MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

ANNUAL REPORT 2019

Securing Our Cyberspace

COVER RATIONALE

"Axis" as defined by Cambridge dictionary is a real or imaginary straight line going through the center of an object that is spinning, or a line that divides a symmetrical shape into two halves.

In this context, it reflects the function of CyberSecurity Malaysia as a pillar to provide optimum cybersecurity services towards safer and secure cyberspace. It also acts as a reference center for cybersecurity-related matters which will contribute to national sustainability, political stability, social well-being, economy and wealth creation.

Menara Cyber Axis or ***Cyber Axis Tower*** symbolizes CyberSecurity Malaysia's direction towards driving cybersecurity to the future as a hub in welcoming the industry for cybersecurity information, best practices, capacity building and awareness programmes.

CyberSecurity Malaysia Annual Report 2019 is inspired by the concept and definition of this building.

TABLE OF CONTENT

02 Introduction

About CyberSecurity Malaysia **05**
History **06**
Our Services **07**

15 Corporate Governance

Chairman's Statement **15**
Board of Directors **18**
Corporate Governance **20**
Notice of Annual General Meeting **24**
Form of Proxy **25**

27 Operation's Review

Foreword from CEO **27**
Management Committee Members **31**
Review of Corporate Performance **33**
2019 Calendar of Activities **36**
Achievements and Awards **50**
Professional Certifications **51**
Technical Papers and Journals **52**
Editorial Committee **54**
Social Media **55**

INTRODUCTION

05 About CyberSecurity Malaysia
06 History
07 Our Services

ABOUT CYBERSECURITY MALAYSIA

CyberSecurity Malaysia is the national cybersecurity specialist 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

MyCERT
Malaysia Computer Emergency Response Team

Cyber999

Cyber999 Help Centre

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.

www.mycert.org.my/cyber999

Cyber Threat Reseach Centre

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.

CMERP
Detection | Eradication | Remediation

Coordinated Malware Eradication & Remediation Platform

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.MY
CyberSecurity Honeynet Project

Lebahnet

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.

Digital Forensics (DF)

CyberCSI

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.

www.cybercsi.my

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

Information Security Management & Assurance (ISMA)

Information Security Management System (ISMS)

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

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.

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 Evaluation 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.

Malaysia Vulnerabilities Assessment Centre (MyVAC)

Vulnerability Assessment and 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

The Fourth Industry Revolution (IR4.0)

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

Information Security Certification Body (ISCB)

MyCC Scheme

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).

www.cybersecurity.my/mycc

CSM27001 Scheme

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.

csm27001.cybersecurity.my

Malaysia Trustmark

Malaysia Trustmark Certification is a service offered to organization for third-party validation to assess good e-commerce practices, legitimate business and secure web application. Malaysia Trustmark principles are guided by the World Trustmark Alliance (WTA) Code of Conduct.

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.

Cyber Security Professional Development (CSPD)

CyberGURU

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.

www.cyberguru.my

Global Accredited Cybersecurity Education (ACE) Scheme

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).

www.cybereducationscheme.org

Outreach & Corporate Communications (OCC)

CyberSAFE

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.

www.cybersafe.my

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.

CyberSecurity Industry Engagement and Collaboration (CIEC)

CyberSecurity Malaysia Collaboration Program (CCP)

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.

ccp.cybersecurity.my

Cyber Security Malaysia Awards, Conference and Exhibition (CSM-ACE)

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

www.csm-ace.my

My CyberSecurity Clinic (MyCSC)

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.

www.cybersecurityclinic.my

Government Engagement

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.

cnii.cybersecurity.my

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.

CORPORATE GOVERNANCE

15 Chairman's Statement
18 Board of Directors
20 Corporate Governance
24 Notice of Annual General Meeting
25 Form of Proxy

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

CHAIRMAN'S STATEMENT

Cybersecurity forms the critical backbone of successful digital transformation. As Malaysia pushes ahead to become a fully digitalized economy, cybersecurity will invariably become an integral part of our cyber ecosystem. In fact, our annual Cyber Security Malaysia – Awards, Conference & Exhibition (CSM-ACE) continues to make its mark as the region's premier cybersecurity event, drawing enthusiastic participation from local and regional cybersecurity professionals & experts. It has become a strategic platform to deliberate latest cybersecurity issues and leverage on the many technical training courses.

Over the years, CyberSecurity Malaysia's stature has grown in leaps and bounds. 2019 was no exception with several key milestones achieved. CyberSecurity Malaysia continues to play an important role in promoting and strengthening cybersecurity across government and industry sectors.

Cybersecurity forms the critical backbone of successful digital transformation. As Malaysia pushes ahead to become a fully digitalized economy, cybersecurity will invariably become an integral part of our cyber ecosystem. In fact, our annual Cyber Security Malaysia – Awards, Conference & Exhibition (CSM-ACE) continues to make its mark as the region's premier cybersecurity event, drawing enthusiastic participation from local and regional cybersecurity professionals & experts. It has become a strategic platform to deliberate latest cybersecurity issues and leverage on the many technical training courses.

The recently published 2019 (ISC2) Cybersecurity Workforce Study projected a severe shortage of cybersecurity professionals with some 4.07 million headcounts needed to defend organizations against cyber threats. Since our inaugural conference edition in 2009, CSM-ACE has collectively trained up to 1,049 cybersecurity professionals, thereby contributing significantly to Malaysia's capacity-building.

The 2019 Global Cybersecurity Index (GCI) ranked Malaysia 8th overall, which puts us in the same league as world's most developed nations. Each country was assessed based on five pillars of a nation's cybersecurity culture from legal, technical, organizational, capacity building to cooperation. I am pleased to report that the index also rated Malaysia as displaying high commitment which reflects the culture and determination in CyberSecurity Malaysia.

Cisco's 2019 Asia Pacific CISO (Chief Information Security Officer) Benchmark Study showed that Malaysia posted an improvement in the percentage of companies receiving more than 10,000 cyber alerts a day from 46 percent in 2018 to 43 percent in 2019. Be that as it may, there is still room for improvement.

On the regional front, CyberSecurity Malaysia continues to spread its wings through cross-border cooperation and global collaboration. We have

proactively reached out and expanded our regional linkages and efforts. CyberSecurity Malaysia was elected as deputy chair for Asia Pacific Computer Emergency Response Team (APCERT) in 2018 and subsequently in 2019, was named as chair for 2019-2020.

