JOURNAL OF QURANIC SCIENCES AND RESEARCH
e-ISSN: 2773-5532

JQSR

Vol. 4 No. 2 (2023) 28-33
https://publisher.uthm.edu.my/ojs/index.php/jqsr

Development of Cybersecurity Competency and Professional Talent for Cyber Ummah

Rabiah Ahmad[1], Noraini Abdul Rahman[2]*, Zefrieda Zahrullayali[2], Siti Rahayu Selamat[2], Robiah Yusof[3]

[1] *Faculty of Engineering Technology*
Universiti Tun Hussein Onn Malaysia, KM1 Jalan Panchor, Panchor, Johor, MALAYSIA
[2] *Cybersecurity Malaysia,*
Level 7 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, MALAYSIA
[3] *Department of Computer System and Communication*
Universiti Teknikal Malaysia Melaka,
Jalan Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, MALAYSIA

*Corresponding Author: noraini@cybersecurity.my
DOI: https://doi.org/10.30880/jqsr.2023.04.02.004

Article Info

Received: 3 October 2023
Accepted: 8 November 2023
Available online: 31 December 2023

Keywords

Cybersecurity, competency, training, professional talent

Abstract

The world is facing threats in digital transformation. Cyber threats have become trending as reported by my countries. Developed countries like Britain, America, Europe and Japan already prepared countermeasures for various incidents on computer threats since Internet was introduced. They formulated and developed a successful model to produce computer security experts and highly skilled talent at various level diploma, bachelor and professional. University and College established academic program in computer and internet security at bachelor and postgraduate level. Industries at those countries introduced certification program in computer and internet security. Throughout our studies, limited initiatives related to talent development in combating computer security issues including cyber threats. Previous studies showed development of cybersecurity talent in Muslim countries is critical. Malaysia needs 20000 cybersecurity professionals in 2025 and only achieved 2500 at present. This study presents our experience in developing cybersecurity competencies and professional talent for OIC-Country. We collaborated virtually with OIC-CERT (OIC Centre for Emergency and Response Team) in knowledge exchange, proposed appropriate competency model and participate in professional certification development. We presented the eight years active involvement with OIC-CERT activities. All initiatives established by OIC-CERT have produced outstanding impact to OIC Countries. One of the impactful initiatives known Global Ace, is getting serious attention by many Muslim countries. We also get the benefit of other programs such as training for risks analysis, incident management and policy development. Our students be able to participate with virtual lecture on combating insider threats, cyber threats drill, and security audit. OIC-CERT also introduces the first Industry Journal in Cybersecurity known as OIC-CERT Journal of Cybersecurity.

© 2023 UTHM Publisher. All rights reserved.
This is an open access article under the CC BY-NC-SA 4.0 license.

J. of Quranic Sciences and Research Vol. 4 No. 2 (2023) p. 28-33

1. Introduction

Internet and computer technology has gained much attention since it was introduced in 1995. Netscape navigator started in the same year and became useful tool for information searching. Due to the tremendous growth of Internet Technology and increase in usage we are exposure to cyber danger. Cyber security is one of the topics that gain a great deal of attention since it could create significant threats in our life. In 2013 to 2017, an average of 10,000 incidents related to cyber security was reported to Cyber Security Malaysia every year (Selamat *et al*., 2018). This creates a sense of urgency to address this problem in a holistic way.

Various initiatives executed by organizations with authority which covers people, process, and technology. Cybersecurity awareness program become a priority to many departments around the world. As reported by cybersecurity agencies, since 2013 the government has put a lot of effort to promote awareness and education in cybersecurity. Cybersecurity program at Bachelor and Diploma level introduced by 29any Universities in country like Britain and United States of America. Siponen (2008) highlighted effective awareness program in cyber security. The program must be able to create awareness to user. It should be able to provide steps need to be taken in protecting information and device while connecting to the Internet and computer Technology.

