MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

2020 ANNUAL REPORT

COVER RATIONALE

At the end of 2019, the world was hit by a devastating Covid-19 pandemic. Malaysia is no exception, the whole country affected by this pandemic. Some of them lost their job, lives, and family members.

To mitigate this pandemic, the government has implemented the Movement Control Order. All economic sectors including offices, factories, and schools were shut down to break the chain of this Covid-19 pandemic.

Various new norms were introduced throughout 2020 to ensure that the company's operations could be carried out despite being in the Movement Control Order. Online meetings have become a new norm and working from home has become routine for every sector of the economy to enable the operations of a company to remain running.

CyberSecurity Malaysia's 2020 Annual Report is inspired by the implementation of the new norms of working at home.

TABLE OF CONTENT

1

INTRODUCTION

ABOUT CYBERSECURITY MALAYSIA

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency under supervision of the Ministry of Communications and Multimedia Malaysia (KKMM). Pursuant to the Federal Government Ministerial Order 2019, with effect from 21 May 2018, CyberSecurity Malaysia is placed under KKMM.

CyberSecurity Malaysia is committed to provide a broad range of cybersecurity innovation-led services, programmes, and initiatives to reduce vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace.

The agency provides the following specialised cybersecurity services.

1. Cyber Security Responsive Services
2. Cyber Security Proactive Services
3. Outreach and Capacity Building
4. Strategic Study and Engagement
5. Industry and Research Development

History of CyberSecurity Malaysia

Our journey started with formation of the Malaysia Computer Emergency Response Team or MyCERT (www.mycert.org. my) on 13 January 1997 as a unit under MIMOS Berhad (www.mimos.my). On 24 January 1998, the National Information Technology Council (NITC) chaired by the Prime Minister of Malaysia proposed for the establishment of an agency to address emerging ICT security issues in Malaysia. As a result, the National ICT Security and Emergency Response Centre (NISER) was formed in 2001 as a Department in MIMOS Berhad, and MyCERT was placed under NISER.

The Cabinet Meeting on 28 September 2005, through the Joint Cabinet Notes by the Ministry of Finance (MoF) and Ministry of Science, Technology and Innovation (MOSTI) No. H609/2005 agreed to establish NISER (now known as CyberSecurity Malaysia) as a National Body to monitor the National e-Security aspect, spun-off from MIMOS Berhad to become a separate agency and incorporated as a Company Limited-by-Guarantee. On 30 March 2007, NISER was registered as a not-for-profit, Company Limited-by-Guarantee under supervision of MOSTI.

The NITC Meeting No. 1/2006 decided to implement the National Cyber Security Policy (NCSP) led by MOSTI. NISER was mandated to provide technical support for NCSP implementation and was rebranded to CyberSecurity Malaysia to reflect its wider mandate and larger role. On 20 August 2007, the Prime Minister of Malaysia officiated CyberSecurity Malaysia and launched its new logo.

Vision

World-class cyber security specialist agency.

Mission

Leading the development of a safer and more resilient cyber ecosystem to enhance national security, economic prosperity, and social harmony through

- Provision of quality and impactful services
- Frontier-expanding cyber knowledge and technical supremacy
- Continuous nurturing of talent and expertise

HISTORY

2018

19 OCTOBER 2018

The Cabinet Meeting decided CyberSecurity Malaysia to be placed under the Ministry of Communications and Multimedia Malaysia (KKMM)

2007

30 MARCH 2007

NISER was officially registered as CyberSecurity Malaysia

20 AUGUST 2007

CyberSecurity Malaysia was officially launched by the Prime Minister of Malaysia

2005

28 SEPTEMBER 2005

The Cabinet decided for NISER to spun-off from MIMOS Berhad as a Company Limited-by- Guarantee under the Ministry of Science, Technology and Innovation (MOSTI)

2001

2001

The National ICT Security and Emergency Response Centre (NISER) was established as a Department in MIMOS Berhad, and Malaysia Computer Emergency Response Team (MyCERT) was placed under NISER

1997

13 JANUARY 1997

The journey started with formation of the Malaysia Computer Emergency Response Team or MyCERT (www.mycert.org.my) as a unit under MIMOS Berhad (www.mimos.my)

OUR SERVICES

1 Malaysia Computer Emergency Response Team (MyCERT)

MyCERT
Malaysia Computer Emergency Response Team

Cyber999 Help Centre
www.mycert.org.my/cyber999

Cyber999 Help Centre provides expert service to internet users and organizations on cyber security incidents. Cyber security incidents can be reported via online form, email, SMS, phone call, fax, Cyber999 Mobile App and walk-in reporting. Cyber999 Help Centre also produces Malaysia Threat Landscape report, technical findings and analysis based on the incidents reported by Internet users.

Cyber Threat Research Centre (CTRC)

Cyber Threat Research Centre (CTRC) provides specialized service in multiple cyber security domains to create visibility and awareness in order to encounter current cyber security threats and identify upcoming threats. It supports Cyber999 operations and establishes cyber security research on malware, mobile security, threat hunting, web security and network security.

MASSA

Coordinated Malware Eradication & Remediation Project (CMERP)

Coordinated Malware Eradication & Remediation Platform (CMERP) provides specialized service that mitigate malware threats, minimize incident response time and spread security awareness to end user in Malaysia. Its objective is to decrease cyber incidents cases involving malware threats. The service is offered based on CTRC technical expertise research outcomes.

Lebahnet (Honeynet Project)

Lebahnet 2.0 Project provides supporting information on network trends and malicious activities for MyCERT to handle incident as well as advisory activities. Honeypots which is a collection of computer software mechanisms established to mimic a legitimate site to ensnare malicious software into believing that the device is in a weak position for attacks. It allows researchers to detect, monitor and counter-attack malicious activities by understanding activities completed during intrusion phase and attacks' payload.

CSIRT Consultancy

Computer Security Incident Response Team or CSIRT Consultancy provides specialized expert service for organizations in terms of People, Process and Technology. It creates an implementation plan to develop and implement CSIRT in organizations. The consultancy also provides Incident Handling & Network Security trainings, Job Attachments, including Professional Memberships to FIRST, APCERT and OIC-CERT.

2 Digital Forensics (DF)

CyberCSI
www.cybercsi.my

CyberCSI provides digital forensics services to Law Enforcement Agencies (LEA) through these offering:

- Onsite Evidence Preservation
- Evidence Analysis
- Expert Witness in Court
- Professional Training

CyberCSI is committed to provide quality and accurate forensics outcome based on well-trained and experience analysts. Our digital forensics laboratories are accredited with ANSI National Accreditation Body (ANAB) since 2011.

CyberDEF

Cyber Detect, Eradicate and Forensics (CyberDEF) provides pro-active cyber defense forensics service to mitigate operational risk in cyberspace. This service is offered to Critical National Information Infrastructure (CNII) organizations sectors such as the government, banking and finance, information and communication and health services. CyberDEF identifies solutions for cyber intrusion, APT malware and ransomware by detecting threat, eradicate source and conduct forensic investigation to outline potential cause.

Cyber Discovery

CyberDiscovery is a cyber forensics service offered for private organization. It addresses concern on Electronic Stored Information (ESI) in order to provide solution to civil litigation. It provides the following services:

- Onsite Evidence Preservation
- Evidence Analysis
- Expert Witness in Court

PenDua x-Forensik 2.0 Kloner x-Forensik 2.0 CamMuka 2.0

3 Information Security Management & Assurance (ISMA)

Information Security Management System (ISMS) Guidance Series

Information Security Management System (ISMS) Guidance Series is a service provided to government agencies, corporate organizations, small medium enterprises (SME) and any interested corporation to guide the organization on the implementation of information security. It ultimately prepares them to fulfil all requirement for ISO/IEC 27001 Information Security Management System certification.

Information Security Governance, Risk & Compliance (ISGRiC)

Information Security Governance, Risk & Compliance or ISGRiC Health Check Assessment is a service provided to government agencies, corporate organisations, small medium enterprises (SME) and any interested corporation to assist them in determining their current level of readiness and initiatives in information security governance, risk management and compliance. It also assists management in making informed decisions based on ISGRiC results to justify information security investment and support the business case for managing information security.

4 MalaysianSecurity Evaluation Facility

Malaysian Security Evaluation Facility

Evaluation and Assessment Service

Evaluation and Assessment Service is an independent evaluation facility by CSM MySEF to evaluate the ICT products and systems under various certifications schemes or initiatives, namely Common Criteria Evaluation & Certification (MyCC), Technology Security Assurance (TSA), ICT Product Security Assessment (IPSA) and Cloud Security Assessment.

Cloud Security Audit Service (CSAS)

Cloud Security Audit Service (CSAS) is a niche security auditing on cloud computing services, focuses on cloud computing implementation on all types of cloud services model (IaaS,PaaS and SaaS). This service is provided to Cloud Service Providers, Cloud Service Subscribers and Cloud Service Brokers which allow organizations to ensure secured cloud deployment and service subscription.

Common Criteria (CC) Laboratory Development and Advisory Service

Common Criteria Evaluation Laboratory Development and Advisory Service provides technical services and advisories to existing and potential CC laboratories, in terms of developing Standard Operating Procedure (SOP) and preparing for accreditation.

ISO/IEC 17025 Professional Laboratory Service

ISO/IEC 17025 Professional Laboratory Service is offered to external laboratories for laboratory/ equipment rental and Inter-Laboratory Comparison (ILC) exercise.

- Laboratory/equipment rental for ICT products testing and evaluation services;
- Inter-Laboratory Comparison (ILC) exercise is mandatory for any ISO/IEC 17025 Test Lab in Malaysia. CSM MySEF offers this service based on the Scope of Work (SOW) agreed by both Test Labs which covers security evaluations, security functional testing or penetration testing.

