Network Security and Digital Forensic Curricula Development for private Institute of Higher Learning (IHL) in Malaysia

Zuraidy Adnan
Faculty of Communication, Visual Art and Computing
Universiti Selangor (UNISEL)
Malaysia

Mohd Fahmi Mohamad Amran
Faculty of Defence Science and Technology
National Defence University of Malaysia (UPNM)

Norhayati Mohd Amin
Center for Foundation and General Studies
Universiti Selangor (UNISEL)
Malaysia

Muhammad Fairuz Abd Rauf
Faculty of Communication, Visual Art and Computing
Universiti Selangor (UNISEL)
Malaysia

ABSTRACT
In this paper we share our experience in developing hybrid majors' undergraduate program which combines network security and digital forensic using Information Security and Critical Information and Communication Infrastructure Protection (ISCIP) common body of knowledge (CBK) as a reference. We also share the challenges and parallel effort, mostly from government, that help us in developing this program.

Keywords
Network Security, Digital Forensic, Curricula Development, Private IHL.

1. INTRODUCTION
Network security and digital forensic field nowadays has become more matured in parallel with the boost of Internet usage all around the world. Computers and Internet were used for communications widely, in various kinds of online interactions and transaction [11]. In this period of time, issues involving security has become more pressing problem for both nationally and internationally [12].

Process of developing a new curriculum cannot escape from the use of CBK (Common Body of Knowledge). CBK can be viewed as the conceptual means that defines the knowledge, which is considered essential for the cognitive background and the required skills of the professional [13]. The CBK can act as a tool to (a) characterize the content of a knowledge field, (b) provide an overview of a domain and at the same time a snapshot of its contents, (c) clarify the boundaries of the field with regard to other disciplines, and (d) can provide foundations for curriculum development, training program/seminar design or professional certification and accreditation [13]. There is no direct CBK that has been developed under Network Security and Digital Forensic flagship. Network Security and Digital Forensic always had been describing in two different domains in Information Security CBK.

Nowadays, there's a lot of organization body who developing and enhancing CBK for information security (IS) [1]. Among them are like Representative on Information Assurance Curriculum Development, NIST, ISC^2, ASIS, Oney, CPP, and also Information Security and Critical Information and Communication Infrastructure Protection (ISCIP) CBK, that has been developed by Information Security and Critical Infrastructure Protection Research Group, Department of Informatics, Athens University of Economics and Business (AUEB) [13]. Our goal is to use two of the main domain in the CBK that has been develop by this organization, namely, (a) network, web, and communication security and (b) forensics, to develop new undergraduate curriculum under Network Security and Digital Forensic flagship, as these field has become more mature nowadays [6].

The new ISCIP CBK, as proposed in [13], have ten domains, and has been develop for graduate student's curricula. The domains cover (1) Prerequisite Knowledge, Basic Terms and Security Models, (2) Ethical, Social, Psychological and Legal Issues, (3) Cryptography, (4) Software Security, (5) Access Control and Authentication Access Control, (6) Network, Web, and Communication Security, (7) Database Security, (8) Forensics, (9) Information Systems Security Management, and (10) Physical Security and Critical Infrastructure Protection.

2. COURSE VISION
2.1. The Challenges
In [7], it describes Information Assurance (IA) in many points of view. They were looking in Academia, Industry, and Government perspectives, on how these three most important stakeholders sees Information Assurance. We are looking from the same perspectives as they were, while building this Network Security & Digital Forensic for the undergraduate students.

As discussed in Institutional Program Goals subtopic, the first objective for private IHLs in Malaysia is to reduce gaps between academic curriculum and the industrial needs. The course that has been developed is seen as a bridge for the students before they enter the industry as knowledgeable and skillful workers [2]. Still, principles that underlie in every course inside it are emphasized. The bridge that connects

students with the industry is the approach that is taken to educate the students [8].

2.2. Institutional Program Goals

Generally, private IHL in Malaysia are aiming to be regional ICT faculty producing knowledgeable graduates for local and international employment. Its mission is to enhance student's capability by providing highest quality of education with up to date curriculum and professional certifications with continuous research and development (R&D) support [4].

The main objectives for private IHL in Malaysia is (1) to reduce the gaps between the academic curriculum and the industrial needs, (2) to produce knowledgeable student incorporate positive attitude, soft skills, and ICT skills set, and (3) to equip competence academic staff with up-to-date technology, dynamic feature, with continuous monitoring ICT industry [4].

Seven strategies were implemented in order to achieve the objective, which are, (1) offering academic program align to the industrial need, (2) identify & coordinate relevant professional certification and ICT skills training, (3) acquiring MSC Institute of Higher Learning (IHL) status, (4) collaboration with other IHL on curriculum development, (5) Training the lecturers with up-to-date ICT skills set, (6) R&D and consultancy activity among academicians, and (7) leveraging on available facilities [3].

