OFFICIAL BULLETIN 5TH EDITION - KDN: PQ1780/J/187

MBOT
LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

TECHIES

05
OCT. 17 -
MAR. 18

COMBATING
CYBER THREATS

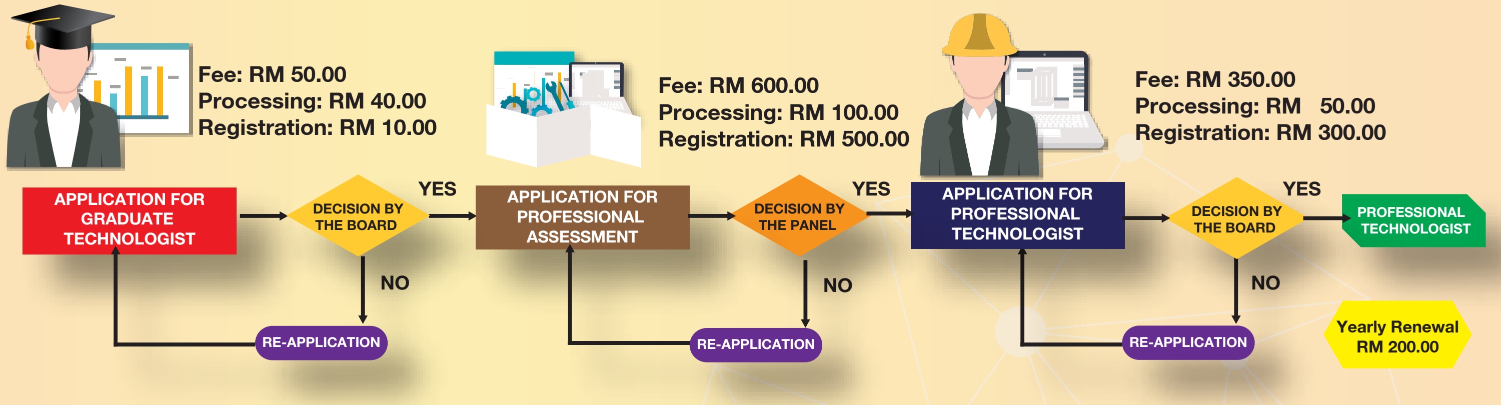
BUILDING CYBER
WARRIORS

AI : THE FUTURE OF CYBERSECURITY

ISSN 0124-1317
9 770124 131007

LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

FLOWCHART: APPLICATION FOR PROFESSIONAL TECHNOLOGISTS



Fee: RM 50.00
Processing: RM 40.00
Registration: RM 10.00

APPLICATION FOR GRADUATE TECHNOLOGIST → DECISION BY THE BOARD → YES / NO → RE-APPLICATION

Fee: RM 600.00
Processing: RM 100.00
Registration: RM 500.00

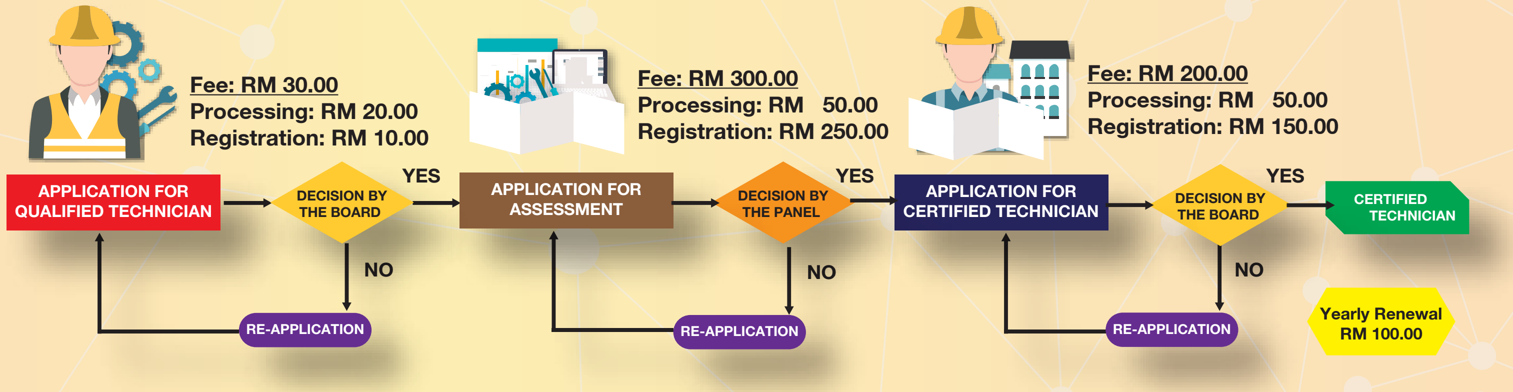
APPLICATION FOR PROFESSIONAL ASSESSMENT → DECISION BY THE PANEL → YES / NO → RE-APPLICATION

Fee: RM 350.00
Processing: RM 50.00
Registration: RM 300.00

APPLICATION FOR PROFESSIONAL TECHNOLOGIST → DECISION BY THE BOARD → YES → PROFESSIONAL TECHNOLOGIST / NO → RE-APPLICATION

Yearly Renewal
RM 200.00

FLOWCHART: APPLICATION FOR CERTIFIED TECHNICIAN



Fee: RM 30.00
Processing: RM 20.00
Registration: RM 10.00

APPLICATION FOR QUALIFIED TECHNICIAN → DECISION BY THE BOARD → YES / NO → RE-APPLICATION

Fee: RM 300.00
Processing: RM 50.00
Registration: RM 250.00

APPLICATION FOR ASSESSMENT → DECISION BY THE PANEL → YES / NO → RE-APPLICATION

Fee: RM 200.00
Processing: RM 50.00
Registration: RM 150.00

APPLICATION FOR CERTIFIED TECHNICIAN → DECISION BY THE BOARD → YES → CERTIFIED TECHNICIAN / NO → RE-APPLICATION

Yearly Renewal
RM 100.00

TECHNOLOGISTS AND TECHNICIAN ACT 2015

TECHNOLOGISTS AND TECHNICIANS (FEES) REGULATIONS 2017

LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

FINDINSIDE
TABLE OF CONTENT

ACKNOWLEDGEMENTS
APPRECIATION

EDITORIAL ADVISER
Datin Paduka Ts. Dr. Siti Hamisah Tapsir
(Head of Publication Committee & MBOT Board Member)

PUBLICATION COMMITTEES
Dr. Marlia Puteh (Lead Columnist)
Elena Mazlinda Mazlan (Coordinator)
Prof. Datin Dr. Zuraidah Binti Mohd. Zain (Senior Editor)
Assoc. Prof. Dr. Suraya Abdul Rashid (Editor)
Dr. Naimah Binti Md Khalil
Dr. Mohamad Asmidzam Ahamat
Assoc. Prof. Dr. Muhammad Fahmi Miskon
Assoc. Prof. Dr. Kushsairy Abdul Kadir

DESIGNER
Media Perintis Sdn Bhd

PUBLISHER
Malaysia Board of Technologists (MBOT)
TECHies is an official publication of MBOT. The bulletin is published and distributed to our members, government agencies, private sectors and the public at large.

