Teaching Cyber Security: The Hack-Space Integrated Model

Maria Teresa Baldassarre[1], Vita Santa Barletta[1], Danilo Caivano[1],
Domenico Raguseo[2], Michele Scalera[1]

[1]University of Bari Aldo Moro,
Department of Computer Science, Via Orabona 4 - 70125 Bari, Italy
[2] IBM Security, Italy
{mariateresa.baldassarre,vita.barletta,danilo.caivano,
michele.scalera}@uniba.it, dom.raguseo@it.ibm.com

Abstract. Nowadays cyber security is becoming an ever more stringent requirement and warned by organizations and companies all over the world. Furthermore, the educational offer on the topic is still modest and universities are struggling to design training courses capable of producing professionals directly employable. In this work, this need is addressed with the proposal of an integrated model "The Hack Space", developed within the Master of Science in Computer Security of the University of Bari, composed of four main elements: Organization, Knowledge, Skills/Tools and Collaboration. The Hack Space aims 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, using an in-depth knowledge structure of the company.

Keywords: Cybersecurity, Education, Hacker.

1 Introduction

The numbers are those of a real global war in which it is not yet clear who the victims are and who the perpetrators are: 500 billion dollars are the estimated damages of the cybercrime on a world scale; 10 billion euros are the estimated damages in Italy in 2016 alone; cyber espionage has recorded an increase of 46% compared to the previous year, and after all the latest news reports relating to the various attempts to interfere on the political vote of entire countries prove it. The amount of cyber-attacks from 2011 to date have increased by 240%. Despite this, in Italy, for example, there are modest investments in safety, close to about 1 billion euro, equal to the tenth of the damage alone suffered by the country in 2016 [1].

The growing complexity of business processes [2], the ongoing digital transformation of companies, the extensive use of the network to provide services, as well as to communicate and share distributed resources, encourages and increases the interaction between the various subjects for social, economic and work purposes. At the same time, it opens the front to criminal attacks aimed at compromising the confidentiality, integrity and availability of resources and information. For example, just note that the adoption of mobile technology and cloud computing has led to an exponential increase in cyber-attacks [3]. Nonetheless, the use of low cost devices in health-care [4,5], WSN based device and systems [6,7,8], and the emerging smart home systems [9] also represents a high risky trends.

In this highly changing scenario, the dynamic growth of new threats attacking vulnerabilities requires timely identification, definition and adjustment of the strategies and activities needed for facing security threats and incidents. This requires to continuously update skills, abilities, tools to defend oneself [10]. The cybersecurity talent gap is an industrial crisis and according to recent estimates made by Forbes, there will be as many as 3.5 million unfilled positions in the industry by 2021 [11]. In this scenario a solution seems to be simple: universities have to start offering more courses in cybersecurity. But universities are slow to change and furthermore cyber security education needs to be structured and designed according to the organization adopted, processes, security functions and instruments already used in industry, not only in a theoretical and abstract way. Otherwise the risk for universities is to produce professionals with a knowledge that is too far from what is currently in the state of practice of industry, proving ineffective and forcing companies to invest more time and effort to fill this gap. Indeed, it is no coincidence that today many of the training resources on the subject of cyber security are the result of an effort only minimally supported by the system of university education that indeed seems to trudge [12].

To meet these needs, this paper presents an integrated model called "The Hack Space" resulting from a joint effort between the University of Bari, IBM Security and the Puglia Region in an effort to fill the existing talent gap. The model is structured along four main dimensions: (i) Knowledge, which defines the skills that a Cyber Security expert must possess; (ii) Organization, which identifies the organizational structures dedicated to security, security functions and security controls that must be implemented in order to correctly deal with problems related to cyber security; (iii) Skills and Tools, which identifies the platforms and software tools that must be used and the ideal architecture of a laboratory dedicated to cyber security; (iv) Collaboration, whose goal is the definition of sustainable collaboration models that allow other subjects to be able to use The Hack Space solutions.

The rest of this paper is organized as follows: Related work in Cyber Security Education is addressed in section 2; in section 3 The Hack Space Model is presented. Section 4 illustrates the empirical validation initiatives. Conclusion and discussion, as well as directions for future research work, are pointed out in section 5.

2 Related Work

The amount of training that universities offer and the distance between it and the real needs of industries has been a well-known problem for a long time [13]. There are various experiences and attempts, even successful, able to fill this gap. The world of cyber security impacts on at least three dimensions: organizational security, network security and application security. Training along these dimensions is crucial because it is not enough to rely on technology as the main defense, instead of recognizing that the easiest attack vectors are the people who operate computers [14]. Therefore, the need for training in cyber security emerges. In the training of new professionals, it is necessary to consider two fundamental aspects: the principles of computer security such as cryptography and how technologies and threats evolve [15]. For example, analyzing a malware like MIRAI starting from understanding how it can propagate can also help to apply defense strategies to protect itself from its illegitimate children as SATORI, plus remote code injection; JENX, plus third party tools; OMG, plus http and SOCK proxy to add VPN layer to connecting with IoT devices; WICKED, dedicated to Netgear and CCTV-DVR devices and then spread OWARI botnet. In [16] it is considered necessary to practice countermeasures to become aware of security incidents in the same situation as reality and to learn cooperation through teamwork and improve individual skills. Using KIPS (Kaspersky Industrial Protection Simulation), a game based on gamification theory aims at educating university students in operational technology (OT) security; while in [17] a mobile device evaluation and testing platform were developed to evaluate the mobile malware to provide students with a safe and sandboxed environment for malware analysis, tool enhanced lab environment, updated malware repository, log collection and exact assistance. Using the platform, the authors have created several courses in mobile device security. The research of [18] confirms how participatory teaching methods lead to greater learning. The results obtained from experiential learning, a lesson in the classroom with a teacher to learn the principles of computer security and practical exercises to implement what has been learnt from the theory, indicate that students are more likely to retain the knowledge acquired than the non-experiential knowledge that was not provided for exercises. Along this line the research shows how the evaluation of the students is also positive [19], i.e. 85% of students thought “Hackademic” (a virtual framework that allows them to perform hacking attacks and penetration testing in a deliberately vulnerable, but isolated, safe and controlled environment) helped them significantly be informed about and/or better understand the security issues each exercise was addressing. In [20] a competition-based scenario is described for teaching some basic concepts of network security. Initially, the instructor demonstrated the methods and the tools, later the students were separated in two groups: group A and group B. At first, group A acted as the red team (attackers) and group B played the blue team (defenders). The following week, group roles were exchanged. In this phase the instructor covered the role of coach and motivator offering advice and technical support.

The previous experiences mentioned represent cases of success that are nevertheless isolated and not part of a structured training path. The importance of having cutting-edge laboratories certainly emerges, as well as the importance of conceiving integrated training interventions that, in addition to this aspect, also look at the organizational and knowledge dimensions.

3 The Hack-Space Integrated Model

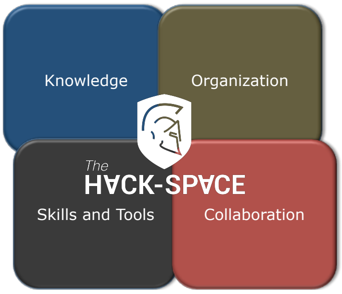

Fig. 1. The Hack Space Dimensions

The integrated model, the Hack Space, was established two years ago thanks to a joint effort between three partners: (i) the Department of Computer Science at the University of Bari, which decided to start a master's degree course in cyber security; (ii) the Apulia Region, by sharing the hypotheses and objectives of the initiative; (iii) the IBM Security, became a project partner providing tools and know-how useful for this purpose.

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.

3.1 Organization

Along this dimension, the overall organization of the intervention was developed. The starting point was the NIST framework with its functions and controls [21]. The NIST Cybersecurity Framework (CSF) provides a risk-based iterative approach for cyber security. The Core framework is the core of NIST CSF, a set of activities, security controls, and guidelines [22]. It consists of five concurrent and continuous functions: *Identify*, *Protect*, *Detect*, *Respond*, *Recover*. The Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop most pervasive and dangerous attacks [23]. Table 1 reports the mapping of the NIST Core Framework with the priority of security controls.

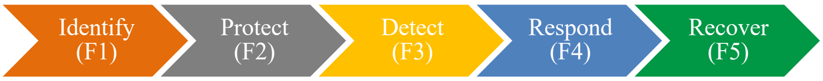

Fig. 2. NIST Cyber Security Functions

Subsequently, 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 in [24], 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).

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

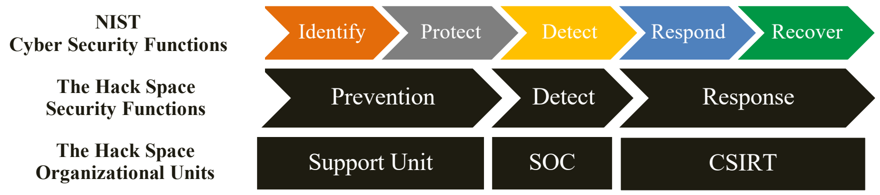

Fig. 3. The Hack Space Security Functions and Organizational Units

Security Operation Center (SOC). The SOC monitors and analyzes activity on networks, servers, endpoints, databases, applications, websites, other systems looking for anomalous activities that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported [25]. A SOC is a centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.

Computer Security Incident Response Team (CSIRT). The CSIRT coordinates incident management and facilitates an understanding of cyber security issues for the community [26]. A computer security incident can involve a real or suspected breach or the act of willfully causing a vulnerability or breach. Typical incidents include the introduction of viruses or worms into a network, DoS (denial of service) attacks, unauthorized alteration of software or hardware, and identity theft of individuals or institutions. Response time is a critical aspect for an effective CSIRT. A quick and effective response can minimize the overall damage to finances, hardware and software caused by a specific incident. Another key point is the ability of the CSIRT to track down the perpetrators of an incident so that the guilty parties can be shut down and effectively prosecuted.

Support Unit (SU). The Support Unit is the unit defined within The Hack Space where all the activities for monitoring the assets of the organization are concentrated, as well as the internal training activities for the prevention and improvement of all the processes and procedures for managing internal security. A final consideration involves: the "enforcement" of the software and infrastructure to minimize the number of incidents that take place over time and all the practices to put in place to face the application security.

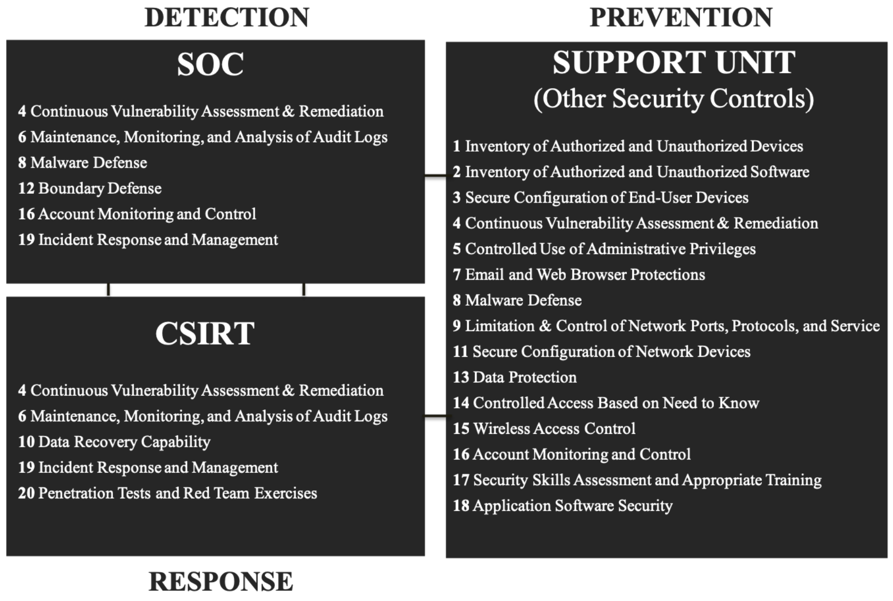
DETECTION
PREVENTION
SOC
4 Continuous Vulnerability Assessment & Remediation
6 Maintenance, Monitoring, and Analysis of Audit Logs
8 Malware Defense
12 Boundary Defense
16 Account Monitoring and Control
19 Incident Response and Management
SUPPORT UNIT
(Other Security Controls)
1 Inventory of Authorized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

Fig. 4. The Hack Space Organizational Model

3.2 Knowledge

Within this dimension and in line with the defined organizational model, the whole curricula of the Master Degree Course in Cyber Security of the University of Bari [27] has been defined. It consists of 120 training credits in a two-year course. The most relevant courses are presented below in Table 2. Furthermore, the project foresees 9 international and 6 national seminars held by world experts in the sector. The seminars are designed to provide students with an up-to-date regulatory framework for the industry, an overview of the frontiers of research and tools to the state of practice in security support.

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 Security Controls 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.

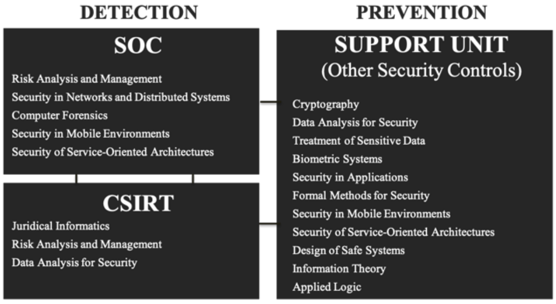
DETECTION
PREVENTION
SOC
Risk Analysis and Management
Security in Networks and Distributed Systems
Computer Forensics
Security in Mobile Environments
Security of Service-Oriented Architectures
CSIRT
Juridical Informatics
Risk Analysis and Management
Data Analysis for Security
SUPPORT UNIT
(Other Security Controls)
Cryptography
Data Analysis for Security
Treatment of Sensitive Data
Biometric Systems
Security in Applications
Formal Methods for Security
Security in Mobile Environments
Security of Service-Oriented Architectures
Design of Safe Systems
Information Theory
Applied Logic

Fig. 5. The Hack-Space Knowledge Model

Table 2. Study plan of Master's Degree in Cyber Security.

YEAR 1	YEAR 2
English Language	Formal Methods for Security
Security in Networks and Distributed Systems	Security in Mobile Environments
Cryptography	Security of Service-Oriented Architectures
Data Analysis for Security	COMPLEMENTARY COURSES
Treatment of Sensitive Data	- Design of Safe Systems
Biometric Systems	- Computer Forensics
Business Organization for Cyber Security	- Juridical Informatics
Security in Applications	- Information Theory
Risk Analysis and Management	- Applied Logic

3.3 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 lab was equipped with the following software platforms provided by IBM Security:

- IBM Security Privileged Identity Manager (PIM) and IBM Security Access Manager (ISAM): help mitigate threats within the organization by centrally managing and controlling the use of privileged access credentials between systems, applications and platforms. This allows you to respond to security regulations, protect sensitive assets and improve security.
- IBM User Behavior Analytics (UBA): analyzes user behavior by promptly highlighting anomalies and atypical patterns.
- IBM BigFix Endpoint Management and Security: constantly monitors the update status of all installed operating systems and applications, highlighting the need to update them with respect to critical security patches. Prioritizes risks and allows vulnerability resolution. Discover, protect and manage thousands of endpoints on over 90 different operating system versions. It allows you to automate operating system migrations, perform real-time endpoint queries to check for malicious files, and install software updates.
- IBM X-Force Threat Intelligence: is a continuously updated knowledge base on the various types of threats that allows to power the remaining systems of the IBM platform by providing useful knowledge to discover and fight possible threats.
- IBM QRadar Security Intelligence: collects events and logs from many sources, including security devices, operating systems, applications, network resources, databases, and access and identity management products. Collects also data from network streams, including Layer 7 data, from switches and routers. Effectively analyses correlation between observed events and promptly highlights any threats. This is the heart of the entire solution.
- IBM WATSON Advisor for Cybersecurity (WfCS): starting from the data collected internally by QRadar, allows the use of cognitive technologies to monitor and analyze security problems that come from numerous sources providing threat intelligence contents. By examining threats from millions of research documents, blogs and news stories, Watson can provide instant insights to help fight the noise of thousands of reports every day, dramatically reducing response times.
- IBM Security AppScan: is a solution that allows, through the static analysis of the source code of a software system, to highlight and eliminate any known vulnerabilities that are present in it. It can be used both to support the software development and maintenance phases [28].

Fig. 6 below shows what we have defined as the "Immune System", that is, how the individual platforms interact with each other and integrate within the organizational model supporting the Security Functions underlying it. In particular, the Detection phase is assigned to QRadar, the Response phase to Watson Advisor and X-Force, while the remaining applications substantiate the Prevention phase. The laboratory is currently made up of 21 workstations with a data center in which the IBM Cloud applications are installed. Each workstation has a VPN Client that connects to the QRadar Model infrastructure, BigFix, PIM, UBA Watson; WinCollector Client for the collection and sending of system logs to QRadar; Client Access Agent for managing privileged credentials; BigFix Client that allows the workstation to exchange data with BigFix. Indeed, every workstation represents a monitored endpoint.

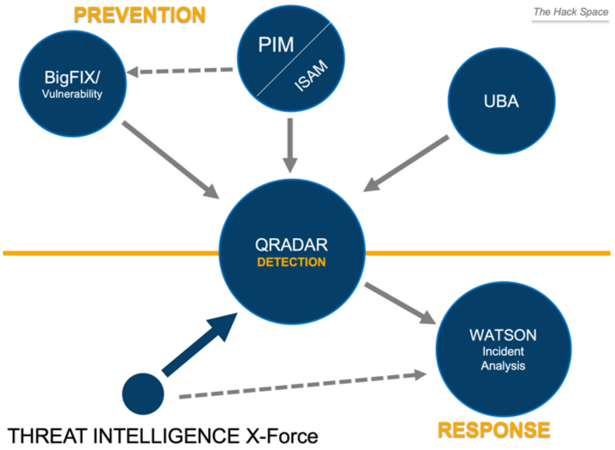

Fig. 6. The Hack Space Immune System

This solution has been implemented to allow serious games to take place [29] during the training courses. Students analyze and perform Red vs. Blue Team objective-based cyber operations as an active approach to establish a defensive posture improvement. The basic idea of Red vs. Blue team countermeasures is a simple war gaming.

A virtual enterprise computer infrastructure is established and the Red Team will attack the infrastructure, whereas, the opposing Blue Team will defend itself against the attack. Red Team must be able to violate a portion of the network and identify vulnerable resources. The ability acquired in trying to achieve this goal is to understand the existence of possible vulnerabilities and weaknesses of the infrastructure, and how to exploit them in order to tamper with systems or steal information. This will not happen through predefined tools, but applying the skills and knowledge acquired during the courses. The ultimate goal is to understand how attackers are able to violate a part of this network, without having the entire list of resources and the various links. Blue Team, on the other hand, must be able to implement all the required security management processes required by the SOC, CSIRT, SU in order to defend itself. To acquire the necessary skills, i.e. Red Team to perform a valid assessment of the infrastructure and Blue Team to correctly manage the security process, the game must have different levels of complexity. Based on Red Team actions and Blue Team responses, changes will be implemented within the infrastructure. The goal is to recreate realistic scenarios as much as possible. In support of the development of serious games and to ensure that each student has clear mind of the role played, from time to time, within the organizational model, the laboratory is physically organized in 4 working islands with 5 positions each. As described in subsection 3.1, the first is dedicated to *SOC*, the second to *CSIRT*, the third to *SU* and, finally, the last island is free of labels and usually used to host the members of the Red Team (Fig. 7).