This is the second time CyberSecurity Malaysia has been bestowed APCERT chairmanship since 2002, underscoring the trust and confidence that the international cybersecurity community has on Malaysia's leadership in regional cybersecurity cooperation.

In May 2019, INTERPOL acknowledged CyberSecurity Malaysia's significant contribution in developing global guidelines for digital forensics. In the same year, CyberSecurity Malaysia's Cryptographic Evaluation Lab (MyCEL) gained acceptance into the National Voluntary Laboratory Accreditation Program (NVLAP) based in Maryland, USA to perform cryptographic module validation and testing, further cementing CyberSecurity Malaysia's capability and expertise in cutting-age cyber security technologies. MyCEL is the first lab in ASEAN, the fourth in Asia and among 22 laboratories in the world which has earned NVLAP accreditation under the Cryptographic and Security Testing program. Malaysia is only one of three countries in Asia to have attained such accreditation.

CyberSecurity Malaysia's cyber incidence and response specialists' team also attained first place in 'ASEAN Capture the Flag' competition in 2019, beating 10 other nations which took part in Australia. With these international accolades and sterling achievement, I am confident that CyberSecurity Malaysia will achieve one of our core missions of being recognised globally as a National Cyber Security Reference and Specialist Centre by 2020.

As Malaysia's national agency for monitoring and curbing cyber threats, Malaysia Computer Emergency Response Team (MyCERT) continues to helm Cyber999 Help Centre, providing 24/7 emergency response to the Malaysian public on cyber harassment, malware, intrusion, hack attempts and other information security breaches.

Over the past years, Internet users in Malaysia have also benefited from good cyber hygiene practices through multiple awareness campaigns organized by CyberSecurity Malaysia in conjunction with global annual 'Safer Internet Day' (SID). In 2019, CyberSecurity Malaysia successfully published a cyber parenting guidebook 'CyberSAFE Parenting: Ke Arah Kesejahteraan Siber' in collaboration with Universiti Malaya (UM), Universiti Kebangsaan Malaysia (UKM) and DiGi Telecommunications. The event was graced by Kebawah Duli Yang Maha Mulia Raja Permaisuri Agong, Tunku Hajah Azizah Aminah Maimunah Iskandariah Binti Almarhum Al-Mutawakkil Alallah Sultan Iskandar Al-Haj on 20 November 2019. The guidebook provides essential resources to help parents educate and monitor children's online activities.

Through our long-standing CyberSAFE initiatives, CyberSecurity Malaysia collaborates with private sector companies to impart practical knowledge on cyber safety and provide resources such as captivating infographics to a wide spectrum of the community. The annual National ICT Security Discourse (NICTSeD) CyberSAFE challenge trophy has become a hallmark discourse competition for secondary school students nationwide which will help nurture cyber knowledge and resilience among Malaysia's youth.

As the world becomes more digitized, cybersecurity must be oriented towards addressing people, process and technology. Everyone has a role to play in strengthening our cybersecurity and resilience.

Going forward, CyberSecurity Malaysia will continue to fortify Malaysia's cybersecurity ecosystem with strategic initiatives from public-private sector collaboration, as well as greater regional cooperation and support for capacity building.

I look forward to another great year ahead!

Thank you.

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)

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

Datuk Dr. Abdul Rahman bin Saad
- *Founder of ARSA LAWYERS (Messrs Abdul Rahman Saad & Associates) and has been its Managing Partner since 1979*
- *Director, CyberSecurity Malaysia*
- *Chairman Audit Governance & Integrity Committee CyberSecurity Malaysia*

Dato' Dr. Suhazimah binti Dzazali
- *Deputy Director General (ICT), Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)*
- *Director, CyberSecurity Malaysia*

** Member Human Resource & Remuneration Committee*
(resigned w.e.f 28 July 2020)

Puan Azizatul Yusna binti Ahmed Yusuff
- *Head Section, Public Asset Management Division, Ministry of Finance*
- *Director, CyberSecurity Malaysia*

**Member Audit, Governance & Integrity Committee
(resigned w.e.f 1 June 2020)

Haji Suip bin Saniman
- *Director, CyberSecurity Malaysia*

****Chairman Human Resource & Remuneration Committee*
****Member Audit, Governance & Integrity Committee*
(end of term 30 June 2019)

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 overall terms and conditions of employment for the Company remain competitive within the local market in order to attract and retain the right talent; and
- 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
2. Puan Azizatul Yusna Binti Ahmed Yusuff

iv. 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.

2. Audit, Governance and Integrity Committee (AGI)

i. Audit Duties:

- 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 Duties:

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

iv. 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.

v. 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.

The board is fully and effectively assisted in the day- to-day management of CyberSecurity Malaysia by the Chief Executive Officer (CEO) and his management team. The profiles of the current members of the boards are set out on pages of the annual report.

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 14th Annual General Meeting of CYBERSECURITY MALAYSIA ("Company") will be held at CyberSecurity Malaysia, Conference Room Jati, Level 10, Tower 1 Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, on or before Thursday, 24 September 2020 at 12.00 a.m. to transact the following businesses:

AS ORDINARY BUSINESS

1.	To receive the Audited Financial Statements for the financial year ended 31 December 2019 together with the Reports of the Directors and Auditors thereon;	Resolution 1
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 forthcoming AGM until the next AGM of the Company;	Resolution 2
3.	To re-elect the following retiring Directors of the Company for a term of two (2) years pursuant to Article 52 of the Company's Constitution and being eligible, offer themselves for re-election; 3.1 Y.A.Bhg. General Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired); 3.2 Y.A.Bhg. Datuk Dr. Abdul Rahman bin Saad	Resolution 3
4.	To elect Y.Brs. Encik Mohd Sori bin Husain as Director who is retiring pursuant to Article 54 of the Company's Constitution;	Resolution 4
5.	To appoint Messrs Jamal, Amin & Partners as External Auditors of the Company for the financial year ended 31 December 2020 and to authorise the Directors to fix their remuneration	Resolution 5

AS OTHER BUSINESS

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

BY ORDER OF THE BOARD

JAILANY BIN JAAFAR (LS0008843)
Company Secretary

Selangor Darul Ehsan
Date : 3 September 2020

NOTES:

i. 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.

ii. 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 appointmnet of the corporate representative.

iii. 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.

iv. 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 24 September 2020 at 12.00 noon at any adjournment hereof.

Signed this .....day of 2020

(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.