5 Malaysia Vulnerabilities Assessment Centre (MyVAC)

Vulnerability Assessment & Penetration Testing (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) is a service offered to public and private organizations to discover and highlight security issues at client environment. It provides recommendations and countermeasures to rectify the vulnerabilities in order to reduce risk of security breach.

Industrial Control System (ICS)

Industrial Control System (ICS) service improves security posture of Critical National Information Infrastructure (CNII) organizations through security assessment or evaluation to increase nation's ability in mitigating cyber threats and exploitation due to critical information systems and technology vulnerabilities. ICS offers the following services:

- Security Architecture Validation
- Security Configuration Validation
- Electrical Power Transmission Simulation Testbed Rental
- Oil & Gas Pipelines Simulation Testbed Rental

Secure Software Development Lifecycle (SSDLC)

Secure Software Development Lifecycle (SSDLC) provides service to organizations to improve system security, build own secure software development process and manage security controls for all stages of software development life cycle. SSDLC services offer the following:

- Security Architecture and Design Review
- Secure Source Code Assessment
- Professional Capacity Facility Center Rental

IR4.0 & Internet of Things (IoT)

The Fourth Industry Revolution (IR4.0) and Internet of Things (IoT) provides service to improve nation's resilience against cyber threats. It consists of several labs available for rental as follow:

- Industrial Robotic Testbed Rental
- Small Scale Smart Manufacturing Testbed Rental
- Smart Meter Testbed Rental
- Smart Home Testbed Rental

These testbeds can be rented for education research, hands-on training and industrial testing.

Training and Facility Services

Training and Facility services promote awareness and educate CNII organizations on vulnerabilities and possible attacks to their critical infrastructures. The services include:

- Introduction to ICS Security Training
- PHP Secure Coding Training
- Certified Secure Web Application Defender/Developer (CSWAD)
- IoT Security Training
- Training Room Facilities

6 Government Engagement (GE)

Government Engagement
cnii.cybersecurity.my

Government Engagement offers strategic engagement services with stakeholders within the Malaysian Government. It aims to identify and lead various cyber security programs, collaborations, working relations and activities to advocate and enhance the prominence of cyber security agenda for the nation. CyberSecurity Malaysia is also the administrator for the Critical National Information Infrastructure (CNII) portal.

7 Government Engagement (GE)

International Engagement

International Engagement provides multilateral relations service to enhance cyber security corporation globally among the Computer Emergency Response Teams (CERTs) and other information security organizations. It assists CyberSecurity Malaysia to establish and support cross border collaboration, bilateral and multilateral platforms in the effort to achieve a safe and secured cyber space.

8 Information Security Certification Body (ISCB)

MyCC Scheme
www.cybersecurity.my/mycc

Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme is a systematic process for evaluating and certifying security functionality of ICT products based on defined criteria or standards. This scheme ensures high standards of competence and impartiality as it is based on the international standards of ISO/IEC 15408 which is known as Common Criteria (CC).

Information Security Management System (ISMS) Audit and Certification - CSM27001 Scheme
csm27001.cybersecurity.my

CyberSecurity Malaysia Information Security Management System (ISMS) Audit and Certification (CSM27001) Scheme is an audit and certification services offered to the organizations based on the ISO/IEC 27001 standard. It identifies data security breaches and reduces information security risks in an organization. Effective ISMS ensures organizational confidentiality, integrity and availability of information, thus, achieve business efficiency and minimise business loss.

Business Continuity Management System (BCMS)

BCMS Certification Scheme is a service offered to various organizations which envision resiliency based on the ISO 22301 international standard. It helps to plan an effective business continuity management to protect, reduce and ensure business recovers from disruptive incidents.

Technology Security Assurance (TSA)

Technology Security Assurance (TSA) is a national scheme specially developed for product evaluation and certification. It is MyCC fast-track which includes security evaluation, certification and assurance maintenance. The Security Functionality Testing and Penetration Testing evaluate local ICT products to identify vulnerability and assist organizations to understand and improve its security features.

Penetration Test Service Provider (PTSP)

Penetration Test Service Provider (PTSP) is a national scheme provided to the local penetration testing service providers and organizations that require penetrating test services. The service encourages local cybersecurity industries' development and competitiveness to ensure organizational ethics are practiced according to guideline and best practices.

9 CyberSecurity Industry Engagement and Collaboration (CIEC)

CyberSecurity Malaysia Collaboration Program (CCP)
ccp.cybersecurity.my

CyberSecurity Malaysia Collaboration Program (CCP) serves as a strategic collaboration initiative with local cyber security industry as well as other government entities to encourage development and innovation of Malaysia's cyber security products and services. CCP provides access to potential collaborations and synergies with CyberSecurity Malaysia, related government entities and with other collaborators. This leverages partners' strengths and bridge market gaps by providing high quality and highly relevant cyber security products and services.

Cyber Security Malaysia Awards, Conference and Exhibition (CSM-ACE)
www.csm-ace.my

Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE) is a public-private-partnership driven and a knowledge sharing platform that recognise individuals and organizations contribution in cyber security field.
CSM-ACE envisions the following:

- to act as a catalyst in driving innovation and growth for cyber security industry
- to inculcate cyber security culture at national level
- to gather industry experts and community to discuss latest cyber security trends
- to showcase trade & investment opportunities by assisting & allowing industry players to promote their products and services

My CyberSecurity Clinic (MyCSC)
www.cybersecurityclinic.my

MyCyberSecurity Clinic provides trustworthy and convenient data recovery and data sanitization services that handle data in a safe, secured and confidential manner.

- Data Recovery Service - a solution to recover data from damaged, failed, corrupted or inaccessible digital storage media.
- Data Sanitization Services - address the organization's need for safe and secure deletion of data from storage devices that are retired, upgraded or reallocated.

10 Strategic Research (SR)

Strategic Research

Strategic Research and Advisory (SRA) provides research, information and advisory services on cyber security, which is the source of reference for partners, industry as well as for stakeholders in order to establish well-informed decisions. SRA covers the area of law and regulations, policies, strategies and guidelines at the global landscape as well as within Malaysia ecosystem.

11 Outreach & Corporate Communications (OCC)

CyberSAFE
www.cybersafe.my

Cyber Safety Awareness for Everyone (CyberSAFE™) is a dedicated program developed to educate and inculcate cyber security awareness and foster a safe digital world to the general public. It addresses technology and social issues faced by Internet users. Amongst the objectives are:

- To reduce vulnerability of ICT systems and networks;
- To nurture culture of cyber security among users and critical sectors; and
- To strengthen Malaysian self-reliance in terms of technology and human resources.

Information Security Management System (ISMS) Audit and Certification - CSM27001 Scheme
csm27001.cybersecurity.my

CyberSecurity Malaysia Information Security Management System (ISMS) Audit and Certification (CSM27001) Scheme is an audit and certification services offered to the organizations based on the ISO/IEC 27001 standard. It identifies data security breaches and reduces information security risks in an organization. Effective ISMS ensures organizational confidentiality, integrity and availability of information, thus, achieve business efficiency and minimise business loss.

CyberSAFE™ L.I.V.E. Galeri

CyberSAFETM L.I.V.E. Galeri is developed as one of the initiatives under the CyberSAFE Program aims at fostering awareness on cyber security and safety as well as to increase understanding and interest in the cybersecurity field. The information displayed in this gallery is expected to raise public awareness on the importance of cybersecurity and the roles and functions of CyberSecurity Malaysia in strengthening cybersecurity infrastructure and ecosystem in the country.

This gallery is recognised by the Malaysia Book of Records as the 'First Cyber Security Gallery' in Malaysia. It is a hub for learning and teaching as well as disseminating information on cybersecurity. L.I.V.E stands for Learning, Interactive, Virtual & Experiential

- Learning - Inductive learning environment
- Interactive - the modules and activities provided are interactive
- Virtual - realizing the virtual world to the physical world and vice versa
- Experiential - at the end of the visit, visitors bring home an experience consisting of cybersecurity knowledge, advancement and guidelines

12 Cyber Security Professional Development (CSPD)

CyberGURU
www.cyberguru.my

CyberGURU consists training services offered to public on cyber security professional development. It aims to increase number of competent and certified cyber security professionals in Malaysia through various competency training courses, certifications as well as knowledge-sharing platform for the ICT workforce.

Global Accredited Cybersecurity Education (ACE) Scheme
www.cybereducationscheme.org

The Global Accredited Cybersecurity Education (ACE) Scheme is a holistic framework of cyber security professional certification that outlines the overall approach, independent assessments, impartiality of examinations, competencies of trainers, identification and classification of cyber security domains and the requirements of professional memberships. It is a national scheme for cyber security capacity and capability programme to certify and recognise cyber security personnel in tandem with ISO/IEC 17024 on people certifications, ISO/IEC 9000 on processes and ISO/IEC 27001 on security management. It is approved locally and globally by Board of Technologist (MBOT), Jabatan Pembangunan Kemahiran (JPK), Ministry of Human Resources. and the Organization of Islamic Cooperation (OIC).