Fig. 7. The Hack Space Laboratory

3.4 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. Finally, we are also working on the definition of methods and instruments, such as those ones presented in [30] to share contents and knowledge for learning cyber security. Currently these activities are underway.

4 Experimentation and expected results

The Hack Space Model is currently under experimentation and thus we still have no definitive results. The master's degree course in Cyber Security is at the second academic year of progress. About 80 students are involved in the teaching activities, 40 for each academic year. As of today, 6 of the 9 international and 6 national seminars have been held.

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. For the survey, we have chosen to follow the method proposed by Eisenhardt [31] to build theories from case study research. Moreover, we plan to use multiple data collection methods: interviews, document analysis, and questionnaires. The semi-structured interviews will be performed with two groups of participants (using different interview scripts): a) university professors and professional staff from companies involved in the Hack Space project, to collect data about the context; b) students of the master degree course to obtain information about their experience with, perceptions about, and attitudes in being involved in the Hack Space experiences following each course. We will validate the interview scripts by conducting pilot interviews with a group of subjects from each sample as well as through focus groups.

5 Conclusion

This paper has presented an integrated model called "The Hack Space" made of 4 main components: *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 details of the project illustrated are the results of a joint effort between Department of Informatics at the University of Bari, Apulia Region and IBM Security. The overall initiative started two years ago thanks to the master degree course in cyber security promoted by the University of Bari and is currently in its successful second year of execution.

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.

Acknowledgements

We would like to thank the Apulia Region for having partially funded the initiative through the “AVVISO PUBBLICO N.3/PAC/2017 Piano di Azione e Coesione - Azioni aggiuntive per il rafforzamento dei corsi di studio innovativi erogati dalle Università pugliesi”.

A special acknowledgement goes to Prof. Teresa Roselli for having contributed with her effort, ideas and suggestions to the production of the Hack Space model.

References

1. Clusit, *Rapporto 2018 sulla Sicurezza ICT in Italia*. Copyright © 2018 CLUSIT.
2. Danilo Caivano, María Fernández-Ropero, Ricardo Pérez-Castillo, Mario Piattini, Michele Scalera, (2018), "Artifact-based vs Human-Perceived understandability and modifiability of refactored business processes: An experiment", JOURNAL OF SYSTEMS AND SOFTWARE, Volume 144, pp. 143–164, doi: 10.1016/j.jss.2018.06.026., (October 2018).
3. IBM, *X-Force Threat Intelligence Index 2018* . IBM (2018).
4. 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).
5. 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)
6. 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).
7. Mainetti, L., Patrono, L., Stefanizzi, M. L., & Vergallo, R.. An innovative and low-cost gapless traceability system of fresh vegetable products using RF technologies and EPCglobal standard. Computers and Electronics in Agriculture, 98, 146-157, doi:10.1016/j.compag.2013.07.015 (2013).
8. Alessandrelli, D., Mainetti, L., Patrono, L., Pellerano, G., Petracca, M., & Stefanizzi, M. L., Implementation and validation of an energy-efficient MAC scheduler for WSNs by a test bed approach. Paper presented at the 2012 20th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2012, (2012).
9. Danilo Caivano, Daniela Fogli, Rosa Lanzilotti, Antonio Piccinno, Fabio Cassano, "Supporting end users to control their smart home: design implications from a literature review and an empirical investigation". JOURNAL OF SYSTEMS AND SOFTWARE, Volume 144, October 2018, pp. 295-313, doi: 10.1016/j.jss.2018.06.035, (2018).
10. Frankie E Catota, M Granger Morgan, & Douglas C Sick, *Cybersecurity incident response capabilities in the Ecuadorian financial sector*. Journal of Cybersecurity, https://doi.org/10.1093/cybsec/tyy002 (2018).
11. FORBES, https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#38966fe5a6b3, last accessed 2018/11/12
12. CIO, Top U.S. universities failing at cybersecurity education: https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html, 2018/11/12
13. F. B. Schneider, "Cybersecurity Education in Universities," in *IEEE Security & Privacy*, vol. 11, no. 4, pp. 3-4, July-Aug. 2013.
14. D. Jacobson, J. Rursch , & J. Idziorek, Workshop: *Teaching computer security literacy to the masses: A practical approach*. Frontiers in Education Conference Proceedings (pp. 1-2). Seattle, WA (2012).
15. J. T. McDonald and T. R. Andel, "Integrating Historical Security Jewels in Information Assurance Education," in *IEEE Security & Privacy*, vol. 10, no. 6, pp. 45-50, Nov.-Dec. 2012.
16. Yonemura, K., Komura, R., Takeichi, Y., Yajima, K., & Sato, J., *Practical Security Education on Operational Technology using Gamification Method*. 7th IEEE International