OPERATION'S REVIEW

27 Foreword from CEO
31 Management Committee Members
33 Review of Corporate Performance
36 2019 Calender of Activities
50 Achievements & Awards
51 Professional Certifications
52 Technical Papers and Journals

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

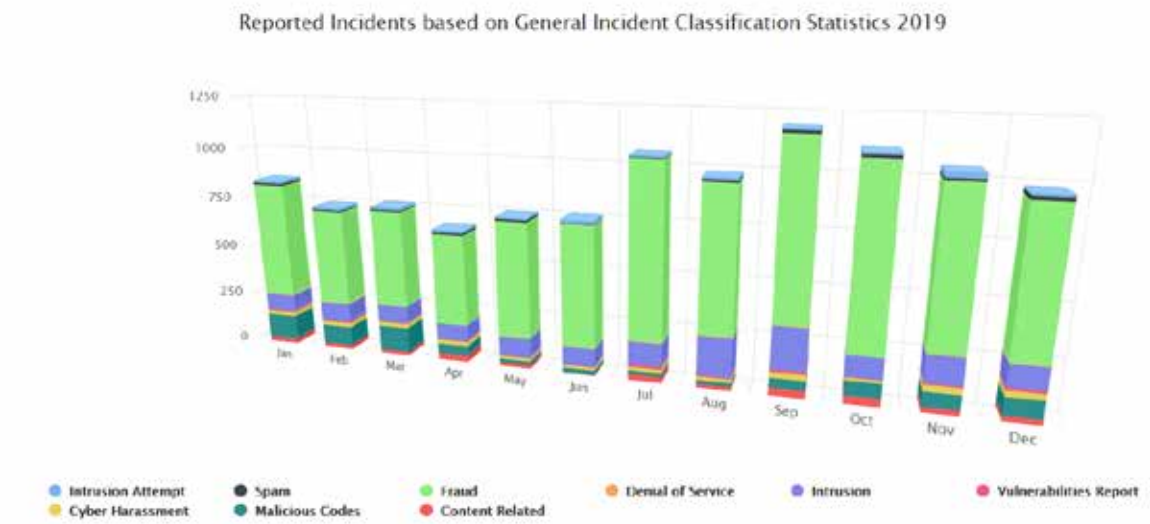
FOREWORD FROM CEO

It is my pleasure to present CyberSecurity Malaysia Annual Report 2019.

The rapid expansion of data-driven technologies from convergence of web, cloud, mobile to Internet of Things (IoT) has made cyber risk management imperative to organizations today. As business operations become ever more reliant on networked systems, the attack surface area for cybercriminals and frequency of cybersecurity incidents will also increase.

With cybercrimes rising exponentially in scale and complexity, CyberSecurity Malaysia remains steadfastly committed to helping government and industries anticipate cyber threats, absorb their impact, as well as react quickly and resolutely to ensure that key systems and processes continue to operate.

In 2019, a total of 10,772 cyber incidents were reported to Cyber999, CyberSecurity Malaysia's Cyber999 help centre. CyberSecurity Malaysia responded swiftly to malicious cyber threats during 2019. This includes taking a proactive role in helping organizations deal with cyber threats by issuing up-to-date advisories, best practices, and guidelines on the latest threat trends.



The top five highest incidents reported in order of frequency were online fraud, intrusion, malicious code, content-related and cyber harassment. In fact, most fraud cases involved job scams, love scams, spear-phishing emails, or social engineering tactics to deceive victims and obtain sensitive information from them. For intrusion cases, hacking or data breach attempts were most prevalent, while cyberstalking accounted for the bulk of cyber harassment incidents reported.

During 2019, CyberSecurity Malaysia has made significant strides in coordinating and strengthening our cyber security efforts. One of the key initiatives include establishment of CyberDEF (Detect, Eradicate and Forensic) service. CyberDEF service identifies holistic solutions for cyber-attacks incident such as cyber intrusion, APT malware, and ransomware by detecting threat, eradicate source and conduct forensic investigation to outline potential cause.

Our digital forensic lab, the first such facility in the Asia-Pacific region, has also successfully attained accreditation from the ANSI-ASQ National Accreditation Board (ANAB). We have the distinction of being the first and only one in the region to have done so. CyberSecurity Malaysia's digital forensic analysis has since been utilized to assist law enforcement agencies, regulatory bodies, and government agencies in criminal investigations related to digital evidence.

One of the solutions developed entirely using CyberSecurity Malaysia resources was the 2D & 3D biometric facial forensics system which deploys machine learning and deep learning algorithms. CamMuka system can identify suspect's faces from video or still-photo evidence even with only fragments or partial of the captured face from CCTV footage and facial recognition analysis used as evidence in criminal investigations case.

A portfolio of national trusted cryptographic algorithms, MySEAL - National Trusted Cryptographic Algorithm List (Senarai Algoritma Kriptografi Terpercaya Negara) has been set up to provide a list of cryptographic algorithms suitable

for implementation within Malaysian context that supports National Cryptography Policy (NCP). While NCP serves as a guideline for Malaysia to achieve cryptographic sovereignty, MySEAL will support in the scientific areas of cryptography and cryptanalysis. MySEAL is a major milestone for Malaysia. It will attest Malaysia's perseverance and stamina in protecting her information infrastructure at the cryptographic algorithm level.

In September 2019, CyberSecurity Malaysia once again successfully organized the 11th Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE). CSM-ACE 2019 was attended by over 5,000 cyber security professionals, industry leaders, tech investors, academia, and government officials from Malaysia and across the region. Aside from a conference with keynote and panellist session, 12 capacity building and trainings programs as well an ICT exhibition were staged showcasing over 50 exhibitors on ICT products and services. A two-day career fair featured 1,000 career opportunities offered by 20 cyber security companies from the private sector and 16 institutions of higher learning.

The 7th edition of National ICT Security Discourse – CyberSAFE Challenge Trophy (NICTSeD) 2019, co-organized with the Ministry of Education and supported by DiGi Telecommunications and BAE Systems, attracted strong participation from 142 schools nationwide. In the grand finals, Sekolah Menengah Kebangsaan Sultan Abu Bakar, Kuantan, Pahang emerged victorious after impressing a panel of distinguished judges with their eloquent discourse and well-delivered key points.

Another public-private collaboration driven by CyberSecurity Malaysia which successfully went into commercialization in 2019 was Coordinated Malware Eradication & Remediation Platform (CMERP). CMERP provides a comprehensive malware detection, quarantine and removal solution that safeguards Malaysian Cyberspace. It is expected to significantly reduce the impact of malware threats for organizations, which include in the critical national information infrastructure (CNII) sectors.