PHOTO CREDITS
MBOT also wishes to extend its heartfelt appreciation to the following institutions and organisations for their contribution of photos used in this publication:
Mustafa Kamil Mokhtar, MOSTI
Universiti Malaysia Perlis (UniMAP)
Universiti Tun Hussein Onn Malaysia (UTHM)
Universiti Teknikal Malaysia Melaka (UTeM)
Universiti Malaysia Pahang (UMP)
Universiti Kuala Lumpur (UniKL)

SECRETARIAT
Mohd Nazrol Marzuke (Registrar)

ADVISORY PANEL
Ministry of Science, Technology and Innovation Level 7, Block C5, Complex C
Pusat Pentadbiran Kerajaan Persekutuan
62662 PUTRAJAYA

MBOT would like to thank all those who have contributed in one way or another towards the successful publication of this bulletin.

LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

PRESIDENT'S NOTE

Tan Sri Dato' Academician (Dr)
Ts. Hj. Ahmad Zaidee bin Laidin FASc

We live in a world where technologies are renewed at an accelerating pace. To respond to the ever-changing requirements of the nation's social, cultural and economic goals, the extent of our planning has to be elevated accordingly.

As far as TVET is concerned, in line with the above aspiration, the best place to start is to consolidate the way it is managed. With seven ministries (Human Resources Ministry, Ministry of Higher Education, Ministry of Education, Ministry of Youth & Sports, Ministry of Rural & Regional Development, Ministry of Works and Ministry of Agriculture & Agro-based Industry) administering TVET training, the need for proper coordination to cope with overlaps and possible disparities become a big concern. That is why the rebranding of TVET training providers, known as TVET Malaysia, is very timely indeed.

Apart from the rebranding exercise, the Government has announced a monumental allocation of RM4.9 billion, as indicated in Budget 2018, for the implementation of TVET Malaysia Master Plan. To add, 100 TVET Excellent Students Scholarships worth RM4.5m is also make known. Apart from monetary provision, the creation of the National Rail Centre of Excellence is a big boost for TVET to flourish in the country. The Centre offers a good platform for skilled workers to thrive and contribute accordingly. No doubt, the Government is doing all it can to ensure the success of TVET Malaysia, in line with the goal to empower people at all levels.

MBOT is continuously proactive in helping to fulfil this purpose. We are grateful for both monetary and non-monetary allotment that will be disbursed, and look forward to play a big role in realising the noble ambition of achieving the 2050 National Transformation (TN50) agenda.

ABOUT

LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

- The Parliament of Malaysia has enacted the Technologists and Technicians Act 2015 (Act 768), an act to provide for the establishment of Malaysia Board of Technologists (MBOT), in line with other professional bodies in Malaysia.
- MBOT is responsible for the registration of graduate technologists and qualified technicians as well as to recognise professional technologists and certified technicians.
- MBOT promotes education and professional training in related technology and technical fields.
- MBOT recognises technological careers and empowering technical and vocational education and training (TVET).
- MBOT will strive to be a signatory to international accords in the field of technology and technical to ensure the technologists and technicians produced in the country meet the international standards and ability to compete globally.

01 VISION

To be a world class professional body for technologists and technicians

02 MISSION

To elevate the standing, visibility and recognition of technologists and technicians

03 OBJECTIVES

- To elevate the standing and recognition of technologists and technicians
- To increase the pool of skilled workforce required to attain a high income economy
- To protect public safety and health

WHO SHOULD REGISTER ?

PROFESSIONAL TECHNOLOGIST

Graduate Technologist with practical experience as stipulated by the Board

GRADUATE TECHNOLOGIST

Holds a bachelor's degree recognised by the Board

CERTIFIED TECHNICIAN

Qualified Technician with practical experience as stipulated by the Board

QUALIFIED TECHNICIAN

Holds a certified qualification recognised by the Board

CERTIFYING CYBERSECURITY PROFESSIONALS

– consideration factors and proposed solution

by : Ruhama Bin Mohammed Zain, CyberSecurity Malaysia

BACKGROUND

The issue of quality of cybersecurity professionals is complex as well as controversial. IT managers, CEOs and government officials agree that the cybersecurity profession is less regulated than the engineering profession, for example. There is a very low barrier of entry into the cybersecurity profession. A person with a non-IT or non-technical academic background might claim to be a cybersecurity expert armed with only self-taught knowledge and skills together with one or two cybersecurity certifications from the industry.

It is clear that if the country is to have assurance that its cybersecurity professionals are really capable, trustworthy and reliable enough to deliver quality work to protect the nation, there must be some way of certifying and accrediting them.

IMPORTANT CONSIDERATION FACTORS

There are a few important factors that any certification scheme must consider in order to have any assurance value. Firstly, it must emphasise the requirement of assessing practical or hands-on skills of the candidate. For illustration purposes, let us take the example of a penetration tester, who is someone tasked to conduct tests to determine if there is any security weakness that might allow unauthorised access into the network or system. Without sufficient skills to do the job, there is no assurance that a thorough and effective penetration test is carried out. It may also be the case that security vulnerability is not found during the test, when in actual fact, it does exist. Hence, there might be a false sense of security on the part of the organisation commissioning the work, which might result in not putting in the necessary security controls that are actually required.

Secondly, there must be an element of background or character check on the penetration tester before she/he can be trusted to conduct tests on mission-critical network or online applications. Thirdly, as technology evolves continuously, the penetration tester must demonstrate that she/he is constantly keeping up-to-date with the current attack tools and techniques as well as countermeasures. This assures that her/his knowledge and skills do not become outdated over time.

THE GLOBAL ACE SCHEME

This is where the Global Accredited Cybersecurity Education Scheme (Global ACE) comes into the picture. The scheme was initiated by CyberSecurity Malaysia in response to the pressing need to have more cybersecurity professionals who are both qualified and dependable to protect and defend the nation's critical national information infrastructures (CNII). The scheme is a holistic framework designed to address all related cybersecurity certification matters. It comprises various layers and components that relate to each other to support the factors mentioned earlier.