13 Cryptography Development

CyberSecurity Malaysia Cryptographic Evaluation Laboratory (MyCEL)

CyberSecurity Malaysia Cryptographic Evaluation Laboratory (MyCEL) was accredited by the National Voluntary Laboratory Accreditation Program (NVLAP), USA

With this accreditation, MyCEL is able to carry out the evaluation and validation activities of cryptographic modules contained in a security product based on FIPS140 security requirements. This enhanced the user's security and trust in using cryptographic module in security products

CyberSecurity Malaysia Cryptographic Evaluation Laboratory (MyCEL) was accredited by the National Voluntary Laboratory Accreditation Program (NVLAP), USA

MY Cryptographic Module Validation - ISO/IEC 19790

Malaysia scheme for validating and certifying cryptographic modules based on ISO/IEC 19790:2012 standard

CD performs validation activities based on testing methods specified in ISO/IEC 24759:2017

Senarai Algoritma Kriptografi Terpercaya Negara

https://myseal.cybersecurity.my

MySEAL is a project to develop a portfolio of national trusted cryptographic algorithms. It is a project specifically designed to provide a list of cryptographic algorithms suitable for implementation within Malaysian context that supports National Cryptoraphy Policy (NCP) or Dasar Kriptografi Negara. While NCP serves as a guiding document for Malaysia to achieve cryptographic sovereignty, MySEAL will support in the scientific areas of cryptography and cryptanalysis.

Cryptanalysis and other Cryptographic Evaluation

Other analysis / evaluation services that related to cryptography:

- Cryptanalysis
- Cryptographic algorithm conformance testing
- Randomness testing using CRTT

Research & Development

CD involves in the R&D initiatives that related to cryptography and Distributed Ledger Technology. Among our R&D projects are:

CiliPadi Lightweight Cryptographic Algorithm

SmartPay System – Cashless payment system on Ethereum Blockchain platform
Under this service, we welcome any partnerships with local and international parties to accelerate the development of cryptography.

14 Secure Technology Services (STS)

Coordinated Malware Eradication & Remediation Platform - Advanced DNS Firewall (CMERP ADF)

Today's threats are evolving at an exponential rate with new methods for distribution, infection, infiltration and evasion. These new techniques are continually overcoming traditional cyber defences. The Internet is becoming ubiquitous, and we live in a hyper-connected world. With CMERP ADF such attacks can be stopped.

CMERP ADF has indexed 99.9% of the Internet, which includes more than 1.7billion websites and 350 million top-level domains growing daily. With this intelligence, CMERP ADF is able to protect global businesses and users.

CMERP ADF blocks zero-day attacks and identifies malicious activity. It handles DNS requests from users and redirects malicious requests to a sinkhole providing a new layer of security with artificial Intelligence.

2

CORPORATE GOVERNANCE

General Tan Sri Dato' Seri Panglima Mohd Azumi Bin Mohamed (Retired),
Chairman, Board of Directors

CHAIRMAN'S STATEMENT

2020 was a year of trials and tribulations for the world. It made a world of difference for us, changing the way we interacted, be it government or the private sector. Digital interactions was the order of the day, ranging from tele conferencing to online shopping. As Tom Standage put it, "the adoption of new technological behaviours in response to the pandemic, tech celeration". In brief, life has gone online. As our dependence and reliance on digitally connected systems and devices grew, our vulnerabilities too grew, forcing us to contend with cyber threats.

According to a research survey by Cisco Systems on Asia Pacific countries, cybersecurity challenges persisted amongst Malaysian organisations during 2020, with 62% of respondents experiencing 25% or more increase in either cyber threats or alerts since the start of Covid-19 pandemic. The study revealed that 60% of respondents in Malaysia practised remote working during the pandemic, compared to 20%. More importantly, the poll showed that 49% of Malaysian organisations ranked cybersecurity as more important than before the pandemic.

On the consumer digital front, the e-Conomy SEA 2020 report jointly issued by Google, Temasek and Bain & Company revealed that 40 million new users in South East Asia joined the Internet bandwagon in 2020, compared to 100 million users between 2015 and 2019. The Covid-19 pandemic also led to an acceleration of new digital services for the first time. Malaysians spent an estimated 3.7 hours online pre-Covid-19, which spiked to 4.8 hours at the height of the lockdown in 2020. The digital focus for business, employees and consumers have been unprecedented.

I am pleased to say that despite challenges in remote working and additional compliance to Standard Operating Procedures (SOPs), CyberSecurity Malaysia consistently delivered outreach initiatives to address growing cyber threats, inculcate cyber safety awareness and enhance capacity building. The list of activities undertaken were extensive, covering community awareness on cyber safety during **Safer Internet Day 2020**, cyber security skills and training workshops for government agencies and private sector.

In August 2020, CyberSecurity Malaysia also signed a Memorandum of Strategic Cooperation with the Department of Personal Data Protection or *Jabatan Perlindungan Data Peribadi* (JPDP) to strengthen cooperation and collaboration in the field of cybersecurity. Through this collaboration, CyberSecurity Malaysia shared the latest knowledge and expertise with JPDP to ensure the standard of personal data protection is upheld to its highest level. Among the key areas of cooperation included sharing of information on cyber incidents related to personal data, advisory services related to cybersecurity, development of digital forensic laboratories and digital data centres, as well as human capital development.

On the international front, I am immensely proud of the recognition bestowed on CyberSecurity Malaysia at the **World Summit on the Information Society (WSIS)** forum held in Geneva, Switzerland in September 2020. CyberSecurity Malaysia was selected as project winner on the Global Accredited Cybersecurity Education (ACE) Scheme: Centre of Excellence for Capacity Building and Lifelong Learning project for ***'Building Confidence and Security in Use of ICTs'*** category. WSIS was jointly organised by the International Telecommunication Union (ITU), the United Nations Educational, Scientific and Cultural Organisation (UNESCO), the United Nations Development Programme (UNDP) and the United Nations Conference on Trade and Development (UNCTAD).

The Global ACE Scheme project is a professional development scheme in the field of cyber security developed by CyberSecurity Malaysia, in collaboration with government agencies, industry, academic institutions and supported by the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT). The scheme, developed in line with international standards, successfully created a single converging platform for the development of capabilities and lifelong learning to enable individuals to improve their skills and enhance their knowledge in the cyber security sector.

Throughout 2020, CyberSecurity Malaysia made good progress as we continued to actively participate in international dialogues to share key learnings and our successes in managing cyber threats including Regional Dialogue CyberDrill 2020: Asia and the Pacific organised by International Telecommunication Union (ITU). The dialogue, attended by senior members from **UNODC Regional Office for Southeast Asia and the Pacific, Asia-Pacific Network Information Center (APNIC), Oceania Cyber Security Centre (OCSC), APCERT** as well as representatives of **CSIRT/CIRT/ CERT** from all member states, allowed for exchanges of experience in dealing with cybersecurity issues during the Covid-19 pandemic.

Another feather was capped on 29 September 2020 when CyberSecurity Malaysia was re-elected as Chair of the Asia Pacific Computer Emergency Response Team (APCERT) at its Annual General Meeting (AGM), held virtually for the first time due to the pandemic.

As Chair for the third time from 2020/2021, CyberSecurity Malaysia is ever committed to galvanize more involvement from the members in moving forward, while continuing to lead the APCERT Malware Mitigation Working Group, a collaborative initiative among the APCERT and OIC countries on malware research, analysis and response to protect the community against malware threats.

The re-election underscored CyberSecurity Malaysia's technical expertise, strong leadership, and professionalism to provide strategic direction and guidance to maintain the relevancy of APCERT. As joint co-founders of APRCET since 2002, CyberSecurity Malaysia also remains on its steering committee until 2021.

Looking ahead, CyberSecurity Malaysia aims to encourage greater multilateral collaboration, develop comprehensive frameworks and sharing of cyber security knowledge to build a more trusted and resilient cyber ecosystem in Malaysia. This is the time for us to think about how to do things differently. Despite the challenging times, we remained optimistic and focused on charting the cyber security future of our nation.

Looking forward to a another productive and successful year ahead for CyberSecurity Malaysia.

General Tan Sri Dato' Seri Panglima
Mohd Azumi Bin Mohamed (Retired)
Chairman, Board of Directors, CyberSecurity Malaysia

BOARD OF DIRECTORS

General Tan Sri Dato' Sri Panglima Mohd Azumi bin Mohamed (Retired)
- *Chairman, Board of Directors, CyberSecurity Malaysia,*

Dato' Suriani binti Dato' Ahmad
- *Secretary General of the Ministry of Communications and Multimedia Malaysia*
- *Director, CyberSecurity Malaysia*

(appointed w.e.f 24 October 2019 - 20 November 2020)

Dato' Ts. Dr. Haji Amirudin bin Abdul Wahab FASc
- *Chief Executive Officer, CyberSecurity Malaysia*
- *Director, CyberSecurity Malaysia*

Datuk Dr. Abdul Rahman bin Saad
- *Director, CyberSecurity Malaysia*
- *Chairman Audit Governance & Integrity Committee CyberSecurity Malaysia*

(appointed w.e.f 24 October 2019 - 20 November 2020)

Mohd Sori Bin Husain
- *Director, CyberSecurity Malaysia*

(appointed w.e.f 24 October 2019 - 20 November 2020)

Shaifubahrim Bin Mohd Saleh
- *Director, CyberSecurity Malaysia*

(appointed w.e.f 24 October 2019 - 20 November 2020)

CORPORATE GOVERNANCE

The Board of Directors of CyberSecurity Malaysia is pleased to report that for the financial year under review, CyberSecurity Malaysia has continued to apply good corporate governance practices in managing and directing the affairs of CyberSecurity Malaysia, by adopting the substance and spirit of the principles advocated by the Malaysian Code on Corporate Governance ("the Code").