Of course, we have also embarked on new initiatives while sharpening our focus on existing core programmes. As part of the Cyber Security Capacity Building Framework, CyberSecurity Malaysia continues to execute programmes targeting three distinct audience groups. CyberSAFE programme is aimed at educating communities and individuals in cyber safety, while CyberGURU caters for cybersecurity practitioners. CyberSecurity Malaysia through the establishment of Global Accredited Cybersecurity Education (ACE) Certification scheme, aims to enhance the skill sets of cybersecurity professionals. The scheme is developed via strategic collaboration with the government, academia, and industries congruent with local and regional requirements, embedding universal values, rules-based, open, and non-discriminatory practices via peer-reviewed curriculum.

As Malaysia's digital economy continues to grow at a remarkable pace, CyberSecurity Malaysia aims to create more strategic public-private partnerships and industry collaborations to spur product innovation and strengthen our cyber security efforts. It is our mission to develop a vibrant and resilient cyber eco-system.

I am proud to report the establishment of a world-class regional cyber security Transparency Centre by Kaspersky in Malaysia during 2019, the first such centre in Asia Pacific. The Transparency Centre, hosted at CyberSecurity Malaysia's headquarters in Cyberjaya, serves as a trusted facility for the company's partners and government stakeholders to verify the source code including threat analysis, secure review, and the application security testing process.

In Q3 2019, CyberSecurity Malaysia also entered a MoU with local telecommunications giant Celcom Axiata to collaborate on a strategic partnership to explore cybersecurity solutions for various industry verticals. The MoU paved the way for CyberSecurity Malaysia to assist Celcom in establishing its security test lab, enhancing development of resource, capability, and capacity in security testing.

On the technical front, CyberSecurity Malaysia demonstrated its thought leadership by participating in various cyber security technical dialogues and discussions on the global stage. Key events include International Common Criteria Conference (ICCC) 2019 in United States of America, the Common Criteria Recognition Arrangement (CCRA) in Italy, International Telecommunication Union (ITU) in Geneva, Switzerland as well as the 11th OIC CERT Annual Conference in Muscat, Oman.

MyCERT and digital forensics team were also invited to the 4th Digital Forensic Specialist Group meeting in Brazil; ASEAN-Japan Cybersecurity Capacity Building Center's Training, Thailand; 3rd International Conference on Information Security (INFOFORUM), Russia; and 31st Annual First Conference on Computer Security Incident Handling in Scotland.

CyberSecurity Malaysia also successfully organized Cybersecurity Modular Professional Certification and Cybersecurity Awareness & Knowledge Systemic High-level Application (YAKSHA) User Conference in Putrajaya which attracted 108 participants from 21 organizations

and agencies. The conference fostered closer cooperation and established a strategic network between Malaysia and European Union (EU) country members to raise cyber readiness and reduce cyber risks.

In December 2019, CyberSecurity Malaysia through the Malaysia Computer Emergency Response Team (MyCERT) had also participated in the International Cyber Shield 2019 held at the Information and Communications Technologies Authority (ICTA) headquarters in Ankara, Turkey. As a wrap up to 2019, CyberSecurity Malaysia attended the Annual Coordination Meeting of the OIC Institutions (ACMOI) 2019 held at the Organization of the Islamic Cooperation (OIC) headquarters in Jeddah, Saudi Arabia.

CyberSecurity Malaysia has certainly made significant progress towards creating a secure and resilient cyberspace. It is critical that we continue to build on this momentum in the areas of capacity building, regional cooperation, and international discussions on cyber defence.

I would like to thank the Board of Directors of CyberSecurity Malaysia for their invaluable guidance and support throughout the past year. My sincere gratitude goes to our loyal management team and employees for their unrelenting commitment, hard work and dedication to the organization.

Going forward, CyberSecurity Malaysia will continue to engage different stakeholders to raise awareness of cyber threats and strengthen security efforts collectively so that we can create a secure, trusted, and resilient cyberspace for all.

I wish you all the best for 2020. Thank you.

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

MANAGEMENT COMMITTEE MEMBERS

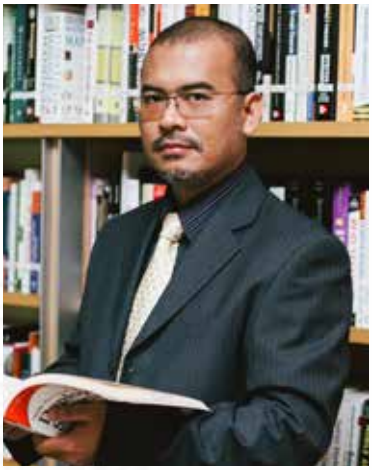
Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab
Chief Executive Officer (CEO)

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)
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

2019 Ministry Performance Indicator

ITEM	SASARAN	PENCAPAIAN	% ACHIEVED
1 Increase the participation of Malaysia Cyber Security Industry Partners	6	6	100%
2 Increase target group engagement in human capital development programmes	1,100	1,355	123%
3 Digital Forensics Case Resolution (Cyber CSI)	75%	85.20%	114%
4 Cyber Security Incident Resolution (Cyber999)	88%	93.14%	106%
5 International Cyber Security Standards (ISO/IEC 15408 And ISO/IEC 27001) Compliance	33%	47%	142%

How We Performed Based on
Corporate Key Performance Indicators (2019 KPI)

The following table are about the 2019 KPI – what were the indicators, and how we performed in relations to the targets.

