International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Cyber Security by Hack-Space Integrated Model

S. Riyazbanu, B. Gouri

Assistant Professor, KSRM College of Engineering, Kadapa

Abstract: ***Cyber Security is one of the Important model by hack-space integrated. This model is design training course produced by professional employees. It is composed mainly four elements, those are organization, knowledge, skills/tools and collaboration. This model is to create professionals capable of dealing of security for more levels with clear ideas of functions, processes, and controls useful security.***

Keywords: Cyber Security, Hacker, Education

1. Method

This study focuses on cybersecurity education for information technology (IT) students, including undergraduate and graduate students in programs in computer science (CS) and computer networks (CN). Most operational jobs that address cybersecurity issues in Ecuadorian financial and other industries are filled with individuals from these backgrounds. Based on the key elements depicted in Figure 1, we prepared interview guides to conduct semi-structured interviews. We also conducted desk research to identify strategies for improvement that have been implemented by other countries that might be suitable for Ecuador.

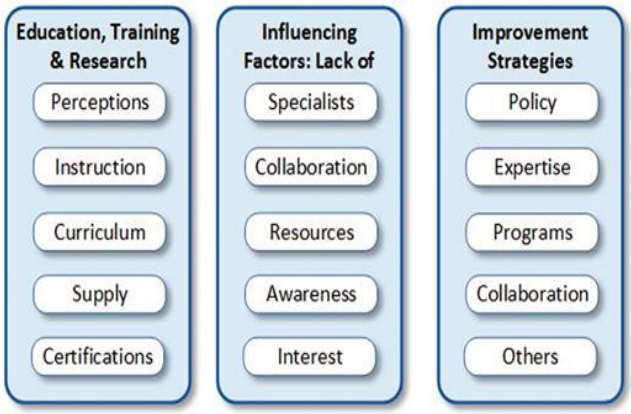

Figure 1: Key Elements of cyber security education.

2. The Hack-Space Integrated Model

It is composed mainly four elements, those are organization, knowledge, skills/tools and collaboration. During the start-up phase of the initiative, five brainstorming sessions were held between the various actors and two focus groups were launched: the first aimed at bringing out the real training needs and identifying the lessons to be included, also in light of the constraints imposed from the MIUR; the second one focused on defining the structure, the organization and the instrumental equipment of the Cyber Security laboratory of expected implementation. The result was The Hack Space, an integrated model developed along four main dimensions presented in detail in the following sections. The objective is to create professionals capable of dealing with security at various levels, with clear ideas on what are the processes, functions and controls useful for security. In other words, professionals with an in-depth knowledge of the company structures in which security is treated and how to deal with it. I t is shown fig:2

Figure 2: The hack space Dimensions

2.1 Organization

The model was simplified by reducing the security functions from 5 to 3: Prevention, Detection, Response. This simplification, inspired by the "The Information Security Process" model proposed was considered necessary in order to: make the process leaner and give immediacy to the approach; allow to better map the software platforms installed in the cyber security laboratory. Obviously, the reduction of the security functions also entailed a consequent reorganization of the security controls. The next step was to identify the Organizational Units responsible for carrying out the CIS controls, that is, the Security Operation Center (SOC), the Computer Security Incident Response Team (CSIRT) and the Support Unit (SU), resulting in the mapping of the CIS security controls Fig. 3, thus arriving at the completion of the organizational model of The Hack Space shown in Fig. 4.The Table 1 reports the mapping of the NIST Core Framework with the priority of security controls. Fig 3: security functions and organizational units.

Table 1. CIS Critical Security Controls in NIST Framework Core.

CIS Critical Security Controls	F1	F2	F3	F4	F5
1 Inventory of Authorized and Unauthorized Devices	X	-	-	-	-
2 Inventory of Authorized and Unauthorized Software	X	-	-	-	-
3 Secure Configuration of End-User Devices	-	X	-	-	-
4 Continuous Vulnerability Assessment & Remediation	X	-	X	X	-
5 Controlled Use of Administrative Privileges	-	X	-	-	-
6 Maintenance, Monitoring, and Analysis of Audit	-	-	X	X	-
7 Email and Web Browser Protections	-	X	-	-	-
8 Malware Defense	-	X	X	-	-
9 Limitation & Control of Network Ports, Protocols, and Service	-	X	-	-	-
10 Data Recovery Capability	-	-	-	-	X
11 Secure Configuration of Network Devices	-	X	-	-	-
12 Boundary Defense	-	-	X	-	-
13 Data Protection	-	X	-	-	-
14 Controlled Access Based on Need to know	-	X	-	-	-
15 Wireless Access Control	-	X	-	-	-
16 Account Monitoring and Control	-	X	X	-	-
17 Security Skills Assessment and Appropriate Training	-	X	-	-	-
18 Application Software Security	-	X	-	-	-
19 Incident Response and Management	-	-	X	X	-
20 Penetration Tests and Red Team Exercises	-	-	-	X	X

Figure 3: The Hack Space Security Functions and Organizational Units

This model is using detection, prevention and response for Security Operation Center (SOC), Computer Security Incident Response Team (CSIRT), Support Unit (SU). It is shown fig.4