BOARD RESPONSIBILITIES

The board maps out and reviews CyberSecurity Malaysia's strategic plans on an annual basis to ensure CyberSecurity Malaysia's operational directions and activities are aligned with the goals of its establishment by the government of Malaysia. The board considers in depth, and if thought fit, approves for implementation key matters affecting CyberSecurity Malaysia which include matters on action plans, annual budget, major expenditures, acquisition and disposal of assets, human resources policies and performance management. The board also reviews the action plans that are implemented by the management to achieve business and operational targets. The board also oversees the operations and business of CyberSecurity Malaysia by requiring regular periodic operational and financial reporting by the management, in addition to prescribing minimum standards and establishing policies on the management of operational risks and other key areas of CyberSecurity Malaysia's activities.

The board's other main duties include regular oversight of CyberSecurity Malaysia's operations and performance and ensuring that the infrastructure, internal controls and risk management processes are well in place.

The following Board Committees, which were set up, have also fulfilled their specific responsibilities.

1. The Human Resources and Remuneration Committees (HRRC)

i. Objectives:

- Develop and periodically review the overall remuneration policy and human resource strategies of CyberSecurity Malaysia to ensure that it is contributing effectively to the success of the company.
- Ensure the integrity of the remuneration policies and human resource practices and their effectiveness and compliance within the Company.

ii. Duties:

Performance-based remuneration for CyberSecurity Malaysia's Chief Executive Officer (CEO).

- To review and recommend to the board a performance-based remuneration for the CEO, or the person performing the duties and assuming the responsibilities of the CEO, by reference to the corporate goals and objectives as resolved by the board from time to time.

The Company's Human Resource Matters including:

- To review the overall market positioning of the Company's remuneration package and policies, on an annual basis, with a view to retain and/or attract high caliber staff and thereafter submit an appropriate recommendation for the Board's consideration and approval.
- To review the Company's Human Resources development programs and policies related to the remunerations and ensure compliance with the applicable laws and regulations of the country.
- To review the rewards and remunerations of the company staff as to demonstrate that rewards and remunerations are considered by a committee which has no personal interest in the outcome of its advice and which give due regards to the interest of the Company and its financial health.
- To undertake, consider and act on other human resource related issues or tasks as the committee consider appropriate or as may be referred to by the Board.
- To periodically review and participate in determining the organizational structure for the Company.
- To review potential candidates for hiring and promotion for the Top Management positions of the Company.

iii. Members:

1. YBhg. Dato' Dr. Suhazimah Binti Dzazali
2. Puan Azizatul Yusna Binti Ahmed Yusuff

iii. Size and Composition

- The HRRC shall consist of not less than three (3) directors from the board members. They are appointed by the CyberSecurity Malaysia's board of directors.
- The duration of HRRC membership shall be the same as appointment of the members for Board. The re-election of

current members or appointment of new member shall be made by the Board after the expiring of the existing term.

- The board may from time to time appoint additional members to the HRRC from among its members and such other persons as the board deems fit.
- The HRRC may invite any director, member of the company's i.e. management or other person to attend its meeting(s) from time to time when it is considered desirable to assist the HRRC in attaining its objectives.

v. Meetings

- The HRRC shall have meetings at least twice a year. Additional meetings may be conducted at any time with the consensus from all members of the committee.
- All decisions of the HRRC shall be by majority vote. In the event of a tie, the chairperson shall have the second or casting vote in addition to his or her original vote.
- The quorum for HRRC meeting shall be two (2) members of the appointed members.
- The Head of Human Capital Department ("HCD") is the secretary for this committee. In the absence of the head of HCD, a representative from HCD shall replace the head of HCD in carrying out the secretariat function.

1. Audit, Governance and Integrity Committee (AGI) Duties:

i. Audit

- Ensure scheduled audits and planning of audit plans are undertaken by the department in charge of audit, governance and integrity as a control and monitoring measure on the financial and operational management of the company.
- Follow-up the audit issues raised in the Laporan Ketua Audit Negara (LKAN) or weaknesses highlighted by the Jabatan Audit Negara by ensuring that the management is performing immediate actions and corrective actions on the issues as well as establishing and monitoring the compliance of the expected completed dates and timeline of corrective actions.
- If the audit issue raised is brought to the attention of the Putrajaya Inquisition or Jawatankuasa Kira-kira Wang Awam (Public Accounts Commitee), the AGI chairman is responsible to be present with the management to explain.
- Reviewing the requirements of the department in charge of audit, governance and integrity including its charter.
- The Audit, Governance and Integrity Committee shall submit reports at Board meetings at least twice a year or at the frequency to be decided by the Committee or requested by the Board. If no audit observation is received, the Audit, Governance and Integrity Committee shall report so at the Board meetings.
- To review the Company's final statements of accounts prior to submission to the Board, to ensure compliance with disclosure requirements and adjustments suggested by the auditors.
- To review the internal controls, performance and findings of the internal auditors and to recommend and implement appropriate remedial and corrective actions.
- To recommend to the Board the appointment of external auditors of the Company, the audit fee and any matter of resignation or dismissal.
- To discuss any matters arising from the previous year's audit, to review the scope of the current year's audit, the plans for carrying out the audit, the extent of planned reliance on the work of other independent auditors and the Company's own internal auditors.
- To review any significant audit problems that can be foreseen either as a result of the previous years' experience or because of new developments.
- To evaluate and review the role of the internal and external auditors from time to time.
- To review any significant related party transactions that may arise within the Company.
- To review any significant transactions which are not a normal part of the ordinary business of the Company.
- To place the internal auditors under the direct authority and supervision of the Audit, Governance & Integrity Committee and to evaluate and approve their performance and remuneration package. Key Performance Indicator of the department in charge of the audit, governance and integrity to be evaluated by the Committee and Chief Executive Officer.
- To recommend changes in the accounting policies to the Board of Directors.
- To review the assistance given by the Company's officers to the auditors.
- To carry out such other responsibilities as may be delegated by the Board of Directors from time to time.

ii. Governance and Integrity

1. Policy

- To review and recommend amendments to any policy so as to overcome weaknesses in management, improve controls against corruption, malpractices, abuse of powers and administrative weaknesses.
- To evaluate and review strategic plans for enhancing the best governance practices, which are capable of achieving delivery system that is infused with integrity, accountability, trust, fairness, monitoring and stewardship, transparent and responsive to clients.

2. Systems and Work Procedures

To evaluate and review systems and work procedures:

- That are giving rise to various bureaucratic red-tapes, which could possibly weaken administration, reduce efficiency, non-accountability at the same time giving rise to avenues for bureaucratic hassles, delays, injustices and indiscriminate (usage of) discretion as well as providing opportunities for corruption, malpractices and abuse of powers.

- That are transparent and with accountability, optimization of resources and information management system that is efficient and effective to achieve Company's missions and visions or objectives.

3. **Noble Values and Code of Ethics**
   - To review activities that enhances integrity of staffs including consolidation and implementation of policies and procedures that are infused with noble values and code of ethics so as to prevent staff from committing all forms of negative conduct inclusive of corruption, malpractices, and abuse of powers.
   - To review and validate organizational code of ethics.

4. **Customer Management**
   To review the strategic and quality system of customer management in order to portray efficiency, sensitiveness, friendliness and responsiveness towards the needs of clients (be they stakeholders, internal or external clients) and be perceived as providing value-added and continuously improved delivery system, as well as to prevent being seen as slip-ups in the fulfillment of entrusted duties and responsibilities.

5. **Detection, Punitive and Rehabilitation Action**
   To evaluate and review any matters primarily significant problems resulting from contravention of laws, regulations, system and work procedures or code of ethics including any form of offences or crime committed by staff.

6. **Recognition and Appreciation**
   To evaluate and review the recognition and appreciation to staff who have shown exemplary services and exhibiting noble values through voluntary activities by giving religious advice and guidance and those who have reported cases of corruption, malpractices and misconduct within divisions/departments.

7. Ensure the direction of the company is clear with the goals and initiatives implemented by the department in charge of audit, governance and integrity, the Board plays a major role in shaping the climate and the tone of the company whether it is to put integrity on the right track or vice versa.

8. Ensure that the structure of the department in charge of audit, governance and integrity is separate and directly report to the Board to avoid any pressure, escalation, rejection and improper act on the part of the company.

9. Ensure the department in charge of audit, governance and integrity performs the core defined functionality of the department.

10. Provide instructions to the department in charge of audit, governance and integrity to ensure this department remains relevant as an entity responsible for the preservation of integrity in the company.

iii. Members:

1. YBhg. Datuk Dr. Abdul Raman Bin Saad (Chairman)
2. Puan Azizatul Yusna Binti Ahmed Yusuff

Terms of Reference of the AGI

v. Authority

- Authorised by the Board to investigate any activity within its terms of reference and all employees shall be directed to co-operate as requested by the Committee.
- Have unlimited access to all information and documents relevant to its activities, to the internal and external auditors and senior management of the Company.
- Authorised by the Board to obtain outside legal or other independent professional advice and to secure the attendance of outsiders with relevant experience and expertise as it considers necessary.

vi. Size and Composition

- The committee shall consist of at least three (3) but not more than five (5) members of whom the majority shall be independent non-executive Directors of CyberSecurity Malaysia.
- The members of the audit committee shall select a chairman from among them who is not an executive director or employee of the Company or any related organization. The chairman of the Committee may also be appointed by the Board.

vii. Meetings

- Meetings of the committee shall be held at least two (2) times a year or at a frequency to be decided by the committee and the committee may invite any person to be in attendance at such meetings.
- The quorum for meetings shall be two (2).
- Meetings may be convened upon request of the auditors of the Company to consider any matter that the auditors believe should be brought to the attention of the directors.
- The Head of department in charge of audit, governance and integrity shall be the secretary for Audit, Governance and Integrity Committee.