KPI	Achievement
SG 1 Increase relevancy and visibility	
■ Recognition from 5 International and Local Organization	Recognition from 5 International Organizations: 1. Kepakaran cybersecurity Malaysia dalam bidang forensik digital diiktiraf INTERPOL (26 May 2019) 2. Overall Champion : Asean Capture the Flag (CTF) competition (27 Jun 2019) 3. Malaysia elected as APCERT chair for 2019-2020 (3 October 2019) and Malaysia elected as APCERT Steering Committee (SC) for 2019-2020 (3 October 2019) 4. Appointed as local host to conduct YAKSHA (Cybersecurity Awareness and Knowledge Systemic High-level Application) End User 2019 event (26 – 28 November 2019) 5. CyberSecurity Malaysia Cryptographic Evaluation Lab (MyCEL) successfully accredited and this is the first lab in ASEAN region, and fourth in Asia (30 July 2019)
■ Anchor 3 local and international co-branding programs	Anchored 8 local and interational co-branding program: 1. Safer Internet Day (SID) 2019 (13 Feb 2019) - Organizer 2. Cyber Heroes Competition 2019 (6 Mar 2019) - Organizer 3. "Youth Cyber Wellness in the Digital Era" Seminar & Safer Internet Day 2019 (7 Mar 2019) - Organizer 4. Cyber Security Malaysia – Award, Conference & Exhibition 2019 (CSM-ACE 2019) (23-27 Sept 2019) - Organizer 5. Cyber Forensics Colloquium (25 Sept 2019) - Organizer 6. Malaysian Technical Cooperation Programme (24 Sept 2019) - Organizer 7. National ICT Security Discourse (NICTSeD) CyberSAFE Challenge Trophy 2019 (25 Sept 2019) - Organizer 8. Cyber Security Malaysia Job Fair 2019 (24-25 Sept 2019) - Organizer
SG 2 Strengthen national holistic capabilities	
■ 3 new products/ services	5 new products/services 1. Penetration Tester Service Provider (PTSP) Scheme 2. CyberSKRIN 3. CariMUKA 4. CMERP 5. ISO 22301 (BCMS)
■ 1,200 trained knowledge workers	1,355 trained knowledge workers
■ 2 strategic facilitation / intervention of development on policy / strategy / framework	5 strategic facilitation / intervention of development on policy / strategy / framework through: 1. Pelan Strategik Jangka Panjang, KKMM 2. National Artificial Intelligence Framework, MDEC 3. Inter Agencies Planning Group for Digital Economy (Digital Industry, Digital Instructure, Digital Inclusion), under KKMM 4. Defend white paper 5. Inter Agencies Planning Group for Public Safety under KDN

SG 3 Leading National Cyber Security Acculturation	
■ 80 CyberSAFE Program and activities via radio, tv and awareness talk	219 CyberSAFE Program and activities via radio, tv and awareness talk
■ 50 schools involved in pilot project for Modul Kesedaran Keselamatan Siber Nasional (MKKSN)	62 schools involved in pilot project for Modul Kesedaran Keselamatan Siber Nasional (MKKSN)
SG 4 Drive commercialization & industry development efforts	
■ 1 new program under Cybersecurity Collaboration Program (CCP)	2 new program under Cybersecurity Collaboration Program (CCP) conducted: 1. Program Kolaborasi • Pelancaran Program Kolaborasi CyberSecurity Malaysia atay CyberSecurity Malaysia Collaboration Program (CCP) (23 April 2019) 2. Program 'Knowledge Sharing' • Seminar Perbincangan Data-Driven Cyber Security bersama industri (17 Jun 2019) • Seminar Perbincangan 'Staying on top of Cyber Security Exclusive Seminar' bersama rakan industri (9 Julai 2019) • Perkongsian ilmi 'Rnabling Secure IT Transformation to the Cloud' bersama rakan industri (18 Julai 2019) • Dialog Industri Keselamatan Siber (23 April 2019)
■ 4 ICT products in evaluation for CCRA certification	6 ICT products in evaluation for CCRA certification: 1. DSonic eID - Datasonic Smart Solution Sdn Bhd 2. CYSECA Endpoint Application Control - Pernec Integrated Network Systems Sdn Bhd 3. Amaris Data Diode - Advance Product Design Sdn Bhd 4. MyDigital ID v1.0 - MIMOS Berhad 5. Mi- Signet - MIMOS Berhad 6. Durio Unified Threat Management (UTM) v3.2.4 - Open Kod Sdn Bhd
SG 5 Enhance service delivery effectiveness and visibility of impact	
■ 85% Cyber Security Resolution	95% cyber security resolution: Total caces received - 11,107 Total cases resolved - 10,561
■ 80% Customer satisfaction	88% customer satisfaction
■ 85% ISMS compliance	95% ISMS compliance
SG 6 Secure and Proficiently Administer Funds	
■ Strategic Business Unit secured 6 Million of net profit	Secured RM6.14 Million of net profit
SG 7 Enhance the Agility, Innovation and Leadership Development	
■ 5 staff received local/international recognition	8 staff received local/international recognition
■ Review of 5 years existing HR program	5 years existing HR program has been reviewed and endorsed
■ 14 information security papers published in journals	23 information security papers published in journals
■ 30 articles in E-Security Bulletin	68 articles published
SG 8 Positive work culture & conducive environment	
■ 75% Employee Engagement Satisfaction Survey	74.1% Employee Engagement Satisfaction Survey Result

2019 Corporate KPI Achievement as of 31 December 2019 is: 93% or 4.72/5

2019 CALENDER OF ACTIVITIES

8 – 12 January 2019

International Bhurban Conference On Applied Sciences & Technology (IBCAST) 2019, Islamabad, Pakistan

17 January 2019

CSM-ACE 2019 Coordination Workshop, Selangor, Malaysia

18 – 20 January 2019

3rd Pre-Phase New Cryptography Algorithm Assessment Workshop (AKBA) For National Cryptography Algorithm List (MySEAL), Port Dickson, Negeri Sembilan

18 - 21 January 2019

YAKSHA (Cybersecurity Awareness and Knowledge Systemic High-Level Application) Project Review Meeting and Workshop, Brussels, Belgium

Memorandum of Understanding Signing Ceremony between Malaysia CyberSecurity and Kedah Skills Industrial & Management Development Centre (KISMEC), Alor Star, Kedah

24 January 2019

Research presentation at The Third International Conference on Smart Trends for Information Technology and Computer Communications (SmartCom 2019) Bangkok, Thailand.

24 - 25 January 2019

Global ACE Scheme Workshop between CyberSecurity Malaysia and DRB-HICOM University (DHU)

11 February 2019

ASEAN Fact-Checking Capacity Building Workshop, Singapore

11 - 12 February 2019

12 - 13 February 2019

Global ACE Scheme Workshop between CyberSecurity Malaysia and Politeknik Mersing, Johor

13 February 2019

Safer Internet Day (SID) 2019 Launching Ceremony, Putrajaya

13 February 2019

The Cloud Platform E-Learning Presentation: Cybersecurity Challenges, Universiti Tun Hussien Onn Malaysia (UTHM)

17 - 18 February 2019

UMT Industry Training Carnival and PITA (KLIP) 2019, Universiti Malaysia Terengganu, Kuala Terengganu.