Zooming to academic program at the University, previous research reported that developed countries like Japan, Europe, Britain, Canada and United States offered Bachelor's Degree in Computer Security, Network Security and Internet Security in various name. In addition to that, those universities provide cybersecurity program at postgraduate level. We also noticed that universities and industries are hand in hand to develop effective academic program as mechanism to increase cyber security talent in their university.

The rapid growth of talent development program at developed countries increase convince many parties to perform business and strategic collaborations in digital platform. Unlike developing countries, talent development program in cyber security is considered limited. Our study explores role of Organization of Islamic Cooperation in promoting cyber security talent including awareness, training, and collaborative engagement to protect cyber world. The members of OIC agreed to establish Center of Emergency Response Team (CERT) in 2014 as platform to share best practice in securing digital system and its connections to each other. Authors actively participated in the organization's activity and compiled all initiatives related to human capital development to present here.

This article is designed in four sections. The first section brings insight information on cyber and computer security. Section 2 provides studies and initiatives by OIC as mechanism to improve skill and knowledge to the members. The following section (section 3) presents results in brief and the last section concludes the overall study.

2. Cybersecurity Threats and Countermeasures

Computing technology has kept evolving since it was introduced by Sir Alan Turing in 1936. Due to the demand in utilization of computers and its related technology, digitalization was introduced. Computer communicated via protocol system and connected in wired or wireless mode. Software is needed to make sure the computer can operate as intended. In a single operation a computer needs data, hardware, and software to operate and it is presented in a system. Computer technology produces information and in late 1980, information technology become sub-cluster of computers and it creates information system. An effective system must be able to perform according to purpose, produce the right information for the right person at the right time. The tremendous development in digital technology, however, creates an opportunity for unnecessary failure caused by human error, system misfunction, attacks and disaster (Al-Mhiqani, 2022). Thus, computer systems become vulnerable, and information can easily expose to unauthorize party.

Data security, computer security and information security become necessary in late 1990. When the Internet was introduced in 1996, network and Internet security get serious attention by computer experts and practitioners. In early 2000 computer security is defined by (Al-Mhiqani, 2022; Apau *et al*., 2019; Anawar *et al*., 2019) as a system that able to provide confidentiality, integrity, and availability (CIA) to data, information, and technology. Threats to information technology are getting serious attention by experts and practitioners in many countries. It can be seen by International Standard Organization ISO introduce ISO 27100 as guideline to industry and organization to secure their information and overall computer system. Each country established an authorized body to govern implementation of information security via enforcement of security policy at national level. Malaysia via Cybersecurity Malaysia and National Cybersecurity Agency are two authorized bodies responsible in establishing, executing, and governing information security.

Due to fast development in Internet technology and increase usage, cases like cyber-attack and information theft dramatically growth. Most developed countries like US, Britain, Canada are taking serious action in improving cyber security technology and talent development related to computer and information security. Universities at those countries established an academic program in cyber security at Bachelor's Degree and Postgraduates Studies. Finance allocations are giving more to research in that area. In addition to that industries start putting effort to promote training and certification program to practitioners and fresh graduate. Topics in cyber security include information security policy, penetration testing, cryptography, access control and very

recent blockchain. It is important to learn or have awareness on cyber-attack and strategy to countermeasures. Risks analysis is important and a must do activity in an organization. In short, all important aspects in computer, information and cyber security are demand area and it needs to be part of content in either skill training or academic knowledge.

2.1 Trends in Cybersecurity Incidents

As stated in (Al-Mhiqani *et al*., 2018) from 2013 to 2017 around 10,000 cyber security incidents reported at Cybersecurity Malaysia. The same researchers reviewed cyber security incidents at oil & gas industries located in Middle East from 2010 to 2017. The research reported tremendous changes in Internet Technology, the IOT exposed to various type of threats, and it affects industries operation which apply cyber physical system. Malware analysis become necessary to every country. National Cyber Security Agency is responsible to conduct analysis of malware in predicting future trend of attacks. The very recent known as ransomware. This target is to destroy a victim's data or disabled the access to those data until the hacker's request is granted. Another challenges that need major attention is cyber-attack on critical infrastructure. This type of attack occurs in many countries and most happen at the oil and gas-based company which located at the Middle East region.

2.2 The OIC-CERT

Organization Islamic Cooperation is an intergovernmental organization consisting of 57 countries and 48 were considering as Muslim-majority as defined from the website (https://www.oic-oci.org/). The headquarters based in Jeddah, Saudi Arabia. The organization concerned issues such as peace and security, Islamic finances, science and technology, climate change, and others emerging issues that important the growth of Muslim world. Under the umbrella of Science and Technology, the IT department at OIC headquarters established Centre for Emergency Response Team to alert all countries member on security threats in computer technology and digital world.

The OIC-CERT established in 2006 with the vision is to be a leading cybersecurity platform to make the world a safe cyber place. The founding members are Malaysia, Saudi Arabia, Pakistan, Tunisia and UAE. With the mission to be a platform for developing cyber security capabilities and mitigate cyber threats by leveraging global collaboration. To date, OIC-CERT initiated various activities related to cyber security capabilities development and risks mitigation. One of the impactful activities is called cyber drill. This program provides insightful information to deal with cyber-attack and critical cyber incident (https://www.oic-cert.org/en/).

In 2015 member of OIC-CERT called for workshop and proposed five pillars in facing dramatic increased of cyber incidents. The pillars are diplomatic issue on digitalization, cyber security talent, cyber security technology, industry and academic engagement to OIC-CERT and cyber inter-cop as part of mitigation framework.

2.3 Membership and Roles

OIC-CERT offer call for membership. Full membership offered to the country. Currently 27 countries majority Muslim registered as full membership. There are other types of membership known as general member, professional member, commercial and fellow. The benefits of the memberships can be seen in many ways which are participating in annual conferences and meetings, participating in cyber drill activity, eligible to lead working groups and many others as presented on the website. Each member in OIC-CERT has roles. It depends on the objective of becoming a member. Overall, it is important to unite and aim for making cyberspace safe for ummah. In this article, we present our journey as part of members of the organization and supported them formulate a program to improve knowledge and skill among cyber security practitioners. We also shared our activities as professional members and general member and benefits gained by our university's students also individual.

3. Related Work

Study on information security awareness started by Siponen (2000). Siponen explored the level of awareness among users regarding information security incidents. It covers user behavioral when facing with security incidents. Late 2010 information security research focuses on education. This includes formulating awareness models for educators in dealing with information security issues. Selamat *et al.* (2018) shared their experience in helping OIC-CERT to establish cybersecurity professional certification known as the Global ACE scheme. The scheme is the first professional certification for cybersecurity practitioners and fresh graduates. Today, the demand in strengthening cybersecurity skills keeps increasing due to the complexity in combating digital attacks. Demand to be certified in cyber security is high due to the increase in job opportunities. Thus, authors and her team explored potential initiatives to develop talent in cyber security for Muslim world.

4. Methods

We considered our study used action research as method for data collection and analysis. The study involves real action, evaluation and reflection. As we mentioned, our participation in the activities organized by OIC-CERT gave

J. of Quranic Sciences and Research Vol. 4 No. 2 (2023) p. 28-33

us good outcome in term of networking, translating our knowledge into real industry needs and improve out publication value. We observed and critically discussed those activities to provide feedback in this study. Our translational model can be seen in many forms and one of them is the Professional Examination for Cybersecurity certification.

5. The Initiatives

Since 2015, we actively participated in OIC-CERT activities. This section presents activities participated by authors organized by OIC-CERT. All activities comprise various types of initiatives covering people, process and technology. It is important to highlight that the activities that we involved were not limited to attending the annual conference. Some of the activity has a continuation by doing small workshops. Example, the development of Global ACE scheme. Table 1 provides the list and summary of initiatives.

Table 1 *Initiatives by OIC-CERT members*

Index	Year	Activity	Impact
1	2015	Cyber Violent Extremism	CoE – based in Jeddah
2	2016	Annual Conference	Global ACE Scheme
3	2017	Industry Journal OIC-CERT Journal of Cyber Security	Industry – Academia Writing
4	2018	Industry-Academia Mini Conference	Articles published OIC-CERT Journal of Cybersecurity
5	2017 – 2023	Professional Examination Committee – Global ACE Scheme	Global Ace Scheme Professional Examination Blueprint and Guideline
6	2018, 2019, 2023	Information Security Training	Student exposure to industry training

5.1 Cyber Violent Extremism 2015 in Jeddah

Our first involvement was OIC-CERT Special Workshop in Countering Violent Extremism. During the workshop all participants are responsible to conduct a discussion on the development of center combating cyber violent extremism. Interestingly the proposed framework four pillars – the first pillar emphasis procedure, the second pillar looking at procedure, the third pillar focus people and the last pillar explain technology to mitigate risks of cyber violent extremism. We were invited to be panel of expert in preparing draft of proposal and it was then presented to Chairman OIC-CERT and OIC for implementation. The proposed framework derived from Yunos *et al*. (2015). Yunos and Ahmad (2014) developed cyber terrorism framework as method to protect critical infrastructure against cyber terrorism.

5.2 Annual Conference 2016 – Advanced Persistent Threats Forum – 2016 Jeddah

This program was executed in November 2016. One of the agenda was discussing the issue *Advanced Persistent Threats.* It was mentioned in (Apau *et al.*, 2019) one of the most serious threats is APT. The mode of attack derived from various methods such as social engineering, spying, intrusion, and malware attack. In the forum speakers addressed strategies to protect critical systems from being exposed to APT. All countries members shared initiatives and best practices in protecting their internal system against unnecessary intrusion. It is important to note here that the session provided sharing best practices from Japan, France and Malaysia. Throughout this session we are able to get new knowledge in combating sophisticated threats. In fact, we were selected as part of the team for Malware analysis. One of the interesting initiatives was selling an idea of professional cyber security certification known as the Global Ace Scheme.

5.3 Annual Conference 2017 – The International Requirement in Mitigating Risks of Cyber Attack – 2017 Azerbaijan

One of the vice chancellors from Malaysia was called to be a keynote speaker at the Annual Conference 2017 OIC-CERT. The main content in his lecture was the need for diplomatic relationships at international level to mitigate risks of cyber-attack. The focus during the conference was to formulate an effective model in developing international policy that able to act like a cyber cop. We found industries players that were interested in participating in the discussion about diplomatic arrangement in reducing intelligent threats on cyber system. During this conference we launched a survey on awareness of industries players in reducing risks caused by Insider Threats. From the selected interview session, we were able to engage with expert from Thales PLT France, his input gave us confident to pursue research on Insider Threats. Our success was won RM300K fund from Ministry of Higher Education for research title Insider Threats for Manufacturing System.

5.4 Annual Conference 2018 – The OIC-CERT Journal of Cybersecurity – Siraj Iran

At this conference we are able to promote the OIC-CERT Journal of Cybersecurity to university located in Iran. It is interesting to note here that we are able to gather undergraduate and postgraduate students to present their projects related to information security. There were various innovations in protecting their cyber system in Iran. The most outstanding discussion was about privacy using social media. We received various articles to published at the journal

5.5 Annual Conference 2019 – Training of Global Ace Certification Kuala Lumpur

During the annual conference OIC-CERT offered invited participants to join training offered by the Global Ace Scheme. We registered the ISMS Auditor scheme and were able to learn the process in becoming an information security auditor. On that session the organizer extended the invitation to our colleagues to join other modules such Penetration Testing and CISAM.

5.6 Online Cyber Drill – The Post Covid

In 2020 – 2023 the OIC-CERT secretariat launched online cyber drill training offered by countries members. The training is open for small group however they allow few students to join. In the training session, participants received real experience in combating cyber security incidents. Our selected students gained a lot of information and industry practices. This session is useful to the participants, particularly the students.