BOARD COMPOSITION AND BALANCE

The board consists of members of high calibre, with good leadership skills and vastly experienced in their own fields of expertise, which enable them to provide strong support in discharging their duties and responsibilities. They fulfil their role by exercising independent judgment and objective participations in the deliberations of the board, bearing in mind the interests of stakeholders, employees, customers, and the communities in which CyberSecurity Malaysia conducts its business.

The ratio between Government Directors and other Directors appointed or to be appointed to the Board of CyberSecurity Malaysia may be determined by the Supervising Ministry; and the appointment of any person as a Director shall first be consented to by the Supervising Ministry. All selected members of the board must obtain the prior approval from the Minister of Domestic Trade and Consumer Affairs (MDTCA). Currently, there are seven (7) members of the Board of CyberSecurity Malaysia.

SUPPLY OF INFORMATION TO THE BOARD

Board meetings are held regularly, whereby reports on the progress of CyberSecurity Malaysia's business and operations and minutes of meetings of the board are tabled for review by the members of the board. At these board meetings, the members of the board also evaluate businesses and operational propositions and corporate proposals that require board's approval.

The agenda for every board meeting, together with comprehensive management reports, proposal papers and supporting documents, are furnished to all directors for their perusal, so that the directors have ample time to review matters to be deliberated at the board's meeting and at the same time to facilitate decision making by the directors.

DIRECTORS' TRAINING

Directors are encouraged to attend talks, training programmed and seminars to update themselves on new developments in relation to the industry in which CyberSecurity Malaysia is operating.

ANNUAL GENERAL MEETING (AGM)

The annual general meeting represents the principal forum for dialogue and interaction with members of CyberSecurity Malaysia namely the Ministry of Finance (Inc.) ("MOF (Inc.)") and the Supervising Ministry. Members are given an opportunity to raise questions on any items on the agenda of the general meeting. The notice of meeting and annual report is sent out to the members of CyberSecurity Malaysia at least 21 days before the date of the meeting which is in accordance with the Constitution of CyberSecurity Malaysia.

NOTICE OF ANNUAL GENERAL MEETING

NOTICE IS HEREBY GIVEN THAT the 15th Annual General Meeting ("AGM") of CYBERSECURITY MALAYSIA ("Company") will be conducted on a fully virtual basis via live streaming from the broadcast venue for the purpose of considering and, if thought fit, passing the resolutions set out in this notice:

AS ORDINARY BUSINESS

1.	To receive the Audited Financial Statements for the financial year ended 31 December 2020 together with the Reports of the Directors and Auditors thereon.	
2.	To approve the payment of Non-Executive Directors' monthly allowances of up to RM204,000 and other benefits payable to the Directors from the date of the forthcoming 15th AGM until the next AGM of the Company.	Resolution 1
3.	To re-elect the following retiring Directors pursuant to Article 54 of the Company's Constitution and being eligible, have offered themselves for re-election: 3.1 YBrs. Encik Shaifubahrim bin Mohd Saleh; 3.2 YBhg. Dato' Dr. Suhazimah binti Dzazali; and 3.3 YBrs. Encik Azih bin Yusof.	Resolution 2
4.	To re-appoint Messrs Jamal, Amin & Partners as External Auditors of the Company for the financial year ending 31 December 2021 and to authorise the Directors to fix their remuneration.	Resolution 3

AS OTHER BUSINESS

5.	To transact any other business of which due notice shall have been given in accordance with the Companies Act, 2016.	

BY ORDER OF THE BOARD

JAILANY BIN JAAFAR
LS0008843
SSM PC No. 201908002687
Company Secretary

Selangor Darul Ehsan
Date : 3 June 2021

NOTES:

i. (a) Due to the on-going Movement Control Order and as part of continuing measures to stem the spread of the Coronavirus Disease (COVID-19), the 15th AGM of the Company will be conducted on a fully virtual basis where members are only allowed to participate and vote remotely via live streaming. Meeting login details and credentials will be provided separately.

(b) The venue of the 15th AGM is strictly for purposes of complying with Section 327(2) of the Companies Act 2016 which requires the Chairperson of the Meeting to be at the main venue ("Broadcast Venue") and to facilitate the conduct of the fully virtual meeting. No members or proxies will be allowed to be physically present at the Broadcast Venue.

ii. A proxy need not be a member of the CyberSecurity Malaysia PROVIDED that a member shall not be entitled to appoint a person who is not a member as his proxy unless that person is an advocate, an approved company auditor or a person approved by the Registrar of Companies.

iii. As an alternate to the appointment of a proxy, a corporate member may appoint its corporate representative to attend the meeting pursuant to Section 333 of the Companies Act 2016 ("Act"). For this purpose and pursuant to Section 333(5) of the Act, the corporate member shall provide a certificate under its common seal as prima facie evidence of the appointment of the corporate representative.

iv. The instrument appointing a proxy shall be in writing under the hand of the appointor or his attorney duly authorized in writing of is the appointor is a body corporate, either under seal or under hand of the officer or attorney duly authorised.

v. To be valid the proxy duly completed/corporate representative certificate must be deposited at the Registered Office of the CyberSecurity Malaysia at Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia not less than forty-eight (48) hours before the time for holding the meeting.

FORM OF PROXY

(COMPANY NO. 200601006881 (726630-U)

*I/We.....

of.....

being a Member of the Company hereby appoint .....

of .....

..or failing him / her .....

of .....

as *my / our proxy to vote for *me / us on my / our behalf at the 14th Annual General Meeting of the Company to be held at *Bilik Conference Jati, Level 10 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor* on the 25 June 2021 at 10.00 am at any adjournment hereof.

Signed this .....day of 2021

(Signature of Appointor)
*Delete whichever is not desired

NOTES :

1. A proxy need not be a member of the CyberSecurity Malaysia PROVIDED that a member shall not be entitled to appoint a person who is not a member as his proxy unless that person is an advocate, an approved company auditor or a person approved by the Registrar of Companies.
2. As an alternate to the appointment of a proxy, a corporate member may appoint its corporate representative to attend the meeting pursuant to Section 333 of the Companies Act 2016 ("Act"). For this purpose and pursuant to Section 333(5) of the Act, the corporate member shall provide a certificate under its common seal as prima facie evidence of the appointment of the corporate representative.
3. The instrument appointing a proxy shall be in writing under the hand of the appointor or his attorney duly authorized in writing of is the appointor is a body corporate, either under seal or under hand of the officer or attorney duly authorised.
4. To be valid the proxy duly completed/corporate representative certificate must be deposited at the Registered Office of the CyberSecurity Malaysia at Level 7 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia not less than forty-eight (48) hours before the time for holding the meeting

3

OPERATION'S REVIEW

When Malaysia went into nationwide lockdown due to escalating number of Covid-19 cases, CyberSecurity Malaysia issued a security best practices alert on 'Work From Home (WFH)' to organisational network system managers and Internet users. As part of our cybersecurity awareness initiatives, we also launched a series of online forums via YouTube from "Makcik Kiah Goes Digital" to "Makcik Kiah Goes Online...Kad Pak Salleh Pulak Decline," which was primarily to spread awareness on safe online purchase methods, procedures and transactions.

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab FASc
Chief Executive Officer

FOREWORD FROM CEO

It is my pleasure to present CyberSecurity Malaysia Annual Report 2020. The year 2020 was unprecedented on many levels. Covid-19 pandemic struck and almost brought the entire world to its knees.

SMEs and small-scale businesses across multiple industries in Malaysia were forced to hasten their move to digital platforms. The work-from-home directive and social distancing restrictions compelled more Malaysians to go online in work, study and daily chores from grocery shopping to paying bills. Although Malaysia's crime index reportedly dropped, a total 10,790 cyber incidents were reported by MyCERT with fraud accounting for 70.3% of incidents.

The Movement Control Order (MCO) not only caused a spike in the usage of technology and Internet, but also elevated the risks of cyber threats and attacks. In spite of the extraordinary challenges presented before us, CyberSecurity Malaysia responded with great tenacity. We continued to innovate across our services and forged new partnerships. The global pandemic also further strengthened our commitment in doing business responsibly while streamlining our processes and best practices. I believe we emerged from 2020 stronger than ever.

In February 2020, CyberSecurity Malaysia led the nation in commemorating Safer Internet Day (SID 2020) with a theme 'Fasih Digital' or 'Digital Fluency'. In line with the theme, the Communications & Multimedia Ministry and CyberSecurity Malaysia launched a nationwide campaign aimed at inculcating ethical and responsible digital citizenship through increased cybersecurity awareness. Throughout the SID campaign, a plethora of activities and programs were carried out to promote and maintain a safer Internet environment and infrastructure, while increasing public understanding on various Internet related issues and topics.

The Malaysian Youth @ Safer Internet Day 2020 (MY@SID) was a one-day youth-led event where 100 selected youth across Malaysia came together to discuss the latest trends, risks and solutions related to the Internet. MY@SID was organised by the youth initiative of the Internet Society Malaysia Chapter and the University of Malaya Law Society, in collaboration with CyberSecurity Malaysia. At the conclusion of the event, the youth produced MY@SID Synthesis Document based on their input and feedback. These participants were also named National Youth Ambassadors for Safer Internet Day Malaysia 2020 for their role in advocating positive use of the Internet and practising good cyber hygiene.

When Malaysia went into nationwide lockdown due to escalating number of Covid-19 cases, CyberSecurity Malaysia issued a security best practices alert on 'Work From Home (WFH)' to organisational network system managers and Internet users. As part of our cybersecurity awareness initiatives, we also launched a series of online forums via YouTube from "Makcik Kiah Goes Digital" to "Makcik Kiah Goes Online...Kad Pak Salleh Pulak Decline," which was primarily to spread awareness on safe online purchase methods, procedures and transactions.