Defence Practice Against Cyber Security Training, Tokyo, Japan

17 February - 2 Mac 2019

Malaysia Urban Forum (MUF) 2019, Kuala Lumpur Convention Center

18 - 19 February 2019

Asia Pacific Internet Conference on Operational Technologies (APRICOT) & FIRST Technical Colloquium Daejeon, Korea

18 February 2019

ISO 22301 BCMS Certificate Presentation Ceremony, Tun Dr. Ismail (DTI)'s Hall, Nuclear Agency Malaysia

19 February 2019

20 February 2019

ICORS Round Table Discussion "The Ethics of Artificial Intelligence", Dewan Besar Ikim, Kuala Lumpur

24 February 2019

Asia Pacific Computer Emergency Response Team (APCERT) Steering Committee Meeting 2 / 2019 , Deajeon Convention Center, Korea

25 February 2019

Signing Ceremony of The Collaboration Agreement with Onwards Security, New Taipei City, Taiwan

26 - 28 February 2019

7th Annual Cyber Intelligence Asia Conference and Exhibition Bangkok, Thailand

MBI Synergies Forum, Saujana Hotel, Kuala Lumpur

28 February 2019

Signing Ceremony of Collaboration Certificate with Politeknik Mersing, Johor

2 March 2019

RSA International Cyber Security Forum (ICSF) 2019, Intercontinental Hotel, San Francisco, United State of America (USA)

4 - 8 March 2019

Cyber Heroes Competition 2019, Asia Pacific University, Bukit Jalil

6 March 2019

7 March 2019

"Youth Cyber Wellness in the Digital Era" Seminar & Safer Internet Day 2019 - Malaysia Edition Closing Ceremony, Putrajaya

18 - 19 March 2019

CyberSecurity Malaysia (CSM) - Universiti Malaysia Terengganu (UMT) Cloud Technology Security& Industry 4.0 Collaboration Workshop CyberSecurity Malaysia (CSM) - Universiti Malaysia Terengganu (UMT), Zenith Hotel, Putrajaya

25 - 30 March 2019

Critical Infrastructure Protection Forum CIP Forum IV 2019 Romanian Parliament Palace, Bucharest, Romania

28 March 2019

Cyber Security Awareness Seminar - Combating and How to Respond to Cyber Threat, Ipoh, Perak

IPQUORUM 2019, Kaliningrad, Russia

5 - 12 April 2019

Common Criteria Recognition Arrangement (CCRA) Meetings, Rome, Italy

8 - 11 April 2019

2019 – 2020, Ministry of Communication And multimedia (KKMM) Cyber Security Service Requirement Projection Workshop KKMM, Le Meridien IOI City Mall, Putrajaya.

9 April 2019

Brunei Darussalam Ministry of Transportation and Info Communication visit to CyberSecurity Malaysia

12 April 2019

23 April 2019

OIC-CERT Board Face2face Meeting, Cyberjaya

23 April 2019

Cyber Security Industry Dialogue 2019, Menara Cyber Axis, Cyberjaya.

23 April 2019

Cybersecurity Malaysia Collaboration Programme (CCP) Launching Ceremony, Cyberjaya

24 April 2019

Week Without Wall: Uncovering the Truth Beyond Digital Imagination, UiTM, Malacca, Jasin Campus.

Kembara Amal CyberSAFE 2019, Ipoh, Perak.

18 May 2019

4th Digital Forensics Expert Group Meeting, Sao Paolo, Brazil

22 - 24 May 2019

Visit of Personal Data Protection Department (JPDP) to CyberSecurity Malaysia, Cyberjaya

27 May 2019

ISO/IEC TC 307 Blockchain And Distributed Ledger Technology; 5th Plenary Meeting, Dublin, Ireland

27 -31 May 2019

28 - 31 May 2019

AUSCERT 2019 Cyber Security Conference, Gold Coast, Australia

10 - 12 June 2019

3rd International Conference on Information Security (INFOFORUM), Ugra, Rusia

17 June 2019

Data-Driven Cybersecurity Roundtable Discussion, Cyberjaya

1 July 2019

Memorandum Of Understanding Signing Ceremony And Meeting "Global ACE Scheme" Between CyberSecurity Malaysia And Universiti Teknologi Petronas (UTP), Tronoh, Perak

Security APISC Safety Training Course 2019, Seoul, Korea

7 - 14 July 2019

Asean Course - Japan Cybersecurity Capacity Building Centre (AJCCBC), Bangkok, Thailand

8 - 12 July 2019

Workshop On Developing Guideline On The Usage And Implementation Of Cryptography Algorithm AKSA MySEAL, Cyberjaya

9 July 2019

International Conference On Electrical Engineering And Informatics (ICEEI 2019), Bandung, Indonesia

9 - 10 July 2019

9 - 12 July 2019

SEACEN-CPMI Course On Technology And Emerging Risks In Payment And SEACEN-CPMI Conference Of Directors , Payment And Settlement System , Udaipur India

9 July 2019

"Staying On Top Of Cyber Security Exclusive" Seminar, Cyberjaya

11 July 2019

KSA Descriptor 3.0 Workshop-Pathway Towards Technical & Vocational Education Training (TVET) Excellence With Professional Certification, Menara Cyber Axis, Cyberjaya

11 July 2019

Visit By The Director Of Personal Data Protection Department To CyberSecurity Malaysia, Cyberjaya

Global ACE Scheme Workshop Collaboration Between Cybersecurity Malaysia And DRB-HICOM University, Cyberjaya

12 July 2019

National ICT Security Discourse (NICTSeD) 2019, Kuantan, Pahang

12 - 18 July 2019

2019 RSA Conference, Asia Pacific & Japan, Singapore

15 - 18 July 2019

Opengov Leadership 2019 Indonesia Conference In Jakarta, Indonesia.