3. NETWORK SECURITY AND DIGITAL FORENSIC ATTRIBUTES

In this new curricula development, we highlight two out of ten domains that have been proposed in new ISCIP CBK (Theoharidou et al., 2008), namely, (1) Network, Web, and Communication Security and (2) Forensics. The reasons to take these two domain to be blended in one course are, (1) Network, Web, and Communication Security and Forensic are the nearest domain in ISCIP CBK that can we used to develop Network Security and Digital Forensic for undergraduate students, and (2) there are predetermined relevant topics that we can refer in creating subjects for the course. ISCIP CBK for both domains is as shown in Table 1.

Table 1: A portion of new ISCIP CBK to develop new Network Security and Digital Forensic course

Domain 6: Network, Web, and Communication Security	Domain 8: Forensics
Network Security Protocols Cryptography Wireless Network Security Distributed Systems Secure Networking Attacks, Intrusions and Malware IDS and Malicious Software Protection Security Network Technologies Specific Network Systems Network Forensics Legal Issues	Steps Data Collection Network & Web Forensics Database Forensics Hardware Forensics Data Usage Prerequisites Psychology

The team has been created in order to propose subjects for this new program. The team then develops new subjects using both domains that have been extracted from ISCIP CBK. The subjects which has been developed is shown in Table 2.

Table 2: Subjects that has been develop referring to domain 6 and 8 in ISCIP CBK.

Network Security	Digital Forensics
1. Computer & Network Security 2. Mobile & Wireless Security 3. Hacking & Countermeasures 4. Hardening Network Systems 5. Data Security & Cryptography 6. Computer Ethics	1. Digital Forensic 2. Digital Data Recovery 3. Digital Evidence & Computer Forensic 4. Cybercrime & Digital Investigation 5. Forensic Tools & Techniques 6. Forensic Analysis

The mapping between our developed courses versus ISCIP CBK as in Table 3.

Table 3: Domain 6 ISCIP CBK versus Developed Course

ISCIP CBK	Developed Course
Domain 6: Network, Web, and Communication Security	Network Security
1. Network Security Protocols 2. Cryptography 3. Wireless Network Security 4. Distributed Systems 5. Secure Networking 6. Attacks, Intrusions and Malware 7. IDS and Malicious Software Protection 8. Security Network Technologies 9. Specific Network Systems 10. Network Forensics 11. Legal Issues	1. Computer & Network Security 2. Mobile & Wireless Security 3. Hacking & Countermeasures 4. Hardening Network Systems 5. Data Security & Cryptography 6. Computer Ethics

Part 1, 4, 5, 8, and 9 in ISCIP CBK is covered by Computer & Network Security subject in our developed course. Part 2 in ISCIP CBK is covered by Data Security & Cryptography subject. Part 3 in ISCIP CBK is covered by Mobile & Wireless Security subject. Part 5 in ISCIP CBK is covered by Hardening Network Systems subject. Part 6 and 7 in ISCIP CBK is covered by Hacking and Countermeasure subject, and lastly part 11 is covered by Computer Ethics subject. Part 10 of ISCIP CBK is covered in Digital Forensic domain of our developed curricula.

It seems that our Computer and Network Security subject handling a lot of ISCIP CBK domain 6. All parts that covered by Computer and Network Security subject are represented in form of chapters. This subject is the most important subject in this program, since it covered a lot of ISCIP CBK parts. Researcher prioritize this subject by putting higher grade as passing grade (grade B) compared to other major subject. Researcher also put this subject as a prerequisite for other major subject. This is to ensure that the student is focused and serious while attending this subject.

Table 4: Domain 8 ISCIP CBK versus Developed Course

ISCIP CBK	Developed Course
Domain 8: Forensics	Digital Forensics
1. Steps 2. Data Collection 3. Network & Web Forensics 4. Database Forensics 5. Hardware Forensics 6. Data Usage Prerequisites 7. Psychology	1. Digital Forensic 2. Digital Data Recovery 3. Digital Evidence & Computer Forensic 4. Cybercrime & Digital Investigation 5. Forensic Tools & Techniques 6. Forensic Analysis

The approach of forensic domain in ISCIP CBK is mapping the steps of general forensic process. In our developed course, researcher try to expand the steps into a wider scope. The steps approach in ISCIP CBK is repeatedly and redundantly explained in the subjects in our developed course. This is to ensure that the critical forensic steps is planted in student's mind.

4. PARALLEL EFFORTS

4.1. Government Effort (Industry)

Malaysia via Malaysian Digital Economy Corporation (MDEC) is focusing in developing Malaysia Digital Economy through various program to assist technology enthusiast to establish themselves in digital economy world. The programs developed by MDEC are tailored for four talent group, which is, (1) primary and secondary students, (2) undergraduates, (3) fresh graduates and working professional, and (4) digital marker [9].