One of the main goals of the scheme is to provide a way to effectively assess candidates before they are recognised as cybersecurity professionals. The quality of the assessment method is key. Assessments combine both knowledge and practical tests where applicable. Another goal of the scheme is to assure employers that certified professionals are trustworthy. This is achieved by requiring that scheme-certified members adhere to a code of conduct. They must also provide a referee to vouch for their claimed professional experience. To add, certified members need to accumulate a certain number of Continuing Professional Development (CPD) points each year as evidence of their continual self-development and upskilling effort.

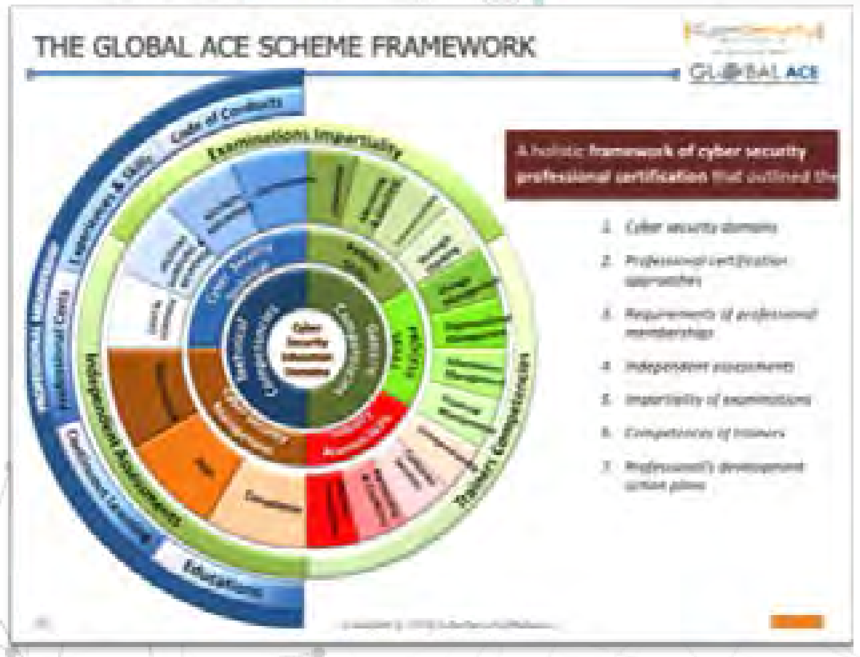

THE GLOBAL ACE SCHEME FRAMEWORK
GLOBAL ACE
Code of Conducts
Experience & Skills
Examinations Impartiality
Professional Certs
Independent Assessments
Trainers Competencies
Education
A holistic framework of cyber security professional certification that outlined the
1. Cyber security domains
2. Professional certification approaches
3. Requirements of professional membership
4. Independent assessments
5. Impartiality of examinations
6. Competencies of trainers
7. Professional's development action plans

Figure 1: The Global ACE Scheme framework

KNOWLEDGE, SKILLS AND ATTITUDES (KSA)

At the heart of the scheme is a clear definition of the required Knowledge, Skills and Attitudes (KSA) for identified job roles within the cybersecurity industry. Knowledge elements refer to the required theoretical knowledge, whereas Skills elements describe what the practical skills are. Attitudes refer to the values and ethics required. At present, there are more than ten KSAs already defined under the scheme. The KSAs have been jointly developed by working groups comprising representatives from the government, academia and the industry. This collaborative development effort ensures that the KSAs are relevant, complete and current. The KSAs play a critical role and are used as a reference to develop cybersecurity training and assessment questions. Future development plans include using the KSA as a guide to develop documents that become a common body of knowledge for major technical domains of the cybersecurity profession. More KSAs will be developed in the future to cater for additional cybersecurity domains and technologies.

WAY FORWARD

The Malaysia Board of Technologists (MBOT) has decided to appoint CyberSecurity Malaysia as a member of its technology expert panel for cybersecurity. The Global ACE Scheme initiative by CyberSecurity Malaysia can be leveraged by MBOT as a means to assess cybersecurity professionals before they can be recognised as technologists by the Board. The scheme's CPD system can also be used to continuously assess the technologists as part of their yearly renewal requirement. In conclusion, MBOT, CyberSecurity Malaysia and the whole country will benefit from the synergy between the Global ACE Scheme and the MBOT scheme by having a pool of certified cybersecurity technologists ready to protect and defend the nation against cyber threats and attacks.

ISSUES AND RESEARCH INITIATIVES ON CYBER SECURITY IN MALAYSIA (ABRIDGED VERSION)

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. This creates a sense of urgency to address this problem in a holistic way. Some of the common cyber security issues are ransomware attacks, Internet of Things, security of critical infrastructure, insider threats and blockchain.

Ransomware attacks a victim's data or disabled the access to those data until the hacker's request is granted. Otherwise, attempts to recover the data through reverse ransomware encryption are a tricky and laborious task. It is believed that a highly accurate prediction based on a good classification strategy would lead to an efficient detection technique, subsequently stop any potential attacks. However, one of the main obstacles to effectively reduce the number of incidents is the lack of sufficient data on such attacks; more research is required.

Internet of Things enables interaction between physical objects equipped with communication system. Access control and privilege management are the keys to avoid intrusion and prevention of unauthorised control by hackers. Cross-domain identification and trust are very essential when the system moves from one domain to another.

Critical infrastructure requires the establishment of communication networks which are independent and has a multilevel security system. Several cases on attacks to critical infrastructure proved that such events could disrupt airport operations, lead to flight delays and inadequate security measures at immigration. An attack to power plants or fuel supply network would lead to a catastrophic failure to the entire country.

Insider threat in cyber security usually has unbounded patterns, including irregular time gap between consecutive activities. If the role of employee in an organization is keep changing, the complexity of threats may be increased due to non-stationary data on attack activities. In a collusion attack, few small changes are made at a particular time which could be considered as a normal behaviour which would be easily penetrating a less sensitive detection system. On the other hand, a highly sensitive detection system would trigger numerous false alarms.

Blockchain is a list of records that are increasing in its quantity and linked through secured cryptography technique. Data integrity is one of the main challenges, particularly on data verification and protection from being altered or tempered.

In Malaysia, the Ministry of Higher Education, the Ministry of Science, Technology and Innovation, industry players and academia are working closely in combating cyberattacks. As reported in Global Security Index 2017, Malaysia is ranked as the third highly committed country in securing transaction over cyber platform. More than 80% of public universities had received research funds from the Ministry of Higher Education or the Ministry of Science, Technology and Innovation. At least four industry partners are involved in these research activities. Focus areas of these researches are closely related to contemporary cyber issues which are data security, network security, multimedia security, security management and digital forensics. In future, non-technical research topics on cyber related issues such as effects of cyberbullying, cyber ransom and cyber violent extremism may become new focus areas.