18 July 2019

18 July 2019

Knowledge Sharing On "Enabling Secure It Transformation To The Cloud" Cyberjaya

19 - 20 July 2019

6th Global Conference Of Engineering And Technology (6th GCOET), Male, Maldives

19 July 2019

Cyber Awareness Talk On Social Media Usage Among Students, Kuantan, Pahang

19 July 2019

Bank Islam Mega Conference, Putrajaya

Strategic Visit By Myung Information Technologies Co. Ltd. And Myung Infotech (M) Sdn Bhd To CyberSecurity Malaysia And Meeting On Direction Of MyCyberSecurity Clinic (MyCSC), Cyberjaya

23 July 2019

Visit By Secretary-General Of Ministry Of Communication And Multimedia Malaysia To CyberSecurity Malaysia, Cyberjaya

23 July 2019

"CyberSecurity Awareness And Knowledge Systematic High Level Application" (YAKSHA) Ambassador Day, Cyberjaya

29 July 2019

Global ACE Scheme Collaboration Meeting Between CyberSecurity Malaysia And Politeknik Mersing Johor (PMJ) Mersing, Johor

1 - 2 August 2019

2 August 2019

Guideline For Securing MyKad EBA Ecosystem Workshop, Putrajaya

6 August 2019

MYCC Open Day 2019, Menara Cyber Axis, Cyberjaya

14 - 16 August 2019

2nd Southeast Asia Cryptocurrencies Working Group Meeting, Singapore

16 - 17 August 2019

APEC Workshop On Facilitating Trade Through Adherence To Globally-Recognized Cybersecurity Standards And Best Practices, Puerto Varas, Chile

Industrial Control System (ICS) Security Training, Lexis Suites, Pulau Pinang

19 - 21 August 2019

Course On Information And Communication Technology (ICT) Risks, Including Cyber Risks In Banks, Hanoi, Vietnam

29 - 30 August 2019

Industrial Control System (ICS) Security Guidelines Refinement Workshop, Cyberview Resort & Spa, Cyberjaya

29 August 2019

ASEAN-Japan Cybersecurity Capacity Building Center Training (AJCCBC) Training, Bangkok, Thailand

9 - 13 September 2019

17 - 20 September 2019

11th Asian Forensic Sciences Network (AFSN) Annual Meeting And Symposium, Ho Chi Minh City, Vietnam

17 - 26 September 2019

Certified Cyber Defender Associate" Malaysian Technical Cooperation Programme (MTCP) Technical Training, Sunway Putra Hotel Kuala Lumpur, Kuala Lumpur

24 - 26 September 2019

Industrial Control System (ICS) Security Training, Cyberjaya Selangor

23 - 16 September 2019

Cyber Security Malaysia – Awards, Conference & Exhibition (CSM-ACE) 2019, Kuala Lumpur

Cyber Forensics Colloqium, Kuala Lumpur

24 September 2019

Grand Final Of National ICT Security Discourse – Cybersafe Challenge Trophy (NICTSeD) 2019, Kuala Lumpur

25 September 2019

Cyber Security For Critical Assets (CS4CA) Summit 2019, Singapore

29 July 2019

2nd Quarter Common Criteria Recognition Arrangement (CCRA) 2019 Meeting And International Common Criteria Conference (ICCC), Singapore

25 September - 2 October 2019

26 Septemeber 2019

OIC-CERT Academic Colloqium 2019, Kuala Lumpur

26 September 2019

Malaysia Cyber Security Awards 2019, Kuala Lumpur

29 September - 2 October 2019

Annual General Meeting And Conference Of Computer Emergency Response Team Asia Pacific (APCERT), Singapore

30 September - 4 October 2019

International Common Criteria Conference 2019, Singapore

Total Security Conference 2019, Kuala Lumpur

1 October 2019

World Trustmark Alliance (WTA) Annual Meeting, Shenzhen

14 - 16 October 2019

Introduction to IT Security & Awareness Training, Malaysia Correctional Institution, Tanjung Kling, Melaka

15 October 2019

10TH International Conference on ICT Convergence (ICTC 2019), Jeju Island, South Korea

16 - 18 October 2019

24 October 2019

Talk At Management & Science University (MSU), Shah Alam, Selangor

26 - 31 October 2019

Talk At Management & Science University (MSU), Shah ALam, Selangor

27 - 31 October 2019

Regional Cybersecurity Summit, FIRST & ITU-ARCC Regional Edutech Asia Expo, Suntec Convention Centre, Singapore

4 - 6 November 2019

Edutech Asia Expo, Suntec Convention Centre, Singapore

Cyber Crime Workshop , Interpol IGCI, Singapore

4 - 6 November 2019

6th Plenary Meeting Of ISO/TC 307: Blockchain And Distributed Ledger Technologies, Hyderabad, India

16 - 23 November 2019

19th Regional Asia Information Security Exchange (RAISE) Forum Meeting, Tokyo, Japan

19 - 20 November 2019

4th International Cyber Warfare and Security Conference 2019 at Ankara, Turkey

20 - 21 November 2019

25 - 27 November 2019

2nd International Research Conference And Innovation Exhibition 2019 (IRCIE 2019), Johor Bharu, Johor

25 November 2019

Launching Of The Modular Professional Certification , Shah Alam, Selangor

27 - 28 November 2019

CyberSecurity Awareness And Knowledge Systemic High-Level Application (YAKSHA) First User Conference, Putrajaya

27 - 31 November 2019

Bangladesh Smart City Expo, Dhaka, Bangladesh

Working Visit From Badan Siber Dan Sandi Negara (BSSN), Indonesia To Cybersecurity Malaysia, Cyberjaya

27 November 2019

Qatar First Technical Colloquium, Doha

1 - 2 December 2019

Modular Professional Certification Launching Event, KISMEC Sungai Petani

2 December 2019

2nd Cloud Guideline Workshop, Bangi Resort Hotel, Bandar Baru Bangi, Selangor

5 December 2019

6 December 2019

Working Visit From Vietnam Agencies To CyberSecurity Malaysia, Cyberjaya

8 December 2019

Modular Professional Certification Launching Event, Hilton Kota Kinabalu, Sabah

9 December 2019

Smart Campus Universiti Malaysia Pahang (UMP) Secretariat Workshop With CyberSecurity Malaysia)

17 - 22 December 2019

International Cyber Shield 2019, Turkey

ACHIEVEMENTS & AWARDS 2019

27 June 2019

Champion at the 1st ACSC-ASEAN Capture the Flag

24 May 2019

CyberSecurity Malaysia has been accredited by INTERPOL for the contribution and assistance of digital forensics expertise in developing the INTERPOL Global Guidelines For Digital Forensics Laboratories.

31 July 2019

CyberSecurity Malaysia Cryptographic Evaluation Lab (MyCEL) successfully accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) based in Gaithersburg, Maryland, USA to perform cryptographic module validation and testing based on FIPS 140-2 Security Requirements for Cryptographic Modules standard. MyCEL is the first lab in ASEAN region, the fourth in Asia and among 22 laboratories in the world that acquires NVLAP accreditation under the Cryptographic and Security Testing program. With the recognition, currently, Malaysia is the third country in Asia region, that obtain the accreditation, alongside Taiwan and Japan.