Conference on Control System, Computing and Engineering (ICCSCE 2017). Penang, Malaysia (2017).

17. S. Jadhav, T. Oh, Y. H. Kim and J. N. Kim, "Mobile device penetration testing framework and platform for the mobile device security course," *2015 17th International Conference on Advanced Communication Technology (ICACT)*, pp. 675-680, Seoul, 2015.
18. Y. Ban, K. Okamura and K. Kaneko, "Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education," *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, pp. 699-704, Hamamatsu, 2017.
19. A. Papanikolaou, V. Karakoidas, V. Vlachos, A. Venieris, C. Ilioudis and G. Zouganelis, "A Hacker's Perspective on Educating Future Security Experts," *2011 15th Panhellenic Conference on Informatics*, pp. 68-72, Kastonia, 2011.
20. A. S. Andreatos, "Designing educational scenarios to teach network security," *2017 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1606-1610, Athens, 2017.
21. SANS, The CIS Critical Security Controls Are the Core of the NIST Cybersecurity Framework*,* https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download, last accessed 2018/11/13.
22. NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, last accessed 2018/11/13.
23. Ioannis Agrafiotis, Jason R C Nurse, Michael Golds, Sadie Creese, & David Upton, *A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate*. Journal of Cybersecurity, https://doi.org/10.1093/cybsec/tyy006 (2018).
24. LaPiedra, J. (2002), *Information Security Process,* https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197, (2002), last accessed 2018/11/13.
25. NCSC, *Building a SOC: start small,* https://www.first.org/resources/guides/Factsheet_Building_a_SOC_start_small.pdf, last accessed 2018/11/10.
26. John Haller, Samuel A. Merrell, & Matthew J. Butkovi, Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0. Software Engineering Institute, (2011).
27. Dipartimento di Informatica, Bari (DIB), *Laurea in Sicurezza Informatica*, https://www.uniba.it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi/sicurezza-informatica-ta/cds-sicurezza-informatica, last accessed 2018/11/12
28. Fernández-Sáez, A., Genero, M., Chaudron, M., Caivano, D., & Ramos, I. (2014). Are Forward Designed or Reverse-Engineered UML diagrams more helpful for code maintenance?: A family of experiments. *Information and Software Technology, Volume 57, January 2015, Pages 644-663, ISSN 0950-5849, doi: 10.1016/j.infsof.2014.05.014*.h
29. Kosa, M., Yilmaz, M., O'Connor, R., & Clarke, P., *Software Engineering Education and Games: A Systematic Literature Review*. Journal of Universal Computer Science 22 (12) : 1558-1574, December 2016.
30. Di Nitto, E., Mainetti, L., Monga, M., Sbattella, L., & Tedesco, R., Supporting interoperability and reusability of learning objects: The virtual campus approach. Educational Technology and Society, 9(2), 33-50. Retrieved from www.scopus.com, (2006).
31. Eisenhardt, Kathleen M. "Building Theories from Case Study Research." *The Academy of Management Review* 14, no. 4: 532-50. http://www.jstor.org/stable/258557, (1989)