In the third quarter of 2020, CyberSecurity Malaysia organised several National Cyber Security Awareness Module (MKKSN) workshops throughout the country, together with the Education Resources and Technology Division (BSTP) of Ministry of Education Malaysia (MOE). These workshops enabled teachers, who were designated Head Coaches (JU), to study and evaluate MKKSN. Through the pilot implementation and feedback from workshop participants, CyberSecurity Malaysia managed to refine MKKSN's module contents, resolved potential technical problems as well as increased the level of cybersecurity awareness among school teachers throughout Malaysia.

I am pleased to report that CyberSecurity Malaysia has also reached out to Malaysia's Arm Forces. In September 2020, officers from Rejimen 502 Askar Wataniah Negeri Selangor attended a seminar presented by CyberSecurity Malaysia's Department of Strategic Studies and Advisory Services at Kem Sungai Buloh. The event enabled Malaysia's security forces to acquire more cybersecurity knowledge and further improve relationship between stakeholders in national security and defense.

In addition to cybersecurity awareness training, CyberSecurity Malaysia also embarked on Cyber Security Professionals development workshops including the Global ACE Certification Scheme. Such events provided the opportunity for joint-review between representatives of industry, academic, government and Professional Examination Committees (PEC) on the examination scope of ACE Global Certification program. A total of 22 Government agencies and Institutes of Higher Learning participated in the workshop.

Overall, our expertise and research-led approach is highly recognized in the industry as we were invited to speak at many cybersecurity events during 2020.

On the regional front, CyberSecurity Malaysia participated as presenter at the Android Mobile Malware Case Study virtual

seminar organised by Asia Pacific CERT (APCERT) and Pacific Cybersecurity Operational Network (PaCSON). The training program assisted the PaCSON community in developing expertise in mobile cyber security and malware analysis.

During 2020, CybeSecurity Malaysia continued to push for wider adoption of Malaysia Common Criteria (MyCC) in line with the Government's initiative to implement a recognized standard to procure Government Information Communication and Technology security product. MyCC is a systematic process for evaluating and certifying security functionality of ICT products based on the international standards ISO/IEC 15408, also known as Common Criteria (CC).

A MyCC Open Day was organised at Menara Cyber Axis in September 2020. Attended by over 90 participants from 49 organisations including representative from public and private sectors, the event was a major success in reinforcing the importance of adhering to cyber security standards. From the panel discussions, various cyber security needs and requirements from the industry as well as government agencies were brought to light.

CyberSecurity Malaysia also successfully organised a CyberSAFE awareness program in Perlis in October 2020. With the support of the Ministry of Communications and Multimedia Malaysia, a Cyber Parenting Seminar: 'Towards Digital Fluency' was held at the Institut Kemahiran MARA (IKM) Perlis. More than 200 participants from the local community as well as IKM staff and Maktab Rendah Sains MARA (MRSM) Beseri staff attended the event.

In addition, cybersecurity awareness programs were organised throughout the last quarter in 2020 involving government agencies, private organisations as well as educational institutions such as Malaysia Digital Economy Corporation (MDEC), Jabatan Pengangkutan Jalan (JPJ), multinational company BASF Malaysia and Universiti Terengganu Malaysia. These capacity building initiatives will continue to play an important role in ensuring our cyber security professionals are updated with the latest developments and best practices to counter cyber threats.

Looking ahead, cybersecurity will remain a dominant agenda as the world settles into a post-pandemic 'new normal'. Despite undergoing one of the most challenging years due to the impact of Covid-19, CyberSecurity Malaysia remains steadfast and resilient in our mission. Our expert teams from MyCERT to Cyber999 are constantly keeping watch over our cyber space and rendering assistance whenever possible.

As a cybersecurity expert agency, CyberSecurity Malaysia will continue to lead the development of a safer and more resilient cyber ecosystem in Malaysia in order to enhance national security, economic prosperity and social harmony.

Our success in 2020 would not have been possible without the hard work and dedication of everyone at CyberSecurity Malaysia. I would like to extend my appreciation and gratitude to all my colleagues for their continued support in the past year.

I look forward to another great year ahead!
Be Smart Be Safe. Together Towards Cyber Wellness.

MANAGEMENT COMMITTEE MEMBERS

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab
Chief Executive Officer (CEO)

Ts. Dr. Zahri Bin Yunos
Chief Operating Officer (COO)

Ts. Dr. Solahuddin Bin Shamsuddin
Chief Technology Officer (CTO)

Roshdi Bin Hj Ahmad
Senior Vice President,
Corporate Strategy and Industry Development Division

Ts. Dr. Maslina Binti Daud
Senior Vice President,
Cyber Security Proactive Services Division

Ts. Dr. Aswami Fadillah Bin Mohd Ariffin
Senior Vice President,
Cyber Security Responsive Services Division

Ts. Mohd Shamir Bin Hashim
Senior Vice President,
International & Government Engagement Division

Lt. Col. Mustaffa Bin Ahmad (Retired) CICSO *psc*
Senior Vice President,
Outreach and Capacity Building Division

Sazali Bin Sukardi
Senior Vice President,
Strategic Research Division

Jailany Bin Jaafar
Head, Legal & Secretarial/Company Secretary

REVIEW OF CORPORATE PERFORMANCE

2020 Ministry Performance Indicator

ITEM	TARGET	ACHIEVEMENT	% ACHIEVED
1 Increase the participation of Malaysia Cyber Security Industry Partners in Cyber Security Industry development	7	8	100%
2 Ensuring Cyber Security talent meets the Digital Economy needs	1,200	1,372	100%
3 Digital Forensics Case Resolution (Cyber CSI)	90%	90.16%	100%
4 Cyber Security Incident Resolution (Cyber999)	90%	92.34%	100%
5 International Cyber Security Standards (ISO/IEC I 5408 And ISO/IEC 27001) Compliance	33	55	100%

How We Performed Based on Corporate Key Performance Indicators (2020 KPI)

The following table are about the 2020 KPI – what were the indicators, and how we performed in relations to the targets.

KPI	Target	Achievement	%
SG 1 **Increase relevancy and visibility**			
1. # Visibility of program through events/programs	30	30	100
2. % Customer satisfaction Level	88	88.48	100
3. # Information security papers accepted for publication	20	29	100
4. % Corporate website accessable	100	100	100
SG 2 **Strengthen national holistic capabilities**			
5. # Trained knowledge workers	1,200	1,372	100
6. # New products / services / applications	3	4	100
SG 3 **Leading National Cyber Security Acculturation**			
7. # Outreach programs and activities	100	115	100
8. # Peoples reach out in Digital Economy community on Cyber Security Awareness Talk	17,000	30,588	100
SG 4 **Drive commercialization & industry development efforts**			
9. # Cybersecurity Collaboration Program for Cyber Security Industry Development	3	3	100
10. # Testing, accreditation, and certification	33	55	100
SG 5 **Enhance service delivery effectiveness and visibility of impact**			
11. % Digital Forensic Case Completed at CSM's end	90	90.16	100
12. % Cyber Incident Case Completed at CSM's end	90	92.34	100
13. % ISMS Compliance	90	95.57	100
SG 6 **Secure and Proficiently Administer Funds**			
14. $ Mil Net Profit for Operation	6 Mil	6.011 Mil	100
SG 7 **Enhance the Agility, Innovation and Leadership Development**			
15. # Award, Recognition & Certification	10	11	100
16. # Articles published	50	67	100
17. # Innovative Concept Implemented	2	3	100
SG 7 **Positive work culture & conducive environment**			
18. % Staff Integrity Awareness	80	99.37	100
19. % Employee Satisfaction Level	78	78	100

2020 Corporate KPI Achievement as of 31 December 2020 is: 100%

2020 CALENDER OF ACTIVITIES

JANUARY 2020

1


2

3

4

1. **9 January 2020** - Visit By Chairman Of Malaysian Communications And Multimedia Commission To CyberSecurity Malaysia
2. **9 January 2020** - Visit By Science & Technology Research Institute For Defence (STRIDE) To CyberSecurity Malaysia
3. **13 -17 January 2020** - CTO Tech Summit And Pursuing Business Meeting On The Development Of Bangladesh Center Of Excellence (COE), Dhaka, Bangladesh
4. **21 January 2020** - CTO Tech Summit And Pursuing Business Meeting On The Development Of Bangladesh Center Of Excellence (COE), Dhaka, Bangladesh

FEBRUARY 2020


5

6


7


8


9


10


11


12

5. **4 - 6 February 2020 -** Executive Technology Briefing And Leading Digital Strategy Workshop , Chiang Mai, Thailand
6. **17 February 2020 -** CCTV Work-Frame Meeting, London, United Kingdom
7. **11 February 2020 -** "Memupuk Fasih Digital Dalam Abad Ke-21" Forum In Conjunction Of Safer Internet Day 2020, Putrajaya21 January 2020
8. **12 - 21 February 2020 -** APT Training Course On Cybersecurity Technologies - "Recent Trend Of Risks And Countermeasures To Them", Tokyo, Japan
9. **18 February 2020 -** KSA Review Workshop, Cyberjaya
10. **19 February 2020 -** Knowledge Sharing On: "Getting Proactive About Assessing Your Cybersecurity Posture", Cyberjaya
11. **19 - 20 February 2020 -** Malaysian Army Unmanned Aerial System (UAS) Seminar, Wisma Perwira Kem Perdana Tentera Darat, Kuala Lumpur
12. **21 February 2020 -** CyberSAFE Security Awareness Talk (CSAT), Universiti Perguruan Sultan Idris, Tanjung Malim, Perak19 February 2020