Two programs are offered for primary and secondary school students, namely, Digital Tech @ Schools program which encourages the use of digital as a tool for educators while embedding computing skills into the school curriculum. The second is eAspirasi immersion program which encourages promising talents to consider enrolling into IT courses at top Institutions of Higher Learning in Malaysia.

For undergraduates, MDEC are working closely with Institutes of Higher Learning (IHLs), the Economic Planning Unit (EPU), and the Ministry of Education (MoE) to develop IT-based graduate courses to ensures a steady pool of quality skilled workers. Technical Vocational Education and Training (TVET) institutions are also deployed to increase diploma and certificate employability.

For fresh graduates, instead of using poaching approach, MDEC change their approach towards coaching approach that develops existing talent through certification programs. Long-term, a sustainable industry-led talent development model will expand the IT-savvy workforce in Malaysia.

Digital marker program is a joint public-private-academia initiative to transform Malaysian youth from digital users to producers in the digital economy. This includes skills such as coding, app development, 3D printing, robotics, embedded programming and data analytics; all of which will ultimately help to strengthen problem solving and creativity amongst our future generation.

Instead of government direct effort, their effort in supporting fourth Industrial Revolution also consider as a big push for the development of this program [5]. Fourth Industrial Revolution or popular referred by the term "Industry 4.0", is the term referring to end-to-end digitization of all assets and integration into digital ecosystems with value chain partners. The difference between Industry 4.0 and Industry 3.0 is for Industry 3.0 focuses more on automation and single machines and processes while Industry 4.0 provides comprehensive coverage of new technologies to create value. Figure 1.0 shows the framework for Industry 4.0:

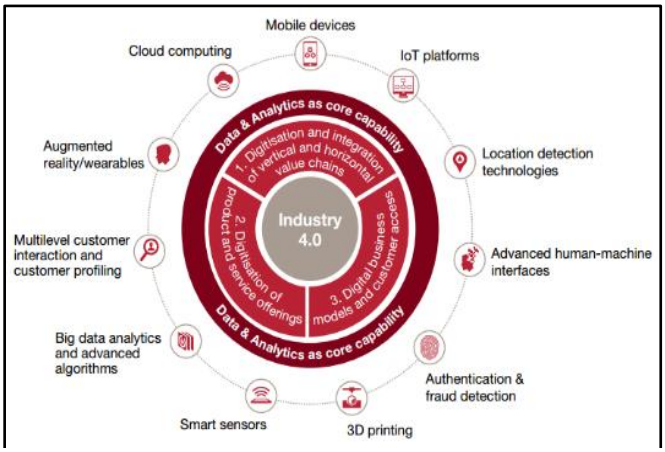

Figure 1.0: Industry 4.0 Framework (Taken from Global Industry 4.0 Survey, 2016)

Framework for Industry 4.0 shows that key digital technologies play a crucial role to ensure success of digitization of various area including vertical and horizontal value chain, product and service offering and business models and customer needs. Technologies such as Internet of Things (IoT), mobile devices, cloud computing and others can help an organization moves towards achieving Industry 4.0. Following are few reasons why organizations should be tempted to move towards Industry 4.0:

- Significant cost reductions
- Positive revenue opportunities
- Increased efficiency especially in managing customers

Based on study reported by [5], companies that do not strategically invest towards Industry 4.0 will lose competitive advantage. Some of the constraint in implementing Industry 4.0 includes lack of digital skills and transformation culture. The following diagram shows the blueprint for digital success:

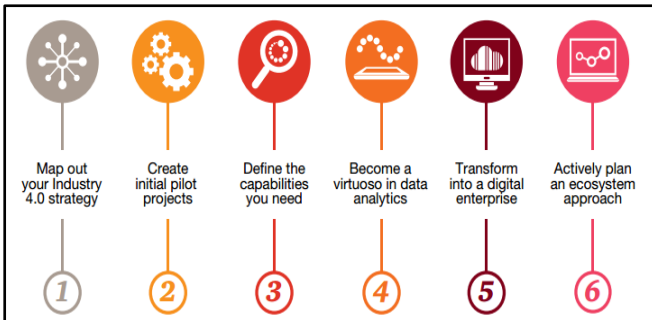

Figure 2.0: Blueprint for digital success (Taken from Global Industry 4.0 Survey, 2016)

In order to assist companies in shifting their paradigm towards Industry 4.0, this program have been created. It focuses on utilizing latest technologies such as cloud computing, IoT and mobile devices as well as data analytics and digital trust that works as pillar for Industry 4.0. This program focuses on producing expert especially in data analytics as shown in figure 2.0. Students graduated from this program will become the backbone for Industry 4.0 in years to come.

