Challenges and Reflections in Designing Cyber Security Curriculum

Teresa Pereira
Polytechnic Institute of Viana do Castelo
Viana do Castelo, Portugal
tpereira@esce.ipvc.pt

Henrique Santos
Department of Information Systems
University of Minho
Guimarães, Portugal
hsantos@dsi.uminho.pt

Isabel Mendes
Algoritmi Research Center
University of Minho
Guimarães, Portugal
mimp@eeg.uminho.pt

Abstract— **Recently it has been noticed an increased number of cyber-incidents, sometimes causing seriously impact to organizations and governments. Cyberattacks exploits a variety of technological and social vulnerabilities to achieve a malicious objective. The emergence of new and sophisticated Cyberthreats demand very skilled operators with a solid knowledge about concepts and technologies related to Cybersecurity and Cyberdefense. However, the landscape of this base knowledge is very diverse in nature, requiring agile learning methods, besides a very demanding training process limited by the intrinsic technology's complexity and broad range of application domains. Although existing Cybersecurity and Cyberdefense curricula spans a wide array of topics and training strategies, its programs content lack focus on some particular aspect, like depth of education/training and its link to professional development. This paper intends to provide some reflections regarding the curricula contents that should be considered when a graduate level curriculum in cybersecurity is designed.**

Keywords— Cybersecurity; Information Security; Cyberdefense; Cyberattacks; Curriculum; Cybersecurity training; Curriculum Development; Cybersecurity Body of Knoweledge.

I. INTRODUCTION

A few years ago, there were no iPhones or iPads and didn't exist Facebook as well as other popular social networks. In fact the emergence of the new and sophisticated gadgets, linked to changes in user behaviors and the increasingly expansion of on-line transactions, have brought many technological challenges, but also new security threats to the end users and also to governments and organizations in general. Additionally, it is noticed an increase dependence on the online operations/services resulted from their conveniences together with the emergence of new technologies. On the other hand, the Cloud-based systems, Internet of Things (IoT), Enterprise 4.0 and so-called BYOD (Bring Your Own Device) trend, or as IT professionals also call it "bring your own demon", has brought serious issues regarding the classical perimeter defense and consequently severe security incidents. The nature of the adversaries has been also changing, from script-kiddies to profit-seeking individuals and groups (Cybercrime) to hacktivists and state actors. In this context, it becomes fundamental to promote cybersecurity awareness for every segment of the population.

Concerning defense, many government bodies have developed significant efforts and disposed considerable resources to strengthening a Cyberdefense posture. US have announced their intention to categorize Cyberattacks against defense and critical infrastructures as acts of war [1]. In line, UK announced high financial investments to develop advanced militarized Cybersecurity skills studies and workforce preparation [2]. These announcements have demanded depth reviews on the cyberspace related policies, requiring increased collaboration between governments, private sector and academia. Several other countries are reporting identical posture. These initiatives have led to some questions such as: why cybersecurity has suddenly become such a topic of interest? While others may ask: why it was waited so long [3].

This paper intends to provide some reflections regarding Cybersecurity education and training emphasizing the curricula contents that should be considered when a graduate level in Cybersecurity curriculum is designed. This paper is structured as follows: in section 2, it is presented an overview on Cybersecurity concept; in section 3, it is introduced the main initiatives conducted in Cybersecurity education, as well as particular reflections regarding curriculum contents; conclusions are presented in section 4.

II. CYBERSECURITY OVERVIEW

In July 2012, the International Standards Organization has published the ISO/IEC 27032: Information Technology - Security techniques – Guidelines for Cybersecurity [4]. This standard defines Cybersecurity as the "preservation of confidentiality, integrity and availability of information in the Cyberspace". Meanwhile Cyberspace is also defined by this standard as a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" [4]. The National Initiative for Cybersecurity Education (NICE) also defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual

This work has been supported by COMPETE: POCI-01-0145-FEDER-007043 and FCT - Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2013.