13

14

13. **24 - 28 February 2020 -** RSA Conference 2020, Moscone Center, San Francisco, United States Of America
14. **29 February 2020 -** Malaysian Youth @ Safer Internet Day 2020, Universiti Malaya, Kuala Lumpur

MARCH 2020

15

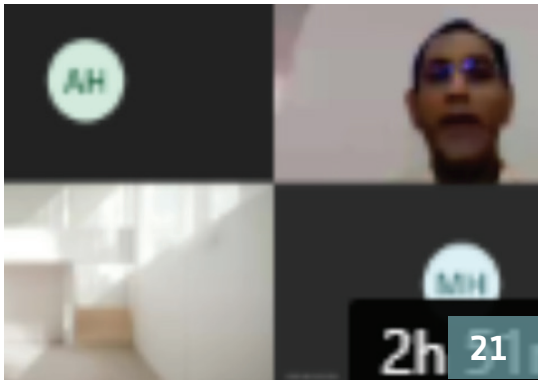
17

16

15. **4 March 2020 -** CyberSAFE Security Awareness Talk (CSAT), Perbadanan Menteri Besar Kelantan (PMBK), Kota Bharu, Kelantan
16. **12 March 2020 -** CyberSAFE Security Awareness Talk (CSAT), Universiti Malaysia Kelantan (UMK), Bachok, Kelantan
17. **16 - 17 March 2020 -** "CamMuka 2.0 Technical And Strategic Workshop, Universiti Malaysia Sabah (UMS), Sabah

18. 16 April 2020 - Bicara Siber PKP Covid-19 "When Makcik Kiah Goes Digital, YouTube Live

MAY 2020



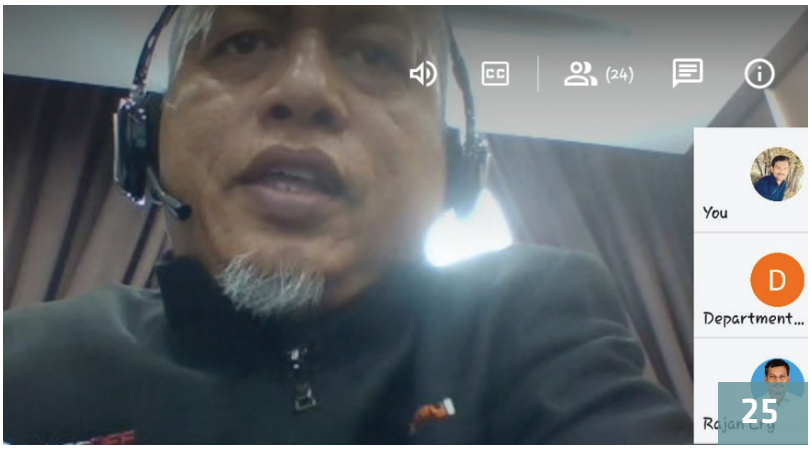
19. **5 May 2020 -** CWFH - Online Meeting Platform Security Demystified, YouTube Live
20. **15 May 2020 -** Online Forum: "Makcik Kiah Goes Online...Kad Pak Salleh Pulak Decline" - YouTube Live
21. **20 May 2020 -** "Cyber Security Awareness For All Users, Microsoft Team
22. **21 May 2020 -** Virtual Hand Over Ceremony: CyberSAFE Corporate Social Responsibility Program, GoTo Meeting

JUNE 2020

23. **16 June 2020 -** Working Visit By Department Of Personal Data Protection (JPDP), CyberSecurity Malaysia, Cyberjaya

24. **25 June 2020 -** Work From Home 2020, Online Forum

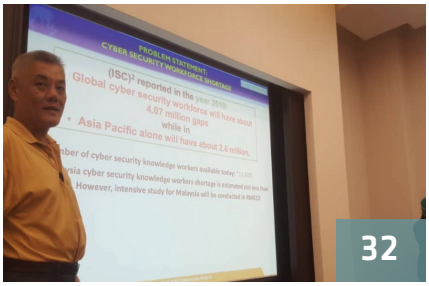
JULY 2020



25. **10 July 2020 -** Industry 5.0 Online Webinar

26. **13 - 24 July 2020 -** National Cyber Security Awareness Module Pilot Workshop (MKKSN) To Main Coaches (JU), Kelantan, Perak And Perlis

AUGUST 2020



27. **8 - 9 August 2020 -** National Occupational Skills And Standards (NOSS) In Digital Forensics For First Responder Development
28. **10 -14 August 2020 -** Global ACE Certification, Exam Review Workshop, Putrajaya
29. **10 - 28 August 2020 -** National Cyber Security Awareness Module Pilot Workshop (MKKSN) To Main Coaches (JU), Genting Highland, Putrajaya, Tawau, Melaka, Kuching, Dan Wilayah Persekutuan Labuan
30. **17 August 2020 -** A Day With Adjunct Professor Of The Faculty Of Computer Science And Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), Johor
31. **19 August 2020 -** Android Mobile Malware Case Study During COVID19 Lockdown Online Training
32. **22 - 23 August 2020 -** Digital Forensics For First Responder (DFFR) Occupational Standard Development Document Verification Workshop And Cyber Security Industry Occupational Framework Development, Putrajaya
33. **24 - 26 August 2020 -** Global ACE Certification: DFFR Item Construction Workshop, Putrajaya
34. **25 August 2020 -** Virtual Cloud Security Day, Online Webinar

SEPTEMBER 2020

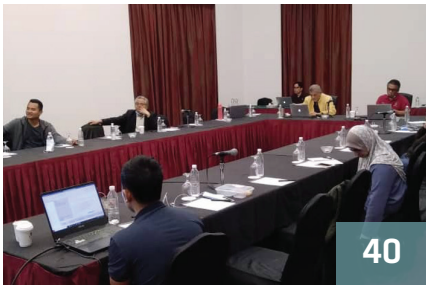

35


36

37


38


39

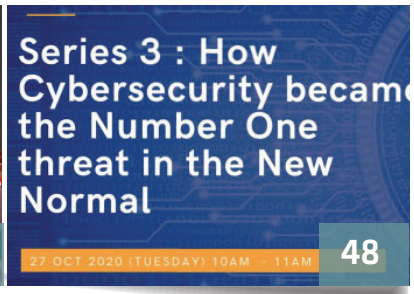

40

41

35. **2 September 2020** - Collaboration Meeting Between CyberSecurity Malaysia And Politeknik Mersing Johor (PMJ), Mersing, Johor, Mersing, Johor
36. **6 - 8 September 2020** - Cyber Security And Defense Seminar, Kem Sungai Buloh, Shah Alam, Selangor
37. **8 September 2020** - NeXGen SOC Launch Ceremony, Heitech Padu With CyberSecurity Malaysia And RSA Security, Cyber Axis Tower, Cyberjaya
38. **9 September 2020** - First Session Standard Evaluation Committee Meeting (JTPS1) For National Occupational Skills And Standards (NOSS) In Digital Forensics For First Responder, Putrajaya
39. **10 September 2020** - Occupational Framework Technical Security Committee Meeting, Putrajaya
40. **12 - 13 Septemberr 2020** - National Occupational Skills And Standards (NOSS) In Digital Forensics For First Responder Development Workshop, Putrajaya
41. **14 - 17 Septemberr 2020** - Cloud Computing Security Training, Cyber Axis Tower, Cyberjaya

42. **19 - 20 Septemberr 2020 -** Occupational Framework Development Workshop In The Cyber Security Field, Putrajaya
43. **22 Septemberr 2020 -** MYCC Open Day 2020 - Cyber Security Evaluation And Certification Services For The Digital Economy Era, Menara Cyber Axis, Cyberjaya
44. **22 Septemberr 2020 -** Workstream 14 (WS14) Cybersecurity Digital Economy Task Force (DETF) Meeting, Menara Cyber Axis, Cyberjaya
45. **29 Septemberr 2020 -** Asia Pacific Computer Emergency Response Team (APCERT) 2020 Annual General Meeting
46. **28 - 30 Septemberr 2020 -** Smart Card Reader Security Training, Cyber Axis Tower , Cyberjaya

OCTOBER 2020



47. **3 October 2020 -** Cyber Parenting Seminar – Towards Digital Fluency, Beseri, Perlis

48. **27 October 2020 -** How Cybersecurity Became The Number One Threats In The New Normal" Webinar Session, Cyberjaya

NOVEMBER 2020

49. **23 - 25 November 2020 -** The 12th Annual Conference Of The Organization Of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT), Cyberjaya

50. **25 November 2020 -** Global ACE Certification Webinar: "Certifying Cyber Security Professionals Towards The Industrial Revolution 4.0", Cyberjaya

51. **26 & 27 November 2020 -** Information Ceremony And Refresher Course For Cyber Security Penetration Testing & Assessment Advanced Diploma

DECEMBER 2020

52

53

52. **9 December 2020 -** 15th Annual Technical Conference For Global Csirt, Cyberjaya

53. **22 December 2020 -** Global ACE Certification Board Of Governance Meeting 1/2020, Cyberjaya

ACHIEVEMENTS & AWARDS 2020

12 September 2020

CyberSecurity Malaysia through Global ACE Certification selected as one of the Champion Project under Category 5: Building Confidence and Security in the USE of ICT at The World Summit on the Information Soceity (WSIS) Prize Award 2020

1 October 2020

CyberSecurity Malaysia has been reappointed as the Chair of the Asia Pacific Computer Emergency Response Team (APCERT). for rhe duration of 2020- 2021.