This article summarized the 'Research Trends in Cyber Security: Malaysia is aligned with Global Needs', authored by Hamisah Tapsir (Ministry of Higher Education Malaysia), Rabiah Ahmad, Sharin Sahib and Mohammed Nasser Al-Mhiqani (Universiti Teknikal Malaysia Melaka) and Zahri Yunos (CyberSecurity Malaysia)
Summary by: Dr Mohamad Asmidzam Ahamat

By :Dr. Naimah Md Khalil

Building Cyber Warriors at Cyber Range Academy,
Politeknik Mersing Johor

Information and Communications Technology (ICT) brings new opportunities in the development of the country, but at the same time it also opens up new vulnerabilities through increasingly sophisticated cyber attacks in different forms. Hence cyber security careers have become lucrative in the face of new and continual cyber security threats against businesses and government agencies. According to Forbes, the global cyber security market reached $75 billion for 2015 and is expected to hit $170 billion in 2020. However the country faces a severe shortage of cyber security talent and skilled expertise.

Thus polytechnics as TVET institutions that need to respond quickly to the demand of the market, began to offer programmes related to cyber security i.e. Diploma in Information Technology (Information Security) at three (3) polytechnics namely Politeknik Ungku Omar, Ipoh(PUO) in 2012, Politeknik Mersing Johor (PMJ) and Politeknik METrO Tasik Gelugor, Penang (PMTG) in 2015. The aim of the programme is to develop students into technically competent cyber security professionals who protect and strengthen the systems of organisations from rising cyber attacks.

PMJ has chosen to venture on the realism idea in the implementation of the said programme through the establishment of Cyber Range Academy (CRA) in 2017. In this academy, the cyber range lab is created to provide students with an authentic learning environment to help them understand visually the threat landscape. The three (3) year diploma programme will equip students with the knowledge and skills in offensive and defensive cyber security methods. They will gain skills in reacting to a myriad of cyber security and application traffic flows. Students will be put through operational scenarios that include malicious and non-malicious traffic in a safe, secure environment. For its success in establishing the Cyber Range Lab idea, it has been given an award by Cyber Security Malaysia (CSM) in the prestigious Malaysia Cyber Security Awards 2017. This award was given in recognition for being an Education Lab Innovator in the country and indeed it is a sweet victory since the lab is only a year old.

So what is special about the CRA? Based on the interview with Mr Tajul Azhar bin Mohd Tajul Ariffin, one of the key personnel responsible for the establishment of CRA as well as being the Head of Technical team tasked with the development of the cyber range module, it is the first educational institution in the country that implements cyber security training by actually bringing the real environment of Attack and Defence in the IT world into the lab. The training uses two teams, comprising of the defence team (blue) and the attacking team (red). By simulating real traffic and attacks using the latest technologies, CRA provides its students with an authentic learning experience. With a complete infrastructure now in place for IT security training, graduates have industry-valued skills and hands-on experience in specialties such as ethical hacking, intrusion detection and prevention, and cloud infrastructure. This methodology is currently used worldwide by security practitioners.

The key factor in CRA's success as an innovator lies in its collaboration with industry. For example Ofisgate, a Network & Telecommunication Solution company that focusses on Security Testing and Network Visibility and Keysight Technologies, the company that recently acquired Ixia. The industry is very much involved in the curriculum and its implementation. Competitions like Capture The Flag (CTF), a Cyber Drill exercise held in collaboration with Open Web Application Security Project (OWASP) and Security Day are held to expose students to the skills and competencies required in the cyber security world. (OWASP is an international non-profit organisation that focusses on software security). Through such consultation, CRA has been given the boost to be on the right track, therefore making sure that the training implemented is relevant and updated. There are also plans to certify students and staff with professional certifications such as Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP) or SANS cyber security training whereby the SANS Institute is the most trusted, and by far the largest, provider of training, certification, and research to cyber security professionals globally. 'Train The Trainer' courses for the lecturers are also being planned in order for them to be recognised as professional trainers. The cost of the certications is, however a major challenge.

There are also plans to collaborate further with CSM and Malaysian Communications and Multimedia Commission (MCMC). It is hoped that these collaborations will enable CRA to place more lecturers and students in these companies for their lecturer attachment and industrial attachment programmes respectively. In this way, more industry relevant practices and competencies can be injected into the programme. With Systematic Competency Alliance Sdn. Bhd. (SCOMA), the organisation appointed by Human Resources Development Fund (HRDF) to train graduates for employment, CRA @ PMJ has already planned to certify students with Wireshark Certified Network Analyst (WCNA) - a certification from Wireshark University, where Wireshark is one of the world's most popular network analyser. All these are in the pipeline for 2018, the second year of operation for CRA.

Besides running courses and activities for their own students and staff, CRA also trains workers from other agencies like MCMC, Setiausaha Kerajaan (SUK) Pahang as well as IT companies in its niche area. CRA has already captured the interests of educational institutions locally and abroad. Many have expressed the intention to visit and to collaborate. CRA has shown its commitment to produce the best. It benefits not only its students but also the industry and community. Even though it is relatively young for an institution, it has already shown its potential and who knows what its impact is going to be like in the future. Thus the tagline “Building the Next Cyber Warrior” is very apt to describe efforts at CRA towards this end.

AI : THE FUTURE OF CYBERSECURITY

by Assoc. Prof. Dr. Kushsairy Abdul Kadir

WHAT IS CYBER SECURITY?

Cybersecurity is a practice of ensuring ways to protect organisations and individuals from unauthorised exploitation of systems, networks and technologies. With it, we are able to defend and recover data from cyber attacks, hence making the cyber world a safer place.

CYBERSECURITY NOW

Cybersecurity is very much needed today due to the ever-increasing number of cyberattack incidences. Unfortunately, there is insufficient number of people in the cybersecurity workforce. Reports show that there is an estimated 3.5 million unfilled cybersecurity positions worldwide. As such, cybersecurity professionals are always overworked - making it hard for them to react to cyber threats satisfactorily and adequately.

SOLUTION

The rapid growth of artificial intelligence (AI) technology is good news to cybersecurity. There are now new ways to make the cyber world more secured. Machine Learning Algorithm, which is a branch of AI, enables computers to learn and adapt input data through experience, just as a human would, but faster and more efficient. This lessens the burden of cybersecurity personnel accordingly.

PITTFALLS OF AI

Although AI is very efficient, its capability is as good as the data being fed. This means AI will never be able to perceive the latest incoming threat with the same adeptness as a human being. Another weakness is, AI can lead to vulnerabilities, especially when it depends on interfaces within and across organizations, which creates opportunities for potential hackers to access the system. More attackers are now beginning to deploy AI, hence enabling it to make decisions that benefit the hackers.

FUTURE OF AI IN CYBERSECURITY

No matter how sophisticated, no single AI entity can act alone against the volley of human and artificial cyber threats that are coming in the future. But rather than being used only as a way to combat cybersecurity threats, AI has the huge potential to support organisations accomplish extraordinary achievements in the years ahead.

