Cooperative Information Security/ Cybersecurity Curriculum Development

Abdelaziz Bouras[1(✉)], Houssem Gasmi[1,2], and Fadi Ghemri[1]

[1] Computer Science and Engineering Department, Qatar University, PO Box 2713 Doha, Qatar
{abdelaziz.bouras,houssem.gasmi,fadi.ghemeri}@qu.edu.qa
[2] Disp Lab, Université Lumière Lyon 2, 160, Bd de L'université, 69676 Lyon, Bron, France

Abstract. It is often difficult to meaningfully convey concepts like security incident management cycle, information sharing, cooperation, as well as the roles of people, processes and technology in information and cybersecurity courses. Such complexity requires immersive and interactive learning based on continuous cooperation between industry and academia. In this paper we highlight the ongoing industry/university cooperative effort towards an cooperative schema to enforce the Information Security and Cybersecurity Curriculum development within an existing Master of Computing.

Keywords: Cooperative education · Cybersecurity · Competency frameworks Mentorship · Ethical Hacking · Tabletop

1 Introduction

The past decade in Qatar has seen a rapid economic development with increasingly fast advances in many fields, particularly in new technologies, due to its fast growing economy. Qatar is currently building large infrastructures in various domains (services, industry, health, tourism, etc.) as part of the Qatar National Vision 2030 [1]. As the country has become more connected, traditional threats from hackers have been rapidly and continuingly changing to include more malicious players such as terrorists, organized criminal networks, and in some cases foreign industrial/government cyber espionage. Critical infrastructures such as power plants, air-traffic and fuel refineries are increasingly targeted by cyber-attacks (ex. Shamoon virus crippled thousands of computers at Qatar's RasGas in 2012). The last must example is when Qatar's state news agency was hacked by anonymous party, this incident provoked a serious diplomatic crisis in the region.

From the education side, it is often difficult to meaningfully convey concepts like security incident management cycle, information sharing, cooperation, as well as the roles of people, processes and technology in information and cybersecurity courses. Such complexity requires continuous interaction between industry and academia to provide immersive and interactive learning experience to students. This will help building innovative solutions and developing new skills and competencies [2]. Qatar's academic community has an interesting young history of responding to the needs of

J. Hu et al. (Eds.): MONAMI 2017, LNICST 235, pp. 178–187, 2018.
https://doi.org/10.1007/978-3-319-90775-8_15

industry. Since few years the cybersecurity topics where highlighted by the Qatar National Research Fund (QNRF)[1] research programs, and dozens of programs have been funded. Some of these programs involve industry partners and stakeholders.

Globally, universities play an important role in multiple ways to contribute in the development and expansion of local competencies, especially in cyber security which is show many lacks related to the content of curriculum, local universities are called to respond to the local needs, by providing efficient local competencies: through the provision of skilled graduates who become key players in local industry; through the conduct of long-term fundamental research that contributes to the science base and understanding available to private firms; through the promotion of an atmosphere of intellectual diversity that tolerates different approaches to the solution of technical problems; through direct collaboration with industry both on specific projects and in longer term relationships. Consequently, the state of Qatar has to invest in the security education, convinced by the idea of a very competitive future world, based on the capacity of countries to develop a well protected knowledge-based economy.

2 Need for Cybersecurity Competency Frameworks

Several paradigms related to information security and Cybersecurity dealing with the complex, multidisciplinary nature of the field have been defined. [3] for instance observed that cybersecurity comprises three planes of study:

- *Operations*: The day-to-day functioning of the information security task.
- *Governance*: The management of the cybersecurity function, including internal policies and procedures as well as law and policy.
- *Education/training*: Transfer of knowledge to cybersecurity professionals and users, ranging from teaching specific skills and competencies to providing systemic understanding and life-long learning.

Within a recent QNRF research project (PROSKIMA NPRP7-1883-5-289) [4], interviews have been conducted in Qatar with Information Technology (IT) representatives and security experts from major companies, organizations and ministries to have their feedback regarding the last point (Education/Training). These interviews highlighted the growing needs for enhanced competencies for Cybersecurity. Consequently, higher educational institutions need to reflect such evolution in their training curricula. Trained students will be able to tackle real world challenges efficiently.

Moreover, to have a clear picture and substantial update, a series of workshops titled "Industry Integrated Engineering and Computing Education Curriculum"[2] has been organized at Qatar University, through its Computer Science and Engineering (CSE) department, where professionals and experts from different organizations and industries met with the academics to identify relevant Cybersecurity competency frameworks, that need to be

[1] https://www.qnrf.org/en-us/.

[2] http://www.qu.edu.qa/newsroom/Engineering/2nd-Industry-Integrated-Computing-Education-Curricula-Workshop-held.

used to enhance existing university curricula or to introduce new integrative programs. Discussions and outcomes of this session are summarized in the Table 1 here below.

Table 1. Outcome from industry/academia brainstorming sessions

Activity	Competencies
Identify	• Security Analysis(Industrial, cloud, IOT, Big Data) • Risk (Identify, User baseline, Perform risk assessment externally, Management, Governance) • Fault forecasting (Before, Lifetime)
Protect	• Design and Implement security mechanism (Authentication, Authorization, Confidentiality, Integrity) • Perform Security Auditing (Gaps, Vulnerabilities) • Follow levels of Compliance (Standard, Maturity, Training, Audit, Review)
Detect	• Deploy and configure intrusion detection system (IDS)/ Monitoring • Analyze Data (logs, application…) to detect threats • Monitor and detect incidents and threats
Respond	• Mitigate and stop attacks • Build a Proper Communication with stakeholders/ Media • Build Information Security incident response skills and awareness
Recover	• Perform all business continuity actions (fault Removal, Data Recovery)
Cross- Cutting (Applies to all function above	• Understand the business process • Build Policies/Framework/standard/Compliance/ Processes • Be up to date regarding Technology (Mobile, Cloud, Cryptography, Electronics, Network, OS, PCs, Directory, Database, Analytics, Linux, Open Standard)

3 Achievement Through Industry/University Cooperative Schema

It is commonly agreed that cybersecurity is more about processes than technology and the answer to the cyber-related security challenges are not solely about information technology and technical solutions but must also involve other related topics such as sociology, national defense, economics, political science, diplomacy, history, and many other social sciences [5].

In our case, and based on the competency needs highlighted earlier, we propose to enforce the current Master of Computing[3] with such vision. Because a global change in the structure of the curriculum needs long time due to several committees' validations (department, college, university), we believe that the achievement of such complete cooperative schema needs the adoption of at least two steps:

[3] Study plan: http://www.qu.edu.qa/engineering/computer/programs/phd/studyPlan.php
Courses: http://www.qu.edu.qa/engineering/computer/programs/phd/cs/csListOfCourses.php.

- Step1: Enforce the current curricula, by adding new cooperative tools (Mentorship, Reflexive Sessions, Industry Projects, Specific courses…). This is highlighted in this paper.
- Step2: Transform the Master's curricula to achieve collaborative sandwich programs (alternate stays of students between industry and university, for ex. Rotation every 2 weeks). A deep involvement of the stakeholders is necessary to shape such relationship and analyze additional challenges related to the certifications, etc. This step is beyond the scope of this paper.

In this following sections we mainly focus on the main components of the first step.

3.1 Project Mentorship

The aim of this component is to provide the students (trainees) with practical experience under the mentorship of two mentors, one from the university and the other from the company. While certainly useful, this approach has scalability issues, since finding mentors for all students is often difficult to achieve. In our case, this should not be a problem to be initiated for the Master of Computing due to its reasonable size. However, its generalization to the Bachelor sections will definitely meet such limitations. Solutions could be found within the TIEE (Engineering Technology Innovation and Engineering Education Unit) for which the students' professionalization is one of its main objectives. In the current schedule (3 years program), all the courses are given during the end of afternoons (5 pm to 8 pm), with an average of 2 to 3 courses per week. The rest of the day the students are free (most of them are working in local companies). Each course last 15 weeks. The final project or thesis of the students has, in general, no connection with the students' workplace him/her self, though several projects deal with industrial implementations. So, there is no direct connection between the students' companies and the Master program.

In the new proposal, the companies need to be involved in the program in proposing projects and providing internal mentors. The student is either a freshman hired by the

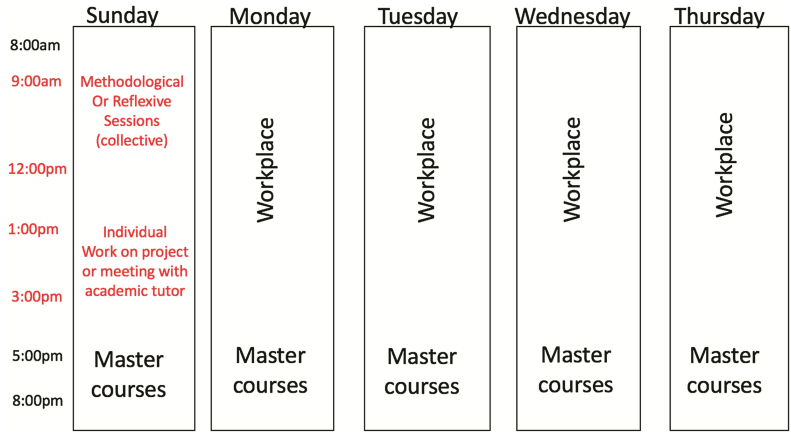

Fig. 1. Typical weekly schedule for the students

company and provided a salary, or an internal IT engineer or technician (having a bachelor level or equivalent) to be trained within this new cooperative process.

The schedule of the courses will be slightly changed to accommodates the students' needs. The department discusses the projects with the partner companies, and signs an agreement with both the student and the company. The student (becoming a worker at the company) will stay one day every week at the university, the rest of the week he/she works on the project in the company. This university day will focus on the assessment of the students' projects (to be made by the student's mentor), with reflexive sessions where the students exchange their experience and discuss common issues related to their work. It will also deal with methodological sessions where the students are coached on project management issues, and follow seminars and workshops related to specific needs of cybersecurity that the lectures do not cover (social issues, policy issues, etc.). Figure 1 highlights the Typical weekly schedule for the students.

During the students stay at the company, he/she receive the visit of his/her university mentor at his/her workplace several times, and make presentation of his/her achievement in front of his/her both mentors (university mentor, company mentor).

Table 2. Cooperative visit planning

Visit	Objectives	Assessment actions
1	Designing a project that is profitable for the company and interesting for student learning	• Mutual presentation • Visit of the company • Discussion about the identified projects and their aims • Selection of a project and definition of the working aims for the student
2		• Presentation and validation of the student's project deliverables • 1st student assessment (behaviour at work, technical knowledge, communication skills)
3	Assessing the progressive participation in the project and the involvement in its management	• Presentation of the project's progress (used methods, intermediate results, student learning progress) • 2nd student assessment (concrete achievements, behaviour at work, technical achievements, management and communication skills)
4	Assessing the ability of management of the project in progressive autonomy	• Presentation of the project's progress (used methods, intermediate results, student learning progress) • 3nd student evaluation (concrete achievements, behaviour at work, technical knowledge, management and communication skills)
5	Finalising the project and thesis writing	• Final presentation of the project (used methods, final results, prospective steps within the company) • Discussion of the project thesis document (to be finalised by the student for the Master Jury) • Last student assessment (concrete achievements, behaviour at work, technical knowledge, management and communication skills)

Table 2 explains the objectives and the tasks of each visit (with an average of one visit per term). Each meeting is specific to the period of the year and to the project's progress. The assessment mainly deals with the concrete achievements of the student, his/her behavior at work and team collaboration, the technical knowledge and the way the student is applying the knowledge he/she acquired at the university, the management of the projects' tasks, the student's communication skills, etc.

3.2 Use of Simulation and Ethical Hacking

Beyond their daily project and courses, the students need to continue participating in other specific activities designed for them, such as the department yearly contest on Ethical Hacking. Such contest is an important exercise for the students around Computer Security. They collectively play the role of Ethical Hackers and have the opportunity to understand the weaknesses and vulnerabilities of computer systems to be able to use this knowledge to assess the security robustness of a target system in a lawful and legitimate manner. In general, the ethical hacker exploits open-source tools for forensic analysis and information gathering to disclose encrypted contents. An Ethical Hacker is a professional who uses his knowledge to assess the security robustness of a target system in a lawful and legitimate manner. An ethical hacker can also investigate cybercrimes by exploiting tools for forensic analysis and information gathering to disclose hidden contents ("he is the good guy").

During the contest, the students are mentored to perform basic ethical hacking activities including information gathering, forensic analysis and secrets' disclosure. As an example, the last Ethical Hacking Workshop[4] had three days duration, 2 first days dealing with the "theory and practical applications" and the last day focusing on a "Ethical Hacking contest".

The covered topics during the workshop first days were mainly:

- Ethical Hacking with Linux
- Data hiding techniques
- Information gathering
- Forensic analysis
- Steganography and cryptography.
- Password hacking
- Wireless communication security.
- WiFi security

During the Ethical Contest of the 3rd day, the students were requested to analyze the evidences hidden in a USB stick. The USB stick has been taken from a person involved in a case of industrial secrets stealing. The secrets were related to diagrams and schemes for machineries and equipment in the field of oil and gas extraction and refining. The suspect was able to partially delete the evidences. The students were asked to investigate the USB sticks and identify all the people (name and surname) involved in the case.

[4] http://www.qu.edu.qa/engineering/computer/ethical_hacking_contest.php.

Each of the evidence discloses information for retrieving the next one. All the evidence files were containing a set of information that should be exploited for the search and identification of the next one.

A presentation by Q-CERT[5] (Qatar Computer Emergency Response Team) was also given during this last day on the policy side, to initiate the students to the national cyber security posture, advices on policies and security standards.

Q-CERT is a national, Government sponsored organization, setup under the auspices of Ministry of Transport & Communications (MOTC). Q-CERT has been instrumental in building resilience into the critical information infrastructure of Qatar and is working to harmonize the secure use of technology through best practices, standard policies, risk mitigations and dissemination of valuable information.

Some demonstrations of Q-CERT projects (Botnet Eradication, Malware Analysis LAB, Threat Monitoring System, etc.) have concluded this day.

Such workshops and contests will be continued all the coming years. The participation of governmental organizations and industrial companies is important. Siemens are Thales groups are already ready to take part in the next workshops.

3.3 Tabletop Exercises for Cybersecurity Education

As tabletop exercises are used to give students the opportunity to practice cybersecurity concepts using real world scenarios, this component is also considered. This deals with interactive learning tools and approaches that are based on the idea of training students through role playing on hypothetical problems. The scenarios and the problems are generally derived from real life situations and the method has been successfully used in classroom environment with students in other contexts [6]. Such tabletop approach is being popular and several tabletop exercises are developed by universities and government agencies. For instance, some tabletop templates developed by the Security Operations Center (SOC) of Washington State could be found in [6]. The goal of these templates is to increase the security situational awareness and to facilitate discussion of incident response in as simple a manner possible, targeting a time range of 15 min.

In our case, the scenarios are conducted under the responsibility of the "Cybersecurity Chair", funded by Thales company (within a Memory of Understanding -MoU- signed between Thales and Qatar University on Nov. 2013)[6]. The "Cybersecurity Chair" is intended to enforce the MoU "*to provide training opportunities for Qatari students on new and emerging technologies in the field of cybersecurity. Its aim is to establish cooperation between the academic environment and industry on information systems and data security and related associated services."* Hence, the Cybersecurity proof of concepts and scenarios are conducted under the responsibility of the Chair in the offices and labs of Thales, situated in QSTP (Qatar Science Technology Park) in Doha. The design of the scenarios emphasizes on the practice of cooperation, and the familiarization of students to their

[5] http://www.qcert.org/.

[6] https://www.thalesgroup.com/en/worldwide/press-release/qatar-university-teams-thales-open-cybersecurity-chair.

responsibilities, in addition to practice crisis management, test experimental solutions for scenarios, and identify shortcomings in resources, procedures or capabilities.

The Cybersecurity Chair has also implemented a useful package of cybersecurity courses that students have to follow (still under validation by the CSE department):

- Cybersecurity and Cyber Physical Systems
- Cybersecurity in software development
- Cybersecurity in industrial systems
- Cybersecurity Management for Business Managers
- Cybersecurity Management for IT managers/professionals
- SAP Security

The students have also the opportunity to participate in the recently awarded research projects (hereunder) and be part of a cybersecurity experts' network:

- NPRP10-0206-170360: Intrusion Detection System (IDS) for Industrial Control Systems – which uses a systematic study of machine learning schemes to build IDS for Industrial Control Systems. This project aims at building of a Test-Bed environment from oil/gas and petro-chemical industry.
- NPRP10-0105-170107: Cyber Security, Monitoring, Diagnostics, and Resilient Control, Recovery of Cyber-Physical Industrial Control Systems – which deals with the design and development of proactive intrusion attack monitoring and attack resilient control recovery methodologies and toolkits. It mainly aims at building of a simulation environment for Industrial Control Systems.

The main objectives of the tabletop exercises are to explain, in an easy way, the general concepts in cybersecurity, such as the global infrastructure and the discovery process and management of security incidents. Tabletop exercises are an invaluable training tool to prepare the students and train them on practical methods applied in the industry. Some authors such as [7] proposed specific methods that reduce the work load from the instructor perspective, in order to encourage more educators to try the tabletop exercises. There is always a test period where the exercises are applied only to one course and gradually introduce it to other courses. The main benefit of the tabletop method is that it provides scalability to deliver practical experience to a large number of students by one instructor. While our program in Qatar University does not have a real problem of scalability because of the reasonable size of the Master and the use of mentors to implement the internship. Moreover, the students will be exposed to real live systems under the supervision of their company mentors.

In order to provide a more dynamic experience, the exercise format includes a scenario based, but adaptable opponent. In [7], the students are divided into two kinds of teams. Blue teams represent the security or investigative teams of various actors on the defensive side, such as law enforcement, national Computer Emergency Response Team (CERT), Internet Service Provider (ISP), media, industry, etc. The Red team represents a malicious actor (defined by the instructor), such as criminal group, hacktivist organization, hostile intelligence service, etc.

Finally, tabletop instructions should be relatively short and require several teams to fully develop their role in the exercise. The tabletop exercise scenario should cover general cybersecurity concepts and not go into too much technical detail.

4 Conclusion

As the country needs to be prepared to protect its infrastructures and sensitive data, contemporary complex issues related to information security and cybersecurity need to be mastered. A strong collaboration between the employment, government, and educational sectors becomes the key for such challenge. This paper highlighted the current initiatives at Qatar University to enforce the Master of Computing curricula, in adding new cooperative tools (Mentorship, Reflexive Sessions, Tabletop methods, Simulation and Ethical Hacking, Specific courses, etc.). International certifications, such as IFIP IP3, ISC2 and SANS for example, tackling new cybersecurity requirements will also bring new issues (risk assessment, threat modeling and design, vulnerability management, etc.) and are gradually integrated within the curricula.

The presented approach is a necessary step before the prospective implementation of a real cooperative program between industry/university based on a sandwich program, where the students gradually develop their skills thanks to their alternate stays between the university and the company (for example 3 weeks in the company and 3 weeks in the university). This needs a serious involvement of all the stakeholders and a substantive change in the Master structure.

Acknowledgement. This publication was made possible by NPRP grant # NPRP 7-1883-5-289 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

1. Qatar National Vision 2030. www.qu.edu.qa/pharmacy/components/upcoming…/Qatar_National_Vision_2030.pdf. Accessed 15 Sept 2017
2. Bouras, A., Veillard, L., Tralongo, S., Lenir, M.: Cooperative education development: towards ICT reference models. In: International Conference on Interactive Collaborative Learning (ICL), pp: 855–861. IEEE Xplore (2014)
3. Kessler, G.C., Ramsay, J.: Paradigms for cybersecurity education in a homeland security program. J. Homel. Secur. Educ. **2**, 35–44 (2013)
4. Veillard, L., Tralongo, S., Bouras, A., Le Nir, M., Galli, C.: Designing a competency framework for graduate levels in computing sciences: the Middle-East context. In: Auer, M.E., Guralnick, D., Uhomoibhi, J. (eds.) ICL 2016. AISC, vol. 544, pp. 330–344. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-50337-0_31
5. Kessler, G.C., Ramsay, J.D.: A proposed curriculum in cybersecurity education targeting homeland security students. In: 47th Hawaii International Conference on System Science, pp. 4932–4937 (2014)

6. Security Operations Center (SOC), Washington State. http://soc.wa.gov/node/413. Accessed 15 Sept 2017
7. Ottis, R.: Light weight tabletop exercise for cybersecurity education. Homel. Secur. Emerg. Manag. **11**(4), 579–592 (2014)