978-1-5090-4886-1/17/$31.00 ©2017 IEEE

environment of information and interactions between people" [5]. Other authors bring different inputs to the discussion, introducing different perspectives, but emphasizing that cybersecurity is not a new domain, rather a method of viewing and correlating existing knowledge to holistically analyze, understand, defend against and respond to Cyberthreats [16].

In truth, Cybersecurity is not a recent field of interest but, with the almost daily news reported by the media about cybersecurity breaches and attacks, cybersecurity have been gaining visibility and consequently a wide interest by governments, enterprises and academia. Among the remarkable incidents it is important to highlight those surrounding the Supervisor Control and Data Acquisition (SCADA) systems, as is the case of the Stuxenet virus [6], recognized in 2009, and moving the threat landscape from computer-focus to Critical Infrastructures, with the capability to seriously affect our daily live (giving another sense to Cyber Terror). Despite the reactions and patches produced at the technology level, there still are significant vulnerabilities recognized by all stakeholders. Cyberattacks have evolved and getting more sophisticated. One can easily recognize Cyberthreats related to the civil liberty, electronic privacy violations, or identity and information theft, critical systems including power grids, emergency communications systems, financial systems and air traffic control networks, cars, among others.

Although many of these systems are owned by the private sector, they represent critical homeland and economic interests, thus governments are also responsible for their stability and security. In fact, the constant rise of cyberattacks frequency, have forced governments worldwide to implement preventive actions to reduce the risk of a successful attacks performed against critical infrastructures. In addition, it is also encouraged to foster appropriate knowledge about security and safety, in order to i) build secure systems and increase likelihood the next generation of IT workers to have background needed to design and develop systems that are engineered to be reliable and secure; and ii) develop a general cybersecurity awareness level, promoting adequate user behaviors in this cyber world.

In this context, and in order to reinforce these actions, the European Parliament have recently (April of 2016) published and approved a new Former Directive 2016/679, requiring all European organizations to prove their capability to protect the organizational processing activities and the free flow of personal data between Member States [7]. This will force organizations to implement an information security plan, for instances to enable them to recover from a security incident. However most of the organizations are facing serious difficulties. First most of the organizations have a completely lack of knowledge of this EU Directive. Second they do not know how to translate organizational procedures into security policies and, much less, how to implement and manage a set of mechanisms to enforce those policies. Third, and in particular concerning small and medium enterprises, they cannot afford to invest the required budget in their IT infrastructure protection and workforce and thus to be in compliance with this Directive.

This EU Directive in conjunction with the cybersecurity challenges, which daily emerge, demand highly skilled workforce capable of responding to a dynamic and rapidly evolving threat scenario. In this context, academia and organizations should join efforts to offer cybersecurity education, training and certification, with well-defined skilled objectives and competences aligned with organizational and social current security needs, at all necessary levels to make it effective to every segment of the population - which is far from being a simple task.

III. CYBERSECUIRTY CURRICULUM REFLECTIONS

This section introduce a brief overview of the main initiatives conducted in cybersecurity education, followed by some reflections regarding the curriculum contents that should be considered when cybersecurity graduate level curriculum is designed.

A. Initiatives for Cybersecurity Education

NICE (National Initiative for Cybersecurity Education Strategic Plan) [5] is lead and coordinated by the National Institute of Standards and Technology (NIST), and the National Science Foundation's (NSF's) CyberCorps: Scholarship for Service (SFS) programs, which have closely worked for years to produce outcomes for students and thereby improve cybersecurity for all. In fact, NICE's National Cybersecurity Workforce Framework (NCWF) proposes the decomposition of the cybersecurity field into 7 categories and some 32 functionalities and skill sets. The complete details of NCWF and its categories can be found at https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework. In this context, some authors suggest the development of a cybersecurity degree program based on each NCWF category [8] [9].

