (iii) capacity building, (iv) establishing legal measures, and (v) fostering public-private sector collaboration and industry guidelines. Due to the wide range of threats and vulnerabilities on different sectors of cyber security, a large number of national governments assume a variety of roles and carry an extensive range or responsibilities that include citizen and professionals capacity-building.

In the US, the NICE proposed a National Cybersecurity Workforce Framework, that defines seven categories of typical job duties, covering cyber security work in 31 speciality areas across industries, organizations, and job types[4]. For each of such areas, the Framework clearly identifies knowledge, skills, and abilities that professionals must demonstrate to perform their job tasks effectively. The seven categories, that correspond to typical cyber security professional positions, are the following:

- *Securely provision*: responsible for conceptualizing, designing, and building secure IT systems
- *Operate and maintain*: responsible for providing support, administration and maintenance necessary to make IT systems secure without affecting effectiveness and efficiency
- *Protect and defend*: responsible for identification, analysis, and mitigation of threats internal to IT systems or networks
- *Investigate*: responsible for investigation of IT systems and networks aimed at identifying suspect events, potential crimes and digital evidences
- *Collect and operate*: responsible of specialized denial and deception operations and collection of cyber security information that may turn useful to develop intelligence
- *Analyze*: responsible for highly specialized review and evaluation of incoming cyber security information to determine its usefulness for intelligence
- *Oversight and development*: responsible of providing leadership, management, direction, and development needed to allow individuals and organizations to effectively conduct cyber security work

4 http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf

Based on the NICE Framework, the US DOL developed a Cybersecurity Industry Competency Model[5]. The Model can be considered an expansion of the Framework, in that it includes competencies required at various career tiers, not necessarily related to cyber security, but somehow needed to safely interact with cyber space. The DOL Model shows different tiers as building blocks of a "cyber security professionals pyramid", covering all categories from entry-level to senior leader. While tiers one to three comprehend generic "personal effectiveness", "academic" and "workplace" competencies, higher tiers show that is needed for "industry-wide technical", "industry-sector functional", till "management" and "occupation-specific" competencies.

Finally, before discussing the development of our competency framework for Montenegro, it is important to keep in mind that despite the government is reasonably expected to provide private organizations with instruments to train and hire highly skilled professionals, the involvement of the private sector in the process is essential.

ICT infrastructures are in fact for the most part owned and operated by the private sector in the large majority of countries worldwide, including the EU, and private companies are typically the first to adopt technological changes and assess its associated vulnerabilities. On an individual basis, businesses are expected to implement an adequate level of cyber security safeguards into their business practices. On a collective level, the private sector has an important role to play in its own right and in cooperation with government in developing any national cyber security effort, including cyber security business norms, standards and codes of conduct, as well as in identifying and encouraging the adoption of good practices or, as in this case, the development of precise competencies schemes.

2.1. Required knowledge and skills, and competency levels

Organizations should identify and develop engineers, technologists, and security professionals who perform reliably under pressure, think together creatively, regroup adaptively, adjust swiftly to changing tactical conditions, and learn quickly from mistakes and failures.

If we study the workforce as a pyramid to measure the knowledge and skills anchored in cybersecurity the pyramid can divide in to three sections: Experts, Professionals and Entering the Field. See Figure 2.2

5 http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

Figure 2.2: Workforce as a pyramid

Experts: difficult to discern real experts from generalists

Professionals: There are not enough qualified professionals to meet the needs across the public and private sectors.

Entering the field: New workforce candidates in traditional educational pipelines are hard to attract and must be developed.

Assessing an individual's ability to apply knowledge we have to evaluate a methods, tools, and perform tasks with skill to meet their responsibilities, and decisions incident to their position:

Positions that have the primary responsibility, either directly or through communications with others, for the implementation of cyber security practices.

Positions directly responsible for complying with program standards, system standards, or regulatory requirements.

Across the chain of technology (designers, integrators, asset owner/operators, third-parties/services)

The Science of Cybersecurity Skill Assessment & Development can be measured by:

1. Competency model development
2. Assessment instrument development and validation
3. Aptitude vs. achievement testing

Assessing cybersecurity skills and competencies are important to identify required knowledge, skills and competency levels. Following assignment would prove methodology which is accepted internationally by intuitions of higher learning publishes in 23 languages. To complete the assignment the interviewer would compose questions similar to the samples below. Once it has been completed a simple check in the appropriate box will help record the assignment for reporting.

Skills and Competency Assignment Scale					
L1. Knowledge	**L2. Comprehension**	**L3. Application**	**L4. Analysis**	**L5. Synthesis**	**L6. Evaluation**

Sample questions:

L1. Are you aware of the subject, tell about it?

L2. Can you explain the subject?

L3. Tell me how you would apply this knowledge?

L4. How would you perform root0cause-analysis related issues?

L5. How would you apply lessons learned to re-design the approach?

L6. How would you assess the effectiveness of your applied strategy?

2.2. Competency framework table

Domain	**Subject**	**Assignment Rating**					
Security Leadership	Program management	L1	L2	L3	L4	L5	L6
	Lead security incident response team	L1	L2	L3	L4	L5	L6
	Manage vulnerabilities	L1	L2	L3	L4	L5	L6
Security Governance	Engage Stakeholders	L1	L2	L3	L4	L5	L6
	Allocate Resources	L1	L2	L3	L4	L5	L6
	Manage external inquires	L1	L2	L3	L4	L5	L6

Security Risk and Management	Lead monitoring and reporting	L1	L2	L3	L4	L5	L6
	Manage risk registry	L1	L2	L3	L4	L5	L6
	Lead risk treatment	L1	L2	L3	L4	L5	L6
Security Architecture	Manage the roadmap	L1	L2	L3	L4	L5	L6
	Consult on technology architecture	L1	L2	L3	L4	L5	L6
	Oversee information architecture	L1	L2	L3	L4	L5	L6

3. Implementation of the competency framework

4. Conclusions