4.2. Government effort (Academic)

Malaysian Qualification Agency (MQA) is an entity which resulted from the merging of National Accreditation Board (LAN) and Quality Assurance Division, Ministry of Higher Education (QAD). MQA establishment dissolve LAN and all its personnel were absorbed into MQA [14].

MQA function mainly to implement the Malaysian Qualifications Framework (MQF) as a basis for quality assurance of higher education and as the reference point for the criteria and standards for national qualifications. Other functions include;

- To develop standards and credits and all other relevant instruments as national references for the conferment of awards with the cooperation of stakeholders;
- To quality assure higher education institutions and programs;
- To accredit courses that fulfil the set criteria and standards;
- To facilitate the recognition and articulation of qualifications; and
- To maintain the Malaysian Qualifications Register (MQR)

The contributions of MQA can be summarize as the following figures;

Figure 3.0: MQA contributions to the education quality assurance in Malaysia (Taken from MQA website)

5. CONCLUSION

We have shared our experience in developing new hybrid undergraduate program that refers to ISCIP CBK. Parallel effort from government helps us a lot in this program development. The accreditation process for this program is handled by Malaysian Qualification Agency (MQA), and takes around a year to finish the process. In final stage of accreditation process, MQA personnel visits the faculty and perform final assessment before the program can be run. The assessment is based on Malaysian Qualification Framework (MQF). The result of the assessment shows the program can be run with minor changes on core subject, as we put the majors on computer science domain. This proves that MQF standard that developed by MQA is at par with international level standard.

In the next curriculum review, the program will be reviewed based on student's acceptance for the program body of knowledge, marketability of program based on industrial needs, and student's achievement on every course offered. Curriculum review for this program will be done annually

6. ACKNOWLEDGMENTS

Our thanks to all who have involved with this project, researchers from Faculty of Communication, Visual Art and Computing, UNISEL. Special thanks for National Defence University of Malaysia (UPNM) for the registration fee that has been provided for this article and team member, faculty management, top management, and government, MQA and Ministry of Higher Education (KPT) for giving us opportunity in developing and running this program.

7. REFERENCES

[1] Brundiers, K., Wiek, A., & Redman, C. L. (2010). Real-world learning opportunities in sustainability : from classroom into the real world. https://doi.org/10.1108/14676371011077540

[2] Bullough, R. V, Young, J., Birrell, J. R., Clark, D. C., Egan, M. W., Erickson, L., … Brunetti, J. (2003). Teaching with a peer : a comparison of two models of student teaching, *19*, 57–73.

[3] Cohen, F. (1999). Managing Network Security : Security Education in the Information Age, 7–10.

[4] Fairuz, M., Othman, I., Bahaman, N., Muslim, Z., & Abdollah, F. (2008). New Curriculum Approach in Teaching Network Security Subjects for ICT Courses in, 637–641.

[5] Industry 4.0: Building the digital enterprise. (2016). Retrieved October, 2017, from https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

[6] Krempl, S. (2005). Universities need lessons in IT.

[7] Lin, C., & Chen, Y. (2005). Teacher-oriented adaptive Web-based environment for supporting practical teaching models : a case study of "' school for all ,'" *44*, 155–172. https://doi.org/10.1016/j.compedu.2003.11.003

[8] Lundin, R. W. (2008). Teaching with Wikis : Toward a Networked Pedagogy, *25*, 432–448. https://doi.org/10.1016/j.compcom.2008.06.001

[9] Mdec.my. (2017). *Malaysia Digital Economy Corporation | MDEC*. [online] Available at:

https://www.mdec.my/?gclid=EAIaIQobChMI3dDar-Hy1wIVU4GzCh2FJQZyEAAYASAAEgKVZvD_BwE

[10] www2.mqa.gov.my. (2017). *:: Malaysian Qualifications Register ::*. [online] Available at: http://www2.mqa.gov.my/mqr/ [Accessed 5 Dec. 2017].

[11] Rutledge, S., & Hoffman, J. (1986). A Survey of Issues in Computer Network Security, *5*, 296–308.

[12] Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses : A hands-on approach, *26*, 290–299. https://doi.org/10.1016/j.cose.2006.11.005

[13] Theoharidou, M., Xidara, D., & Gritzalis, D. (2008). A CBK for Information Security and Critical Information and Communication Infrastructure Protection, *1*(C), 81–96. https://doi.org/10.1016/j.ijcip.2008.08.007

[14] www2.mqa.gov.my. (2017). *:: Malaysian Qualifications Register* [online] Available at: http://www2.mqa.gov.my/mqr/ [Accessed 5 Dec. 2017].