The Committee on National Security Systems produced in 1994 an educational reference framework listing the content knowledge for an Information Security Curriculum [11], which comprise topics from a variety of domains, including areas specified by the National Training Standard for Information Systems Security (INFOSEC) Professionals (NSTISS), such as communications basics, security basics, NSTISS basics, system operating environment, NSTISS planning and management and NSTISS policies and procedures. This standard is a reference and provides a good baseline for Information Assurance and Security Education. However it does not address some of the Cybersecurity current needs. Indeed, cybersecurity workforce is too broad and diverse to be treated as a single occupation or profession, and decisions about whether and how to professionalize the field may vary according to role and context [12].

Notwithstanding the wide range of Cybersecurity application, it is possible to build a structured curriculum that should be both encompassing and unbiased to the reflections presented in the previous section.

B. Competences

The curriculum definition should always include the description of competencies expected to obtain when a training and/or education course is performed. In the Cybersecurity area it is unquestionable the need to encompass deep technical

competences, but also very important to develop thinking abilities, including the capability to recognize and respond to complex and emergent behavior, mastery using abstractions and principles, the ability to assess risk and handle uncertainty, problem-solving and reasoning skills, and facility in adversarial thinking, which consist in trying to identify possible player actions [13]. Concerning this last goal, it can easily be extended to the question raised by Fred B. Schneider and Bruce Schneier: can we teach students to recognize and respond to complex and emergent behavior, and how to handle uncertainty and ambiguity? This is not an easy question. Even those who study Cybersecurity education do not seem to know the answer to the authors' question [14] [15]. Notwithstanding there are a wide array of topics and training strategies which can be implemented in order to fill particular aspects, like depth of education and training and its link to professional development. And in the meantime, these additional skills may help to improve the recognition to the so long-awaited adversarial thinking, hence turn more effective a cybersecurity course development.

The followed described competencies are adapted from Rowe, Lunt and Ekstrom [16], who discuss curriculum development in cybersecurity. In their proposal the authors tried to embrace a sufficient generic approach, in order to enable its adoption by most programs.

1) The students will get familiar with the STEM disciplines - Siences, Technology, Engineering and Mathematics – in order to be able to understand the multidisciplinary nature of cybersecurity and then be prepared to learn and understand new technologies and context throughout their careers.

2) Acquisition of basic cybersecurity skills with a link to the professional environment. This competency emphazise the need to align studies' programs skillsets with the profession.

In fact Fred. B. Schneider suggests the alignment of people from industry and government, who have experience with real systems, users and attackers to the cybersecurity course. Their inputs will largely enrich the universities curriculum initiatives [14].

3) Understand the need for cross-disciplinary and cross-cultural collaboration in cybersecurity and be able to communicate to a diverse technical and non-technical audiences.

It is highly important for students be able to cross both cultural and academic differences to improve systems security and educate users.

4) Ability to apply their security knowledge in a context of Cybersecurity threats, attacks, incident response and defenses. The main idea is to develop security skills in order to develop adversarial thinking. This means to think as a potential attacker, relate to a cybervictim and comprehend the complete picture. For example, in an advanced persistent threat scenario, a cybersecurity professional should be able to understand and correlate all attack vectors and use these in a form of root cause analysis to determine the attack goals, and then implement an incident response plan that should minimize service interruption and additionaly contribute to get defensive abilities against attack.

5) Understand the ethical responsabilities of cybersecurity profession and be able to treat ethical, moral and privacy issues responsibly and with sensitive.

This last competence underlines the importance of cybersecurity professionls being of high moral character.

These five competencies should not be seen as all-inclusive, but just to assist those responsible for a cybersecurity program course development.

C. Topics

Cybersecurity topics are drawn from a wide range of existing disciplines. However this does not imply that it has no innovative content. In fact there are some topics that are simply not found in any other discipline, and therefore we consider that will certainly provide significant contributes to the current lack of qualified professionals. Most of IT professionals have their training background in IT disciplines. As an academic discipline, IT has matured over the years to cover in depth different component technologies and it connects to a variety of socio-technological fields, such as bio-informatics, social computing and technology education, technology innovation, yet it still have room to growth and include cybersecurity and their variations.

In order to provide a flexible Cybersecurity curriculum and establish a relationship with other domains, it is proposed by researchers that Cyberscurity curricula should be defined based on three high-level activities/categories, following a common pre-requisite of Information Security Management [20].

Rowe, Lunt and Ekstrom suggest three high level categories, which are: Prepare, Defend and Act [16]. LaPiedra propose grouping the activities into three distinct phases - Prevention, Detection and Response [17] - they have a lot of similarities. In practice we can only be able to defend against an incident, if it is detected a threat, or an attack, an event and/or vulnerabilities. Moreover, we can have a respond or an act action when a cyberattack is detected. In this context, we consider LaPiedra approach to the following considerations.

Each phase requires strategies and activities that will move the process to the next phase. In fact, due to the dynamic nature and growth of new threats, attacks and vulnerabilities it is required timely adjustments to the methodologies in each phase (prevention, detection and response) of the cycle. A change in one phase, affects in some form the entire process. A proactive strategy adjustment in the prevention phase will require adjusts into the detection and response activities. Lessons learned during the response phase will be addressed in the planning of prevention procedures and detection configurations [17]. Security process is a journey and not a destination [17] hence it is a dynamic cycle that enforce regular changes due to the threat and vulnerability environment.

Each activity – Prevention, Detection and Response - can be contextualized through the following questions:

1. What are the assets' vulnerabilities and what Cyberthreats are there, in order to enable the selection and the implementation of adequate security controls to mitigate potential attacks? (Prevention)
2. What are the tools and mechanisms that trigger when a security event occur and alert for a Cyberthreat or a Cyberattack? (Detection)
3. What should be done, when a security incident of a cyberattack occurs? (Response)

Cybersecurity prevention implies that security risks are recognized, demanding a thorough understanding of the Cyberthreat and its impact. This enables to underline that these are not merely technical topics, but an extensive understanding about cyberspace and the real world. In this activity, the primary technical topics that could be embraced in a cybersecurity curriculum are penetration testing, ethical hacking and advanced persistent/evasive threats, implementation of secure software and awareness.

The detection activity aims to discover signs of a security breaches, with security tools or notification by an insider or outside party about suspected event or an alert. It is important to know mechanisms that enable to trigger events when a suspicious activity occurs. The technical topics to be covered in this activity include intrusion detection systems and penetration testing.

The response activity is about what to do when a security incident occurs. What steps should be taken to assess the potential impact, respond and restore the asset? This includes the analysis of the incident for its procedural and policy implications, the gathering of metrics, and incorporate the "lessons learned" into future response activities and training. When an incident occurs many questions arise and problems are encountered usually different for each incident. The technical topics to be covered include digital forensics and incident response, and auditing. Other areas include cultural and global standardization, legal issues, awareness, counter forensics and the theory of computer forensics.

This relatively high-level topics approach should provide a base to design a cybersecurity graduate level curriculum and highlight the need for cybersecurity education. At the same time emphasizes that cybersecurity is not a new topic, rather a method of viewing and correlating existing knowledge to analyze, understand, defend against and respond to Cyberthreats and Cyberattacks. The OCDE report "Reducing Systematic Cybersecurity Risk" [19] presents an excellent summary of cybersecurity topics and discussion points.

In summary, a Cybersecurity curriculum should consider the following aspects:

- Verify if the programs include up-to-date security elements throughout their curriculum.
- Familiarize students with terminology of cybersecurity.
- Evaluate their current advanced content in cybersecurity topics and when it is possible, teach such content in a cybersecurity context.

A cybersecurity curriculum program spans a wide range of topics. Therefore a program should provide appropriate depth of education and work together with multiple people with different skills.

IV. Conclusions

In this paper it is highlighted the need to develop education strategies to reduce vulnerabilities and respond to cyberattacks on critical infrastructures. It is essential to establish a set of required skills following a broader and deeper approach in educational level for computer scientists, network engineers, electronics engineers, and business process engineers [18]. In addition, the development of professional skills contribute to organizations to respond in a more effective way to cyberattacks, to implement awareness about security good practices, but at the same time enrich them with technological capabilities to built secure systems.

It is recognized the difficulties currently faced with substantial variances in standards, definitions and methods associated to cybersecurity. The "Prevention; Detection and Response" activities are a proposal, which may allow flexibility for organizations and institutions to study these variations, or to align with specific approach. However these suggestions as well as the reflections presented in this paper should not be seen as absolute. They are merely provided to assist those responsible for course development as seed ideas in developing cybersecurity program content.

References

[1] BBC, US Petagon to treat cyber-attacks as "acts of war". *British Broadcasting Corporation*, June 1, 2011.

[2] BBC, UK breefs up cyber warfare plans. *British Broadcasting Corporation,* June 1, 2011.

[3] J. Herrera-Flanigan," Cyber Attention: Why Now?" *Cybersecurity Report*, *Nextgov,* May 27, 2011. Retrieved May 2011 from: http://www.nextgov.com/cybersecurity/cybersecurity-report/2011/05/cyber-attention-why-now/54566/.

[4] ISO/IEC 27032: Information Technology - Security techniques – Guidelines for Cybersecurity. Retrieved September of 2016 from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375.

[5] National Initiative for Cybersecurity Education Strategic Plan. Building a Digital Nation. August 11, 2011. Retrieved December 2016 from: http://www.contegosecurity.com/pdfs/Draft_NICE-Strategic-Plan_Aug2011.pdf.

[6] N. Falliere, L. O. Murchu, and E. Chien, W32.StuxenetDossier.Symantec, February 2011.

[7] General Data Protection Regulation-GDPR, (2016), OJ L 119, 4.5.2016, p. 1-88 (2016), Regulation (EU) 2016/679 of European Parliament and of the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC. Retrieved 12 of Setempber 2016 from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[8] NICE, National Initiative for Cybersecurity Education. Available from: http://csrc.nist.gov/nice/

[9] Homeland Security, National Initiative for Cybersecurity Careers and Studies, Cybersecurity Workforce Framework. Retrived 30 of December 2016 from: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

[10] E. McDuffie, V. Piotrowski, "The Future of Cybersecurity Education", IEEE Computer Society, August 2014.

[11] NSTISS, National Training Standard for Information Systems Security (INFOSEC) Professionals. *Committee on National Security Systems (CNSS),* 1994.

[12] Nat'l Research Council Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making. The Nat'l Academies Press, 2013.

[13] M. Dark, "Thinking about Cybersecurity", IEEE Computer and Reliability Societies, January/February 2015.

[14] F. Schneider, "Cybersecurity Education in Universities", IEEE Security & Privacy, vol. 11, no. 4, 2013, pp.3-4.

[15] B. Schneier, "The Security Mindset", blog; Retrieved July 2010 from: www.schneier.com/blog/archives/2008/03/the_security_mi_1.html.

[16] D. Rowe, B. Lunt, J. Ekstrom, "The Role of Cyber-Security in Information Technology Educatio", 12th Annual Conference on IT Education (SIGITE 2011), October 19-22, 2011, New York, United states. Retrived February 2015 from: http://sigite2011.sigite.org/wp-content/uploads/2011/09/session07-paper03.pdf.

[17] J. LaPiedra, "The Information Security Process Prevention, Detection and Response", 2002, SANS Intitute. Retrived 31 of December 2016 from: https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197.

[18] C. Irvine, S. Chin, D. Frincke, "Integrating Security into the Curriculum" (1998). *Electrical Engineering and Computer Science*. Paper 84. Retrived 23 March 2016 from: http://surface.syr.edu/eecs/84.

[19] P. Sommer, I. Brown, "Reducing Systemic Cybersecurity Risk", OCDE/IFP Project on "Future global Shocks", 2011. Retrieved January 2017 from: https://www.oecd.org/gov/risk/46889922.pdf.

[20] B. Lunt, J. Ekstrom, S. Gorka, *et al.,* Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. *Association for Computing Machinery (ACM); IEEE Computer Society,* November 2008.