PROFESSIONAL CERTIFICATION

No	Name	Department	Certification
1	SARAH KHADIJAH TAYLOR	DF	CERTIFIED CRYPTOCURRENCY FORENSIC INVESTIGATOR (CCFI)
2	MOHD SHARIZUAN MOHD OMAR	DF	CERTIFIED CRYPTOCURRENCY FORENSIC INVESTIGATOR (CCFI)
3	MOHAMMAD HAZIM ZAHRI	DF	CERTIFIED CYBER INTELLIGENCE PROFESSIONAL (CCIP)
4	MUHAMMAD NOORAIMAN NOORASHID	DF	CERTIFIED CRYPTOCURRENCY FORENSIC INVESTIGATOR (CCFI)
5	NUR MOHAMMAD KAMIL MOHAMMAD ALTA	MyCERT	SANS GIAC FORENSICS EXAMINER CERTIFIED (GCFE)
6	MUHAMMAD NUR ARIF TOMIRAN	MyCERT	SANS GIAC CERTIFIED FORENSICS ANALYST (GCFA)
7	NURFAEZAH HANIS HALIM	ISMA	CQI AND IRCA CERTIFIED ISO/IEC 27001:2013 LEAD AUDITOR
8	ZUL AKMAL ABD MANAN	OCC	CERTIFIED DIGITAL MARKETING SPECIALIST (CDMS)
9	FAKHRUL AFIQ ABD AZIZ	DF	CERTIFIED DIGITAL MARKETING SPECIALIST (CDMS)
10	FAKHRUL AFIQ ABD AZIZ	DF	CERTIFIED VEHICLE SYSTEM FORENSICS EXAMINER
11	AFIQ ASRAF MOHD AZHAR	MyCERT	SANS GIAC CYBER THREAT INTELLIGENCE CERTIFIED (GCTI)
12	WAFA' BINTI MOHD KHARUDIN	DF	CERTIFIED DIGITAL FORENSICS FIRST RESPONDER (CDFFR)
13	NUR AFIFAH MOHD SAUPI	DF	CERTIFIED DIGITAL FORENSICS FIRST RESPONDER (CDFFR)
14	SHARIFAH NURUL ASYIKIN SYED ABDULLAH	DF	SANS GIAC CRITICAL CONTROLS CERTIFICATION (GCCC)
15	ADAM ZULKIFLI	ISMA	COMPTIA A+ CERTIFIED
16	MUHAMAD ZUHAIRI ABDULLAH	DF	COMPTIA SERVER+ CERTIFIED
17	FARIDATUL AKHMA ISHAK	CD	CERTIFIED BLOCKCHAIN PROFESSIONAL
18	SUHAIRI MOHD JAWI	CD	CERTIFIED BLOCKCHAIN PROFESSIONAL
19	ISMA NORSHAHILA MOHAMAD SHAH	CD	CERTIFIED BLOCKCHAIN PROFESSIONAL
20	NOR AZEALA MOHD YUSOF	CD	CERTIFIED BLOCKCHAIN PROFESSIONAL

TECHNICAL PAPERS AND JOURNALS

No	Paper Title	Journal/ Conference Proceeding	Date
1	Mobile Malware Classification for Social Media Application	Proceeding of International Conference on Cybersecurity	January 2020
2	Using Text Annotation Tool on Cyber Security News: A Review	Proceeding of the International Conference on Cybersecurity	January 2020
3	Method for Generating Test Data for Detecting SQL Injection Vulnerability in Web Application	7th International Conference on Cyber and IT Service Management	January 2020
4	Ransomware Entities Classification with Supervised Learning for Information Text	Proceeding of the International Conference on Cybersecurity	January 2020
5	Feature Extraction and Selection Method of Cyber Attacks and Threat Profiling in Cybersecurity Audit	Proceeding of the International Conference on Cybersecurity	January 2020
6	TAGraph Knowledge Graph of Threat Actor	Proceeding of the International Conference on Cybersecurity	January 2020
7	A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency	OIC-CERT Journal of Cyber Security Volume 2 Issue 1	February 2020
8	Cloud Forensic Challenges and Recommendations: A Review	OIC-CERT Journal of Cyber Security Volume 2 Issue 1	February 2020
9	Malware Discovery using Lebahnet Technology	OIC-CERT Journal of Cyber Security Volume 2 Issue 1	February 2020
10	OTPAF: A Security Requirement Conceptual Model of Cloud SAAS for Malaysian Government Based on Common Criteria	Proceeding of the International Conference of Electrical Engineering and Informatics	February 2020
11	Cloud Service Provider Security Readiness Model: The Malaysian Perspective	Proceeding of the International Conference of Electrical Engineering and Informatics	February 2020
12	An Attribution of Cyberattack using Association Rule Mining {ARM)	International Journal of Advanced Computer Science and Applications Volume11 No 2	March 2020
13	A Malware Detection Framework Based on Forensic and Unsupervised Machine Learning Methodologies	Proceedings of the 2020 9th International Conference on Software and Computer Applications	April 2020
14	Cryptojacking Classification Based on Machine Learning Algorithm	Proceeding of the 2020 8th International Conference on Communications and Broadband Networking	April 2020
15	The Capabilities that Terrorist Possess in the Digital Age	Proceeding of the Social Science Conferences 2020 Spring	May 2020
16	S-Box Construction Based on Linear Fractional Transformation and Permutation Function	Journal of Symmetry Volume 12 Issue 5	May 2020
17	Secure Information Hiding Based on Random Similar Bit Mapping	International Journal of Machine Learning and Computing	May 2020

18	Slid Pairs of the Fruit-80 Stream Cipher	International Journal of Communication Networks and Information Security (IJCNIS) Volume 12 Number 1	April 2020
19	Randomness Analysis on RECTANGLE Block Cipher	Proceedings of the 7th International Cryptology and Information Security Conference 2020	June 2020
20	Mitigating Insider Threats: A Case Study for Data Leakage Prevention	Proceeding of the 19th European Conference on Cyber Warfare and Security 2020	July 2020
21	OS Kernel Malware Detection through Data Characterization of Memory Analysis	Proceeding of the 19th European Conference on Cyber Warfare and Security 2020	July 2020
22	A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Dataset, Open Challenges and Recommendations	Journal of Applied Sciences Volume 10 Issue 15	July 2020
23	Fraudulent e-Commerce Website Detection Model Using HTML, Text and Image Features *⋆ Received Best Paper Award*	Proceedings of the 11th International Conference on Soft Computing and Pattern Recognition	August 2020
24	Malware Behavior Profiling from Unstructured Data	Proceedings of the 11th International Conference on Soft Computing and Pattern Recognition	August 2020
25	Findings Annihilator(s) via Fault Injection Analysis (FIA) on Boolean Function of LILI-128	Journal of Advances in Information Technology Volume 11 Number 4	November 2020
26	Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT	IEEE Access Volume 8	November 2020
27	Randomness Analysis on Lightweight Block Cipher, PRESENT	Journal of Computer Science	November 2020
28	Cloud Security Pre-Assessment Model for Cloud Service Provider Based on ISO/IEC 27017 : 2015 Additional Control	International Journal of Innovation and Industrial Revolution Volume 2 Issue 5	December2020
25	Secure Password Awareness by Using Educational Gamification	Proceeding of the 12th International Conference on Internet (ICONI 2020).	December2020

EDITORIAL TEAM

ADVISOR

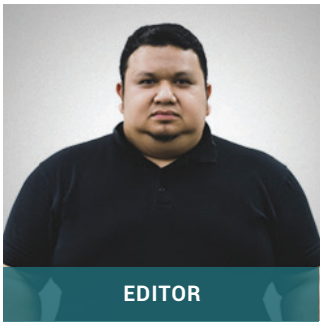
TS. DR. ZAHRI BIN YUNOS
Chief Operating Officer

REVIEWER

LT. COL. MUSTAFFA BIN AHMAD (RETIRED) CICSO *psc*
Senior Vice President

REVIEWER

MOHD SHAMIL BIN MOHD YUSOFF
Head of Department



EDITOR

ZUL AKMAL ABD MANAN
Executive

CONTENT CONTRIBUTOR

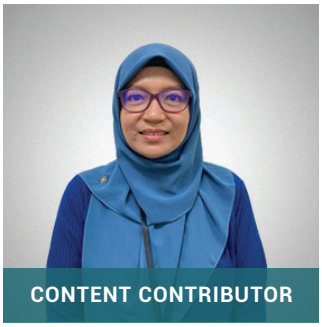
AZLIN BINTI SAMSUDIN
Senior Executive

CONTENT CONTRIBUTOR

NUR HASLAILY BINTI MOHD NASIR
Senior Executive

CONTENT CONTRIBUTOR

NUR ATHIRAH BINTI ABDULLAH
Executive



CONTENT CONTRIBUTOR

ERNIEZA BINTI ISMAIL
Senior Executive

CONTENT CONTRIBUTOR

MOHD ROHAIZAD BIN MOHD GHAZALI
Senior Executive

GRAPHIC DESIGNER

NURUL 'AIN BINTI ZAKARIAH
Executive

SOCIAL MEDIA

CyberSecurity MALAYSIA

@CyberSecurityMalaysia @cybersecurity_malaysia @cybersecuritymy @CyberSecurityMy

@cybersecurity-malaysia

MyCERT

Malaysia Computer Emergency Response Team

@mycert @mycert

CyberSAFE

@cybersafe malaysia @CyberSAFE Msia @CyberSAFEmy @CyberSAFE Msia

Corporate Office:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

Tel: +603 - 8800 7999
Fax: +603 - 8008 7000
Email: info@cybersecurity.my
www.cybersecurity.my

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA