COMPETENCY IN NUGGETS FOR CYBER SECURITY TRAININGS

Eugenia Kovatcheva, Willan Dimitrov, Milena Koleva, Iva Kostadinova, Iglika Getova

University of Library Studies and Information Technologies (BULGARIA)

Abstract

In the last ten years the European Qualification Framework is a base for development of the curriculum corresponding to the business needs in each EU country. Building the competency profile is very important for better communication between business and the educational organisations. This is crucial for new job profiles such as the cyber security area. It is one of the main research topic of the Bulgarian University of Library Studies and Information Technologies (ULSIT). There are bachelor, master, PhD and VET programmes in cyber security. The academic research includes several projects in the last three years namely NATO project MN CD E&T, Erasmus+ projects 573901-EPP-1-2016-1-IT-EPPKAZ-CBHE-JP for development of Bachelor and MSc programmes in Information Security for Moldova, Kazakhstan and Vietnam and 2018-1-LV01-KA202-046987 for reducing the cyber security management skills gap in SMEs and 2018-1-BG01-KA202-047919: Internet of Things security nuggets.

The ULSIT extracts the best practices, combines already established cyber security frameworks according to the needs of Bulgarian business and implements the results in training. The university staff train and support their colleagues from their partners’ countries how to specify and set up their training.

This paper presents the processes of defining the cyber security competency framework for educational levels (from basic to expert) for cyber user, cyber manager and cyber security specialist. The main purpose is to define curriculum in small educational modules and configure the sequences. The education include simulation and inquire approach. The challenge is to specify the educational nuggets and to develop significant set with educational recourses and activities. The paper shows first and second phase of the process: identifications of the gaps between supply and demand and creation of the cyber security competence framework for IoT ecosystems.

The defined model includes common competences such as personal effectiveness, academic and workplace skills as well as specific industry - wide technical and sector functional area and finally managerial specific abilities.

The learning is designed in micro modules sorted in sequence. The educational nuggets support the professional development and give learners flexibility to fix gaps in their specific knowledge and skills.

Keywords: Competence, Competency, Based, learning, Cyber, Security, Training, Nuggets, Micro, Education.

1 INTRODUCTION

The cyber security is a hot topic nowadays and everyone has to take care of it. The main question is how everyone to be trained in it? There are different levels of knowledge that have to be obtained from beginner to expert and manager. There are several competency frameworks in cyber security [1] as U.S. Department of Labour - Cybersecurity Industry Competency Model [2], NICE Cyber Workforce Framework [3], DOL Competency Model Framework [4], etc. There are several curriculum developments as a standard of ACM IEEE [5] and one of the newest ones is developed under the NATO and EU and MN CD E&T projects.

According to Parrish et al. [6] the term “cybersecurity” is used with the specific intent of referring to a broad “meta-discipline” covering a broad spectrum of disciplinary variants (Figure 1).
The authors upgrade their experience for development of cyber security programmes in the course of their work: for five universities in Kazakhstan on Erasmus+ projects 573901-EPP-1-2016-1-IT-EPPKAZ-CBHE-JP; VET 2018-1-LV01-KA202-046987 for reducing the cyber security management skills gap in SMEs; and 2018-1-BG01-KA202-047919: Internet of Things security nuggets. The team proposes a consistent framework around a vision for cybersecurity education. It clarifies the scope of what is included in a cybersecurity educational degree; what is part of the field of study according to the business needs in terms of the set of developed competencies and the needs of the various types of cybersecurity degrees as well as the target group. Focusing on the VET the micro- or the so called nugget education corresponds and meets the needs faster than the traditional courses.

The content is security of the Internet of Things (IoT). IoTs are elements of the cyber physical world that create many new challenges to security and privacy. These are due to the IoT nature, which is characterized by architectural synergy between new telecom services, cloud services and mobile devices, interoperability with the existing Internet. Different threat actors can attack IoT systems at different points in their architecture or organizational decisions. The protection from these attacks is a matter of prophylactic investigation of the security problems and weaknesses in it. In the project we outline the next security and privacy areas:

- **Security incident management and thread hunting**: They are based mainly on SIEM. The highly distributed topology and the large amount of information that is generated is a challenge for the traffic capabilities of the transmission environment. It imposes high storage requirements and complicates forensic analyzes [17].

- **Authentication and physical threats**: highly distributed deployments of a large number of IoT devices, such as RFID tags and wireless sensors, will generally be deployed in public areas without any protection, which makes the devices difficult to manage and vulnerable to physical attacks. This introduces the challenge of authenticating IoT devices, which involves recognizing the device and verifying its association with a correct topological address [14].

- **Integrity**: the unattended environment for IoT devices also makes data integrity a concern. Once deployed, most of these devices will operate in a self-supported manner.

- **Confidentiality**: the communication method between devices and the gateway is primarily wireless, which results in confidentiality risks. Constraints on power, computational capability, storage and other aspects of an IoT device are a high barrier performing the necessary operations to achieve data confidentiality through the process of encryption and key management [12].

- **Privacy**: as an existing public concern for monitoring and interacting with the real world, the consequence of information leakage in local IoT networks becomes exacerbated when integrated into the global Internet [15]. By connecting real world objects and information via the
Internet, data may become accessible to various organizations and domains across the Internet, instead of only being revealed to a small group, which makes it more likely to be exposed to sophisticated malicious parties and therefore increases the probability of being exploited and attacked [14].

Conventional security and privacy techniques are not necessarily appropriate for the IoT due to the special characteristics of the IoT. The attractive prospect of IoT applications, as well as the strong needs of increasing public confidence about security and privacy issues, requires new and comprehensive solutions that not only protect local IoT devices but also the broader Internet aspect of the IoT. In the following sections, we will examine the aforementioned problems and explore security and privacy techniques to support the IoT infrastructure based on the MobilityFirst network, one of the representatives of future Internet architectures.

The IoT defies traditional classification and categorization and is still little understood. People have a hard time understanding the concept. To begin to manage IoT risk, institutional leaders must have some vocabulary for it. The IoT is still new, its effects are largely unknown and its precedents and analogies are few. We need to surface some language and concepts so that it can be discussed [7]. Secondly, the additional risks that the institution faces are still there: safety, liability, financial loss, reputation damage, technology challenges, business competition, etc.

There is an overall lack of awareness regarding the need of security in IoT devices. Even more worrying is the lack of knowledge regarding the threats they are exposed to – most IoT consumers do not have a basic understanding of their IoT devices and the impact on their environment. This may result in the devices not being updated, with a subsequent breach of security.

2 PRELIMINARY STUDY

At the beginning of the project a survey was conducted. Two main directions were in focus: asking and offering training in cyber security. The results show variety of organisations demanding training: universities, industry, IT services and so on (Figure 2). The study covers more than 200 records from Bulgaria, Croatia, Italy, Israel, The Netherlands, Russia, Spain, UK, USA. Mainly Bachelors demand educational level (Figure 4).

![Figure 2 Types of organisations demand for training](image)

The preferred degree is Bachelor (Figure 3).

![Figure 3 Educational Level](image)

![Figure 4 Preferred degree](image)

The training on offer are from 1 month to 2 years. Most of them are with duration of one year. The main focus is on Cyber Security, next is IoT security, followed by Cyber Defence and Cyber Law (Figure 5).
The shortcomings in the existing courses are related to Security issues concerning state of the art technologies. To address the critical security, safety and privacy risks of these devices while retaining open connectivity options, scalability (due to high number of devices), interoperability and application independence (different devices and purposes), we require new solutions. Nowadays, securing data, objects, networks, infrastructure, systems and people under IoT is increasingly relying on Cognitive Systems, Machine Learning, Artificial Intelligence and Distributed Ledger technologies (DLT) and new decentralised approaches [8].

However, the context-aware nature of the IoT means that devices are constantly gathering and distributing personal information – ranging from a person’s location, to their purchase preferences, to the ambient temperature of their living environment or even the serial number of their pacemaker. Thus, any security system must address the issues of “authentication, confidentiality, and access control” to offer a secure and robust privacy paradigm [9].

3 CHALLENGES

Securing IoT devices is challenging for a number of reasons. A rapidly increasing number of gadgets are being turned into smart devices and as manufacturers roll out new products more quickly, little priority is given to security. Eventually we could see almost every home device connected to the Internet, not necessarily with any consumer benefit but instead geared towards data collection, which is incredibly valuable for manufacturers. A lack of awareness among consumers and businesses is also a major obstacle to security, with the convenience and cost-saving benefits of IoT tech appearing to outweigh the potential risks.

Another challenge is securing not only the IoT devices but also the networks over which their data is transferred. In the past, businesses did not always focus on building end-to-end security into the network. This is set to change as attitudes evolve, with 46 percent of organizations ranking ‘securing IoT within the organization as a high priority for 2018, according to the Hiscox Cyber Readiness Report [10].

4 METHODOLOGY

Even before the beginning of the 21st century, academic education had been moving away from the traditional knowledge-based approach towards more competence-based teaching. Recently this process has become more of a preoccupation. With the introduction of the Bologna process, many EU universities have experienced increased interest from the professional and commercial sectors for their interests to be included into the academic environment. As a result, universities have developed initiatives to adapt their academic teaching to the requirements of industry, in order to ensure that their graduates are the most employable, and to increase their competitiveness in the international education market. As a result, a new form of curriculum development has arisen. It has focused on finding the relationship between university education and the competences needed by the graduates in their later careers, by defining exactly which competencies need to be included in the respective
The concept of competence can bridge the world of education, training, knowledge management, and informal learning.

The proposed systematic methodology for competence based curriculum development consists of six phases: (1) Conceptualisation; (2) Planning; (3) Data collection; (4) Data analysis & Create catalog of competences; (5) Develop competence based curriculum and (6) Develop applications & Pilot test.

The development of a competence-based curriculum begins with building a successful strategy. The process consists of two parts: Part I, the readiness of the university to make a transition from a traditional content and time based curriculum to competence based curriculum is assessed, and Part II - translating the strategy into a Competence Based Curriculum.

The next step is concerned with identification and description of the competencies that students should acquire or with describing the final attainment levels of the educational program in terms of competencies. The competences are obtained as a result of researching the existing economic sector competence models and job profiles. Typically this activity is performed by a heterogeneous team, consisting of stakeholders such as curriculum developers, teachers, educational managers, field experts and branch representatives. Together they analyse and collect information about the competences within the domain of interest, identify the competencies, and describe them in a competence map. This is a highly complex and difficult process, as all processes of curriculum development are. It is obvious that a competence profile has important implications, since it constitutes the basis of a competence-based curriculum.

The Methodology for Competence-Based Curricula Development is graphically presented in Figure 6. The methodology promotes continuous improvement through the consideration of the university strategic plans. It is based on the intensive research and needs analysis of the university’s competence based curriculum development and training.

Nowadays the need for fast knowledge and skills training is very important for professional development. One way to respond to it is the micro and nugget education. The Learning nuggets is a standalone mini learning activity [12], usually less than 5 minutes in length, that would vary in size and scope that learners undertake in a particular context in order to attain specific learning outcomes. Nugget (micro)-learning involves learning in smaller steps and goes hand-in-hand with traditional e-learning. Activities that are usually designated for short-term lessons, projects and coursework are designed to provide the student with ‘bits’ of information in an e-learning mediated environment. This holistic approach is especially designed for skills-based training and education which deals with relatively small learning units. It involves short-term focused strategies. This learning technique is flexible. It can be used for sustainable development as well. In a wider sense, nugget education can be understood as a metaphor which refers to micro aspects of a variety of learning models, concepts and processes [13]. Depending on frames and domains of reference, micro, meso and macro aspects
vary. They are relational concepts. In a more general discourse on learning, one might differentiate between the learning of individuals, group learning or learning of organizations and the learning of generations or societies. In the presented case the education is focused on the individuals and cut in nuggets.

The nugget education approach is an emergent paradigm, so there are no hard definitions or coherent uses of the term yet. It marks a transition from common models of learning towards micro perspectives and the significance of micro dimensions in the process of learning.

The nugget education instructional design is focused on the design of micro-learning activities through micro steps in media-rich e-learning and environments, which is a daily reality for today's knowledge workers. These activities can be incorporated into learner's daily routines and tasks. Unlike "traditional" e-learning approaches, nugget education often tends towards push technology through push media, which reduces the cognitive load on the learners. Therefore, the selection of nugget learning objects as well as the pace and timing of activities are of importance for didactical designs.