ASEAN DATA ANALYTICS EXCHANGE (ADAX)

ASEAN Data Analytics eXchange (ADAX) is an initiative by the Malaysia Digital Economy Corporation (MDEC) to enable businesses, governments, academia and professionals to rapidly adopt big data and data analytics as tools to empower decision-making and innovation. It was established at the end of 2016 following a successful public-private partnership between MDEC and Ansys Sdn Bhd to build and enhance Malaysia's big data ecosystem.

Launched in March 2017 as the world's first physical data exchange platform, ADAX is based in Bangsar South, Kuala Lumpur and seeks to be the definitive data analytics exchange hub for knowledge, information, resources and collaboration for the ASEAN region.

ADAX is mandated to build a critical mass of talent pool in big data analytics while developing the ecosystem and fostering collaboration amongst businesses, start-ups, academia and professionals so that data analytics becomes an integral part of business innovation and decision-making.

FUNCTIONS

ADAX focuses on four pillars to drive its initiatives:

Training & Education - For students & working professionals to develop cutting-edge, innovative data analytics and entrepreneurship skills in physical and virtual classrooms.
Best Practices - Providing knowledge to start-ups and organisations on data analytics.

Industry Development – Engaging with businesses and educational institutions to nurture and harness analytics through various initiatives.

Advocacy - Partnering with industry players to grow the big data and analytics ecosystem.

DATA STAR

Data Star is shaping future data professionals of ASEAN and will help Malaysia achieve 20,000 data professionals by 2020.

In an effort to accelerate the talent development of data professionals in Malaysia, ADAX and MDEC, in partnership with universities and leading industry partners, collaborate to introduce the Data Star programme. The programme is a 6-month finishing school for graduates, and includes two months of intensive data science enablement and mentorship with experienced data scientists, and placement at industry partners. It is expected to help Malaysia achieve 20,000 data professionals by 2020.

The learning paths have been curated in accordance to the Data Professional Skills Framework, a platform to support data and analytics knowledge development for data engineers, data analysts and data scientists.

Data Star's first intake was on 24th July 2017

Participants will be provided with the foundation skill sets for a range of knowledge areas. Courses include lectures, lab sessions, hands-on programming and interactive sessions. Each of the learning paths include mentorship, project presentation and soft skill development.

Holders of PhD, Masters and Bachelors in Mathematics/Statistics, Computer Science, Actuarial Science, Engineering, Economics or Science are invited to apply. Those with knowledge in programming has added advantage.

Participants of the Data Star programme are provided with relevant business exposure through mentorship programmes with industry-experienced data scientists. They are also granted an allowance during the training sessions and industry placement.

DELIVERY, TECHNOLOGY AND INDUSTRY PARTNERS

ADAX works closely with several local and internationally renowned delivery partners to ensure the highest quality of services. These include IBM, Microsoft, CADS, SAS, Open Data Institute, FusionEx, EY, Iverson, Quandatics, ABeam Consulting, ITrain, Databyte Academy and Dream Catcher. ADAX also counts Cloudera Inc, Sedania Innovator Berhad, Hewlett Packard Enterprise, TDATA Corporation (Malaysia) Sdn Bhd and Data Micron Systems Sdn Bhd as technology partners.

Currently, ADAX has several partners that offer industry placements for participants who take part in the programme.These industry partners include Kasatria, Fave, Celcom, Petronas, GHL, Leo Burnett, Hong Leong Bank, Tapway, Datalynx, FusionEx, MDEC, Astro, Maybank and Quandatics.

HOW TO APPLY?

Visit http://adax.asia/datastar/ for more information on the program as well as Data Star registration

Cyber Security: Combating Cyber Threats

By Prof Dr Azlinah Mohamed, & Fakariah Hani Mohd Ali

We are living in a world where technology has evolved to the extent that communication, sharing, and team-working have become very fluid and dynamic. Internet connection, embedded electronics and smart software allow data to be transmitted from various physical devices, vehicles, home appliances, etc. With increased availability and accessibility of information over the internet, the risk of cyber threats has also multiplied. Digital technology has not only transformed institutions positively, but it is also now used to disable the same institutions through computer hacking, information stealing, scamming, etc. Incidences of cyber crimes are escalating. For example, in 2016, cyber crime was reported to be the second highest crime among all economy crimes.

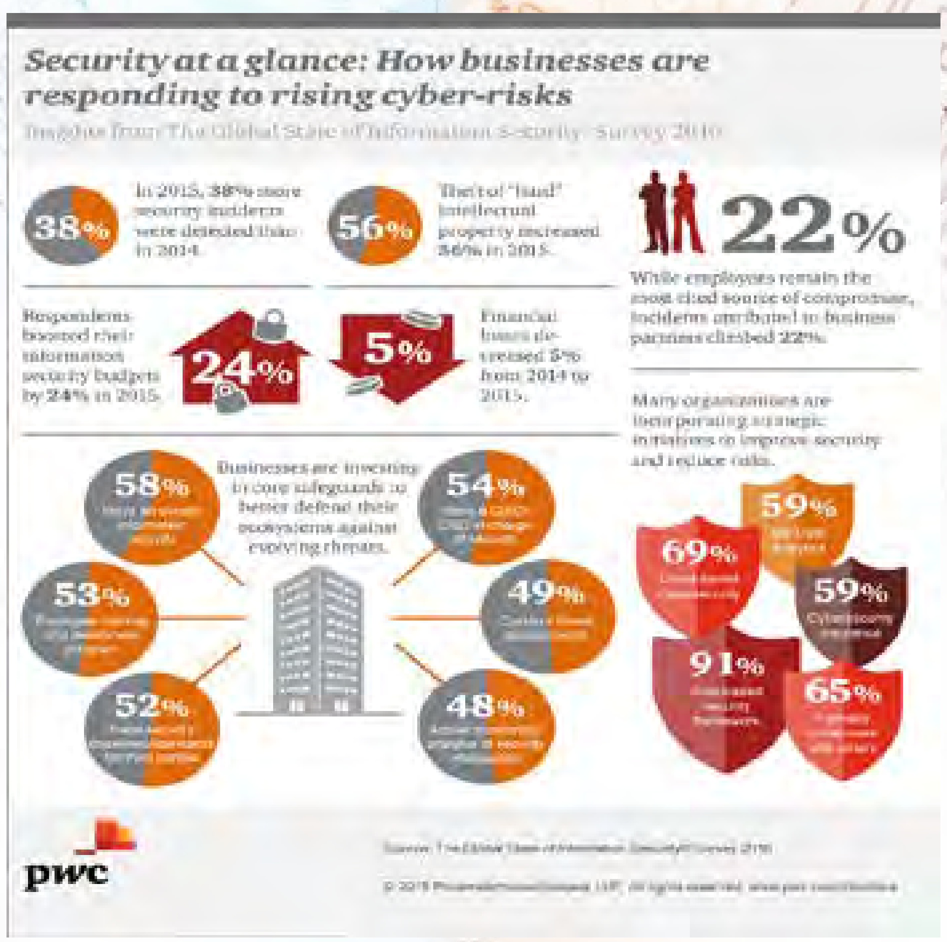


Figure 1: Security Information Survey Report
(Source: Global State of Global Information Security Survey 2016 by PWC- Pricewaterhouse Coopers International Limited)

From a survey conducted, only 37% of institutions have concrete action plans regarding cyber attacks. As they may cause many undesirable consequences, there is a dire need for institutions to be more assertive as far as cyber protection goes. Pricewaterhouse Coopers (PWC) reported in 2016 that companies need to strengthen their cyber security systems to combat the issue. In the 'Cybersecurity As Enabler For Malaysia Digital Economy: The Industry Report 2017' by MDEC, it is stated that two million cybersecurity professionals are needed by 2019. A report entitled "Burning Glass Job Market Intelligence: Cybersecurity Jobs 2015" highlights that the rate of cybersecurity job growth is three times higher than that of IT jobs (2010-2014). The ISACA study also shows that the majority of organisations find it difficult to hire qualified security staff members. In Malaysia, 9000 cybersecurity professionals are needed by 2020. Unfortunately, there are not many experts who can devise systems that can protect against cyber attacks and gather forensic evidences required to complete prosecution after an attack takes place. Indeed, experts in cyber security and digital forensics are in great demand.

In response to this amazing development, local universities have embarked on Bachelor's and Master's programmes to produce cybersecurity professionals, as shown below.

Table 1: Source MADICT 2018

University	Program	Number of Students
Uniten	B ComSc (Hons) Cyber Security	80
UUM	B CompSc (Hons), majoring Cybersecurity MSc Cybersecurity	In progress In progress
UiTM	MSc Cyber Security and Digital Forensics	In progress

UiAM	BCS and BIT specialization on Cryptography;
	Digital Forensic;
	Control and Audit;
		48
		36
		38

UKM	Master of Cyber Security – collaboration with CSM and Standard Chartered	-
UPNM	MSC Cyber Security in collaboration with University of Warwick UK	17

Solving this growing cyber problem requires skilled security professionals who have knowledge in advanced analytics for proactive threat hunting, comprehensive intelligence for real-time threat awareness, cyber policy, cyber law and integrated security architecture. As such, forensics, investigation protocol, data safety, network security, ethical hacking, and a whole lot more need to be incorporated into the programmes. A strong foundation on security should be drilled in so that new threats that emerge from new technology can be aptly taken care of.

It is in the interest of individuals and organisations to understand the nature of cyber crimes and to protect their systems and businesses from any unauthorised access to their platforms. Hence, organisations should invest well in order to shield their businesses. In this interconnected world that we live in, there is no choice but to go all out as far as cyber security is concerned.

Cybersecurity: Why it is Imperative

By Simon Cheong

In the wake of digital disruptions occurring at a massive scale, organisations today face serious challenges when it comes to cybersecurity. As part of embracing digitisation, the biggest change that must take place is the shift from security being seen as an IT task to protect assets, to a strategic business process that enables organisations to succeed faster. This shift in mindset is even more imperative in Southeast Asia and its fast growing economies like Malaysia. According to new research commissioned by Cisco, the digital economy in the Association of Southeast Asian Nations (ASEAN) has the potential to add $1 trillion to GDP over the next 10 years. The research report titled Cybersecurity in ASEAN: An Urgent Call to Action, was conducted by global management consulting firm A.T. Kearney, and emphasises that cybersecurity risk across the region will continue to escalate as countries get more digitally interconnected.

According to A.T. Kearney's research, cybersecurity is a very real danger in ASEAN, with its member countries emerging as launchpads for attacks. For example, Malaysia, Indonesia, and Vietnam are global hotspots for major blocked suspicious Web activities—up to 3.5 times the standard ratio, which indicates that these countries are being used to launch malware attacks. Cybersecurity is also a very real threat to the region for reasons such as:

1. Policy preparedness is still nascent, with a lack of institutional oversight and low levels of spending to fortify digital economies.
2. A nascent local cybersecurity industry faces shortages of homegrown capabilities and expertise.
3. Perception that cyber risk is an IT risk, hence resulting in the absence of a holistic approach to cyber resilience.
4. Multiple vendor relationships and product deployment, resulting in operational complexity and slowing times to detect and respond to attacks

The state of regional policy agenda

A.T. Kearney's research shows that cybersecurity governance and policies are undeveloped in the region, with Malaysia and Singapore being more advanced compared to the other countries in ASEAN. Cybersecurity policies also vary widely across the region, for instance:

1. **National cybersecurity strategies have been laid out by Malaysia, Singapore, Thailand, and the Philippines.**
2. **A few countries have also set up national agencies to consolidate and coordinate cybersecurity agendas. These include Malaysia (CyberSecurity Malaysia), Singapore (Cyber Security Agency of Singapore), and the Philippines (Department of Information and Communications Technology).**
3. **A few countries have also Malaysia, Singapore, Thailand, and Vietnam drafted cybersecurity bills in 2017, although limited progress has been made across the rest of ASEAN. Cybercrime laws have also been passed in Malaysia, Singapore, Thailand, the Philippines, and Brunei. Data protection or privacy laws have only been enacted by five countries.**

Cybersecurity needs to be an integral part of policy discussions, and Cisco is a trusted security partner to governments worldwide. Through our Security & Trust Organization (STO) we engage with world governments to help shape national cybersecurity policy agenda, collaborate to share threat intelligence, and share best practices

The importance of building capability

The shortage of skilled cybersecurity talent represents a worldwide challenge, with the US Information Systems Audit and Controls Association (ISACA) citing a global shortage of more than 2 million professionals by 2019. Malaysia currently has 6,000 cybersecurity professionals but it requires 10,000 by 2020.

Building capability across the region is critical. To help close the security skills gap, Cisco is preparing IT and cybersecurity professionals for these expanding job roles. Cisco has been doing this for 20 years through our Networking Academy. For 20 years, the academy has touched the lives of over 7.8 million students across 180 countries. In Asia Pacific, the Networking Academy has trained 1.26 million students since inception. In Malaysia, we have 100 academies offering courses and over 270 instructors. During the 2017 financial year, 10,000 students in the Asia Pacific Japan region took our cybersecurity courses. Globally we have trained 90,000 security students.

Detecting threats in markets prime for attack

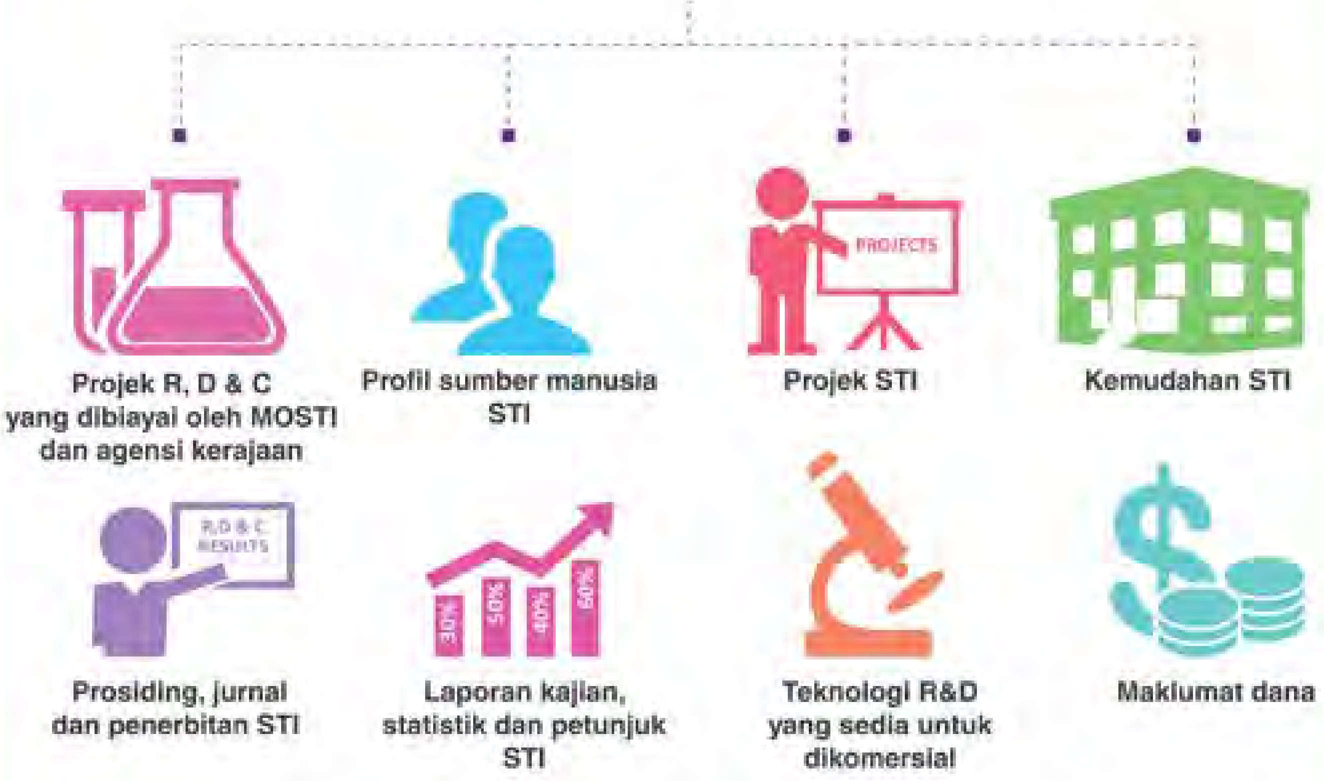
Security is foundational to digital transformation. And with a rise in the different types of attacks and in the level of sophistication, detecting threats quickly is increasingly important. Cisco measures the window of time between a compromise and the detection of a threat, calling it “time to detection”. We have dramatically reduced our time to detection rate from a median of 39-hours to about 4.6 hours. In comparison, the average is 184 days to detect a data breach in ASEAN.

With ASEAN companies facing US$750 billion exposure from cyber attacks – as stated in the A.T. Kearney research – it has never been more important for organisations in the region to invest in automated tools to help their security teams stay on top of alerts, gain visibility into their dynamic networks, as well as detect and respond swiftly to threats. Additionally, ASEAN’s response to the cybersecurity challenge needs to be comprehensive and forward-looking, with more urgency placed on a unified, regional policy agenda and building the next wave of cybersecurity capability.

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI

MASTIC

Platform untuk pengurusan dan pengetahuan maklumat STI. Berfungsi sebagai capaian tunggal kepada bidang pengetahuan dari pelbagai sumber.



Projek R, D & C yang dibiayai oleh MOSTI dan agensi kerajaan

Profil sumber manusia STI

Projek STI

Kemudahan STI

Prosiding, jurnal dan penerbitan STI

Laporan kajian, statistik dan petunjuk STI

Teknologi R&D yang sedia untuk dikomersial

Maklumat dana

PUSAT MAKLUMAT SAINS DAN TEKNOLOGI MALAYSIA (MASTIC)

mastic.mosti.gov.my

FIELDS OF TECHNOLOGY

LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

21 Fields of Technology

(EE) Electrical & Electronics Tech

(IT) Information & Computing Tech

(CM) Chemical Technology

(TB) Telecommunication & Broadcasting Tech

(BC) Building & Construction Tech

(BT) Biotechnology

(NR) Nuclear & Radiological Tech

(GT) Green Technology

(ME) Manufacturing & Industrial Tech

(AF) Agro -based Technology

(TL) Transportation & Logistics Tech

(MT) Material Science Technology

(MR) Marine Science Technology

(AM) Art Design & Creative Multimedia Tech

(RG) Resource Based, Survey & Geomatics Technology

(FT) Food Technology

(OG) Oil & Gas Technology

(AT) Automotive Technology

(AV) Aerospace & Aviation Technology

(NT) Nano Technology

(CS) Cyber Security Technology

* Updated as of Board Meeting No. 9/2017 : Nov 22, 2017

BENEFITS OF BEING CERTIFIED

- Recognition & Acceptance – Individual designation of Ts./ P.Tech or Tc./ C.Tech for peers and industrial acceptance

- Talent Mobility – More opportunity for professionals from every level of technology field

- Lifelong Learning – MBOT adopt CPD hours which will encourage professional to attend professional courses & it can be done directly through TEP members

- Technology Fora & Programs – Regular fora & programs which will be conducted by MBOT and TEP for each technology field

LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

PROFESSIONAL BODY FOR

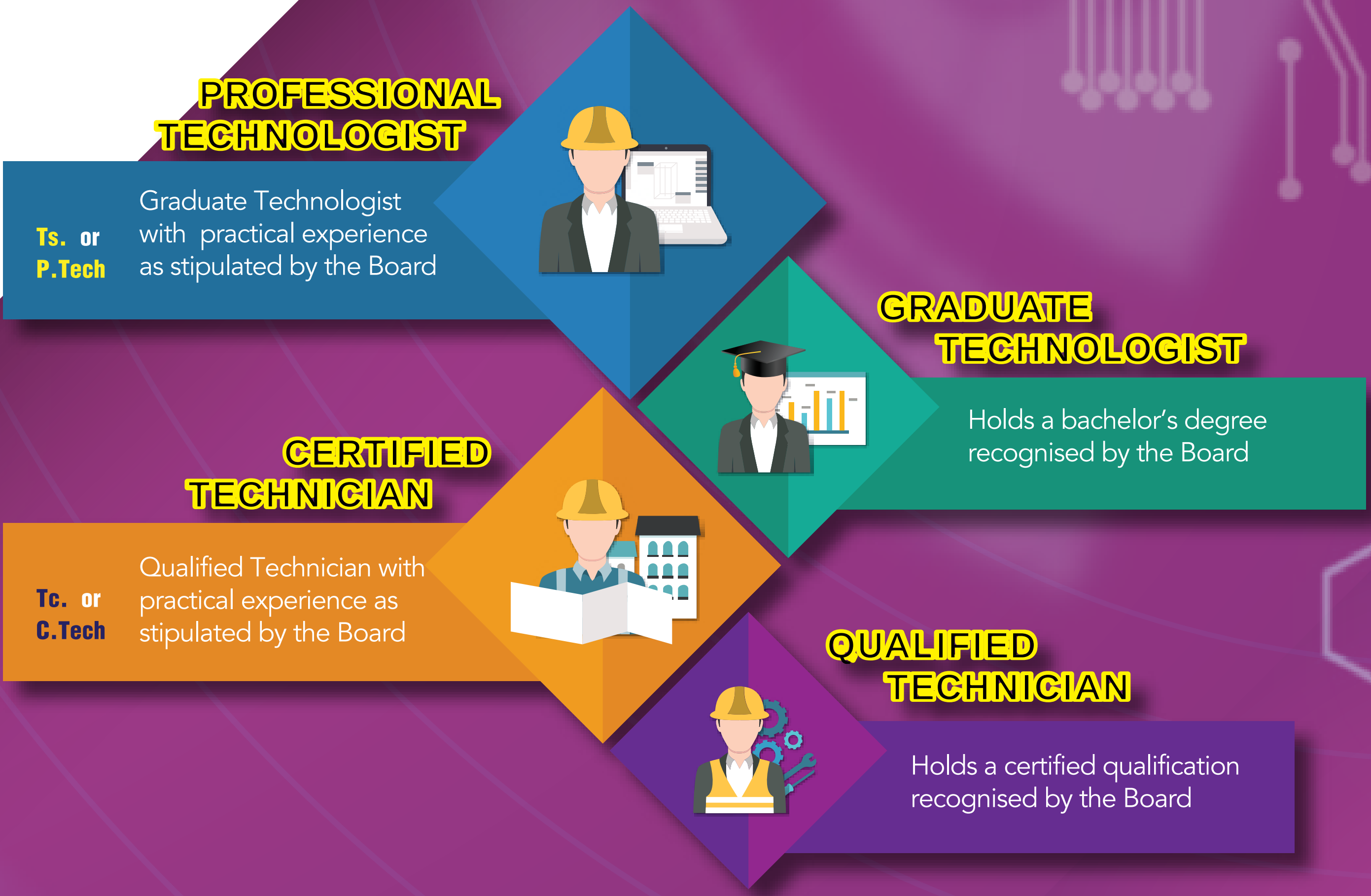
TVET Malaysia

Empowering People • Advancing Nation

www.mbot.org.my

LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGISTS

MEMBERSHIP REGISTRATION



PROFESSIONAL TECHNOLOGIST

Ts. or P.Tech

Graduate Technologist with practical experience as stipulated by the Board

GRADUATE TECHNOLOGIST

Holds a bachelor's degree recognised by the Board

CERTIFIED TECHNICIAN

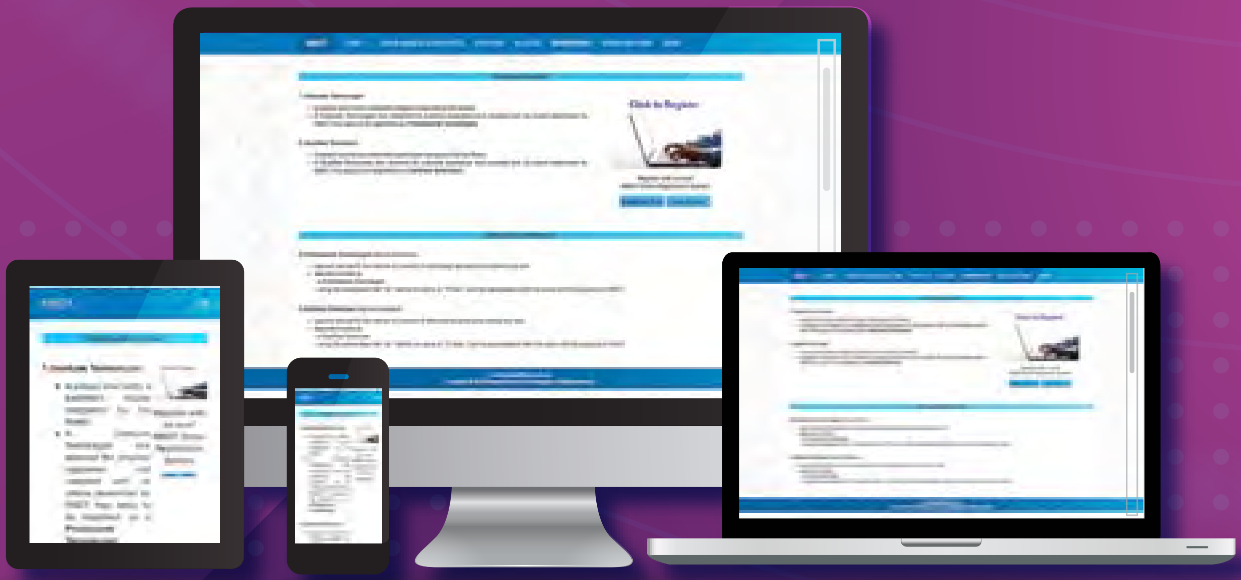
Tc. or C.Tech

Qualified Technician with practical experience as stipulated by the Board

QUALIFIED TECHNICIAN

Holds a certified qualification recognised by the Board

Visit www.mbot.org.my for registration



CONTACT US: registration@mbot.org.my
Malaysia Board of Technologists
A1-3-1, Ayer@8, Jalan P8G, Presinct 8, 62250 Putrajaya | Telephone: 03-8800 6268 | E-mail: info@mbot.org.my