6. Impact and Output

All activities launched by the OIC-CERT have provided us with insightful knowledge, experience, and outcome. The impact from becoming a member can be seen in many views such as:

(i) Cyber Security Talent Development Program through the Global Ace Scheme
(ii) Received Industry Research Fund on Malware Analysis
(iii) Received International Research Fund to Support Cyber Stability experts based in Europe
(iv) Received National Research Fund to mitigate Insider Threats
(v) Becoming Committee Member for Professional Cybersecurity Examination
(vi) Produced Malware Report Analysis
(vii) Produced Guideline for Cyber Stability
(viii) Editorial Members OIC-CERT Journal of Cybersecurity

Our outstanding output can be seen from three aspects Talent, Publications and Product. We noticed that the Global Ace Scheme able to provide professional certification on Digital Forensics to students who graduated in network security bachelor program in several university in Malaysia. The Global Ace scheme received prestige award in 2022 and it shows that the professional certification scheme was not limited to developed country like USA and Britain but as Muslim country we are capable to develop expert in protecting our cyber space.

It is important to note here that there are more than 10 post graduate students that performed research related to projects which we received from all activities mentioned above. Most of them work at reputable industry companies and universities all over the world. Students who were certified with the Global Ace scheme are already working at cyber security as security analysts, penetration tester and security engineer.

7. Conclusions

This article presented our experience journey in making engagement with the OIC-CERT organization and how we benefitted from participating in the activities. We presented all activities and shared impact from the

networking that we established during all sessions from 2015 to 2023. Our focus is that to share with all readers way of talent development created by the OIC-CERT members and our strategy value add and make it real.

Acknowledgement

We would like to thank Universiti Tun Hussein Onn Malaysia, OIC-CERT, Cybersecurity Malaysia, Universiti Teknikal Malaysia Melaka, Ministry of Higher Education Malaysia for supporting us in giving support to development cyber security talent by a productive collaboration between industry, agency, and university.

References

Mikko Siponen. (2000). A Conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1):31-41.

Mohammed Nasser Al-Mhiqani, Rabiah Ahmad, Warusia Yassin, Aslinda Hassan. (2018). Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems. *International Journal of Advanced Computer Science and Applications*, 9(1).

Mohammed Nasser Al-Mhiqani, Rabiah Ahmad, Z. Zainal Abidin, Karrar Hameed Abdulkareem, Mazin Abed Mohammed, Deepak Gupta, and K. Shankar. (2022). A new intelligent multilayer framework for insider threat detection. *Computers & Electrical Engineering*, 97(2022):107597.

Mohd Nazer Apau, Muliati Sedek, Rabiah Ahmad. (2019). A Theoretical Review: Risk Mitigation Through Trusted Human Framework for Insider Threats. In *Proceedings of the 2019 International Conference on Cybersecurity* (ICoCSec).

OIC-CERT Journal of Cyber Security. https://www.oic-cert.org/en/.

Siti Rahayu Selamat, Robiah Yusoff and Lee Hwee Hsiung. (2018). *Development of Examination Framework for Cyber Security Professional Competency Certification*. https://www.oic-cert.org/en/journal/vol-3-issue-1/5.html

Syarulnaziah Anawar, Nurul Azma Zakaria, Mohd Zaki Masu'd, Zulkiflee Muslim, Norharyati Harum, Rabiah Ahmad. (2019). IoT Technological Development: Prospect and Implication for Cyberstability. *International Journal of Advanced Computer Science and Applications*, 10(2).

Zahri Yunos and Rabih Ahmad. (2014). Evaluating cyber terrorism components in Malaysia. In Proceedings of the *5th International Conference on Information and Communication Technology for The Muslim World* (ICT4M), Kuching, Malaysia, pp. 1-6.

Zahri Yunos, Rabiah Ahmad, Nor Amalina Mohd Sabri. (2015). A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia. *Information Security Journal: A Global Perspective*, 24(1-3):15-23.