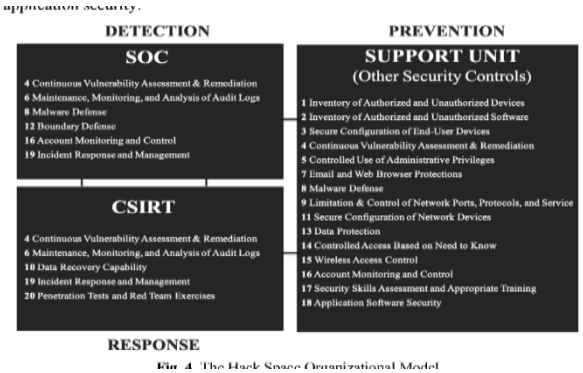

Figure 4: Hack space organization model

Figure 4: The Hack Space Organizational Model

2.2 Knowledge

For all the courses including laboratory activities and project activities, a co-teaching was planned between university professors and experts in cyber security in order to maximize the effectiveness of the interventions. In particular, the experts had the role of assisting university professors during the courses with particular reference to the software platforms used and to the creation of serious games useful to simulate real use scenarios that apply the knowledge acquired during the theoretical lessons and develop the necessary skills. They also supported the students in conducting case studies that involved the use of software platforms installed at the cyber security laboratory. Each of the courses envisaged has been conceptually placed within an identified organizational unit (SOC, CSIRT, SU) in order to clearly highlight the usefulness of the acquired knowledge with respect to the Security Functions and SecurityControls included in the Hack Space Organizational Model Fig. 5. A fundamental course was Business Organization for Cyber Security, which was assigned to an expert of IBM Security, and aimed at transferring The Hack Space Organizational Model to the students providing an overview on the entire initiative.

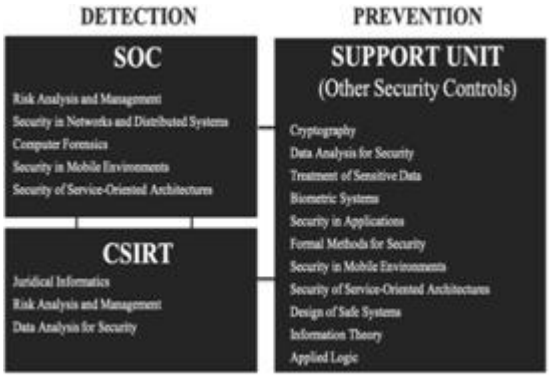

Figure 5: The Hack-Space Knowledge Model

2.3 Skills and Tools

The purpose of the activities developed along this dimension was to set up a cyber security laboratory in coherence with The Hack Space Organizational Model, which was useful to allow students to develop the skills and experience necessary with respect to dedicated IT platforms. The hack-space immune system is shown in fig 6.

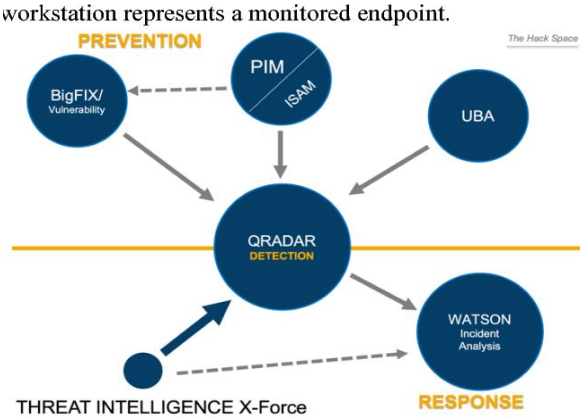

Figure 6: Hack-space immune system

2.4 Collaboration

Along this dimension, a set of activities are being developed to encourage and implement the collaboration between the Department of Computer Science at the University of Bari and other universities, institutions and organizations wishing to use the Skills and Tools Dimension of the Hack Space. These activities include the definition of a Memorandum of Understanding used to formalize the agreements, and the set of technical evolutions of the Laboratory architecture and of the supply environment (processing power, available memory, disk space, events per second analyzed etc.) that must be implemented to make the entire structure a multi-tenant service.

3. Expected Results

We plan to adopt a mix-method research strategy combining various types of studies both qualitative and quantitative to collect evidence. At the moment we are developing a set of serious games in order to improve the teaching and laboratory activities along with a qualitative survey study to evaluate the efficacy of The Hack Space Model.

4. Conclusion

The hack-space model is support 4 major components. These are proposed for Knowledge, starting from the educational needs on the theme of cyber security, proposes a two-year course of study, the master degree in cyber security, aimed at training cyber security professionals of the future; Organization, thanks to which the training path has been articulated in coherence with those that today are the structures, the functions, the controls and the processes already used in companies to face the cyber security problems; Skills and Tools, which, thanks to the launch of a cutting-edge cyber security laboratory equipped with the most advanced software platforms available, allows students to develop skills related to the use of enterprise level tools, usually inaccessible to universities due to the significant acquisition costs, making them ready to operate immediately in real business contexts; Collaboration: which proposes models of public-private collaboration that allow third parties to reuse the model, including the laboratory set up, subject to specific collaboration agreements to regulate the methods of fruition, both organizational and technical. The experimentation of the model is still in progress. In addition, key models for the institutional collaboration between the University of Bari and other subjects interested in using The Hack Space are currently being defined. These models will allow other universities and institutions to be able to use the cyber security laboratory launched, enhancing the results of the initiative and contributing to the growth of knowledge, experience and collaborations on the issue of cyber security.

References

[1] Dimauro G., Caivano D., Girardi F., “A New Method and a Non-Invasive Device to Estimate Anemia Based on Digital Images of the Conjunctiva”, IEEE Access, Volume 6, pp. 46968-46975, doi: 10.1109/ACCESS.2018.2867110, (2018).
[2] Dimauro, G., di Nicola, V., Bevilacqua, V., Caivano, D., Girardi, F., “Assessment of speech intelligibility in Parkinson’s disease using a speech-to-text system”, IEEE Access, Volume 5, pp. 22199 – 22208, doi: 10.1109/ACCESS.2017.2762475, (2017)
[3] Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Vergallo, R. Integration of RFID and WSN technologies in a smart parking system. Paper presented at the 2014 22nd International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2014, 104-110, doi:10.1109/SOFTCOM.2014.7039099, (2014).