The combination of competence-based and nugget approaches represent a powerful tool for training.

5 RESULTS

Defining a Common Set of Cybersecurity Professional Competencies expands the Framework by including the competencies needed to safely interact with cyberspace. The nugget approach in professional development focuses on the competencies corresponding to cyber security expertise, mainly on the so-called industry competencies [4]. They include cybersecurity technology, information assurance, risk management, incident detection, incident response and remediation, security provision systems, operating and maintaining IT security, protection and defence from threats, investigating threats, collecting information and governance of cyber security processes, analysing information, overseeing and operating cybersecurity work.

The intranet technology itself is challenging for curriculum design and learning practice, as the simulation of a smart city or intelligent transport systems in a lab environment is difficult and there is still no experience accumulated in this and other IoT areas. It has not yet reached a maturity stage when it can be effectively implemented in teaching at university level. At the same time, malicious actors increase the sophistication of their instruments and the risks to society.

The nugget training increase the ability of learners to analyse information from different sources and get an idea of the dangers in the associated physical and digital environment. They meet the needs of learners and teachers by presenting personalized information and communication capabilities. In order to fill the gap, it is necessary to overcome the concerns about privacy and security and interoperability related to technology. Careful consideration will be needed on how technology can best be adapted to the learning and teaching environment. Nonetheless, interviews from our study with companies and student masters show a willingness to overcome these gaps and take on the potential of these new technologies organically with the requirements of cybersecurity and confidentiality. This report recommends the following in relation to the deployment of IoT security in an educational environment:

- learners should achieve organized knowledge and skills by studying the basics of cyber security through the prism of small examples on the security of an intranet of things;
- discussing and analysing individual incidents with an intrusion or leak of personal data is related to clarifying basic concepts that are fundamental to cyber security;
- any bite of IoT security should have the ability to provide students with the expertise from simple to complex. This will ensure that students will be able to upgrade their competencies and easily switch to more complicated bites;
- any future deployment of solutions for the IoT should take account of security and confidentiality requirements;
- all IoT applications should also take into account privacy, security and security interoperability;
- every solution to the IoT needs should be accompanied by training to ensure that all staff and students can use it effectively.

Taking into account the present state of digital space, priority should be given to integrating the security and confidentiality especially in the IoT area. In the individual learning disciplines students can achieve knowledge for the security of the existing computer operating systems, networks,
programming, databases, virtualization, and cloud architectures. This is an addition to the current focus of the project on the study about the IoT security integration.

The talent management professionals have identified three gaps: competency, professional experience and education speed-to-market in the education-to-workforce pipeline that are hindering organizations’ efforts to meet current and future cybersecurity needs. The effective implementations of the Cybersecurity Competency Model maps the job tasks to the knowledge units.

6 CONCLUSIONS

The IoT contains huge challenges for the security of the state, industry and privacy. The design, development and support of the IoT faces the increasing expectations of ensuring security, safety and privacy. At the same time, the current shortage of cyber security staff also includes the poor performance of Internet security graduates in higher education. Students complete cyber security specialties without being prepared for the changing cyber security challenges due to the emerging new technologies in the digital world.

The project offers the opportunity to flexibly incorporate security topics in different areas from the application of Internet to higher education and better and more personalized training for students. Our research shows that the IoT of Things evolves extremely quickly and it infuses all emerging technologies - machine training, artificial intelligence, neural networks, dockers and containers. This dynamics dictates the nuggets approach that allows adaptation of learning courses to it.

The Cybersecurity Competency Model serves as a tool for cybersecurity workforce planning, performance management, and articulation of career pathways and educational requirements. The implementation of the cyber security model includes defining curriculum in small educational modules and configuring the sequences. The education includes simulation and inquire approach. The challenge is to specify the educational nuggets (the micro pieces of learning objectives) and to develop significant set with educational resources and activities. The first phase – competency identification has been completed and a further step is to map competencies to the learning objectives and nuggets.

ACKNOWLEDGEMENTS

This paper is supported by the project RedCyberSG: REducing the CYBERsecurity Management Skills Gap in SMEs 2018-1-LV01-KA202-046987 co-funded by the Erasmus+ Programme of the European Union

REFERENCES