PROFESSIONAL CERTIFICATION

No	Name	Department	Certification
1	Shazil Imri Mohd Hizam	MyVAC	Certified Application Security Engineer (CASE) - Java
2	Harmi Armira Mohamad Har	MyVAC	Certified Application Security Engineer (CASE) - Java
3	Farihan Binti Ghazali	MyVAC	Associate Business Continuity Professional (ABCP)
4	Ahmad Khabir Shuhaimi	SMBP	CERTIFIED CHIEF INFORMATION SECURITY OFFICER V1
5	Shuaib Chantando	MyCERT	SANS GIAC Defending Web Applications Security Essentials (GWEB)
6	Mohd Hafiz Mat Tabrani	MyCERT	SANS GIAC Certified Forensics Analyst (GCFA)
7	Muhammad Azri Rafiuddin Basri	MyCERT	GCHQ Certified Security Operation Centra (SOC) Incident Responder
8	Muhammad Azizi Bin Jamadi	MyCERT	GCHQ Certified Security Operation Centra (SOC) Incident Responder
9	Izzatul Hazirah Ishak	MyCERT	GIAC Pyhton Coder (GPYC)
10	Zailin Marjuni	CSIEC	Certified Information Security Awareness Manager (CISAM)
11	Nurkhairunnisya Mohamad Khairi	CSIEC	Certified Information Security Awareness Manager (CISAM)
12	Najatih Faghira Abdul Hamid	SRA	Certified Information Security Awareness Manager (CISAM)
13	Noor Azwa Azreen Abd Aziz	SRA	Certified Information Security Awareness Manager (CISAM)
14	Nurfarhana Nasrulhaq Mohd Zulkifli	SRA	Certified Information Security Awareness Manager (CISAM)
15	Rushidan Ghazali	SRA	Certified Information Security Awareness Manager (CISAM)
16	Wan Zulhamli Wan Abdul Rahman	SRA	Certified Information Security Awareness Manager (CISAM)
17	Mohd Muslim Mohd Aruwa	MySEF	Certified Ethical Hacker (CEH) V10
18	Muhammad Zahid Ismail	DF	GIAC Forensics Examiner Certified (GCFE)
19	Sarah Abdul Rauf	MyCERT	GIAC Certified Incident Handler (GCIH)
20	Ummu Khosyatillah Muzakir	MyVAC	Certified Application Security Engineer-.Net
21	Syazwan Hafizudin Shuhaimi	MyCERT	ITIL® Foundation Certificate In It Service Management
22	Ismamuradi Dato' Hj Abdul Kadir	SM	Certified KPI Professional
23	Mohd Sharulnizam Kamarulzaman	SM	Certified KPI Professional
24	Ernieza Ismail	SM	Certified KPI Professional
25	Amirah Syazwani Ahmad Suparmin	SM	Certified KPI Professional
26	Abdullah Hakim Zamli	SM	Certified KPI Professional
27	Ahmad Mohd Azhar	SM	Certified KPI Professional
28	Raja Nur Zafirah Raja Sharudin	IE	Certified General Translation
29	Khairul Akma Mahamad	IE	Certified General Translation
30	Nur Fazila Selamat	STS	Certified ISO 22301 Lead Auditor (BCM)
31	Wan Shafiuddin Zainudin	ISCB	Certified ISO 22301 Lead Auditor (BCM)
32	I.d. Safairis Amat Noor	ISCB	Certified ISO 22301 Lead Auditor (BCM)
33	Marinah Syazwani Mokhtar	ISCB	Certified ISO 22301 Lead Auditor (BCM)
34	Nur Shazwani Mohd Zakaria	ISCB	Certified ISO 22301 Lead Auditor (BCM)
35	Nurul Husna Khasim	ISCB	Certified ISO 22301 Lead Auditor (BCM)
36	Muhammad Faridzul Sukarni	ISCB	Certified ISO 22301 Lead Auditor (BCM)
37	Amiroul Farhan Roslaini	ISCB	Certified ISO 22301 Lead Auditor (BCM)

TECHNICAL PAPERS AND JOURNALS

No	Paper Title	Journal	Conference Proceeding	Date
1	Cryptographic Randomness Analysis on Simon32 64	International Journal of Cryptology Research Volume 9 Issue 1	N/A	2019
2	New Vulnerabilities Upon Pomaranch Boolean Function Through Fault Injection Analysis	International Journal of Cryptology Research Volume 9 Issue 1	N/A	2019
3	A Systematic Review on Cloud Security Auditing	Journal of Advanced Research in Dynamical and Control Systems Volume 11 Special Issue 1	2nd Global Conference on Computing & Media Technology	January 2019
4	A review of Security Assessment Methodologies in JICS	Emerald Insight -Journal of Information and Computer Security Volume 27 Issue 1	N/A	February 2019
5	Findings Annihilator(s) via Fault Injection Attack on Boolean Function of Grain v0		International Conference on Applied Mathematics, Computational Science and Systems Engineering	February 2019
6	Towards Implementing Scalable and Reconfigurable SCADA Security Testbed in Power System Environment	International Journal of Critical Infrastructure Volume 15 Issue 2	N/A	February 2019
7	Project Report: The CiliPadi Family of Lightweight Authenticated Encryption	Project Report	N/A	March 2019
8	Measuring the Effectiveness of Phishing Detection Tool: Comparative Study on Pattern Matching and User Rating Technique	Journal of Computers Volume 14 No 4	N/A	April 2019
9	A Comparative Analysis Study: Open Data Concepts in Smart Cities	International Journal of Advances in Electronics and Computer Science Volume 6 Issue 5	N/A	May 2019
10	Development of Denial of Service (DoS) Mitigation for Internet of Things (IoT) Sensor Node	Global Journal of Engineering & Technology Review Volume 4 Issue 2	N/A	June 2019
11	Enhanced Automated Scripting Method for Improved Management of SQL Injection Penetration Tests on a Large Scale	IEEE Xplore Digital Library	IEEE 9th Symposium on Computer Applications & Industrial Electronics	June 2019
12	Malware Forensic Analytics Framework Using Big Data Platform		Future Technologies Conference	June 2019
13	Man-in-the-Middle Attacks on Electrical Power Grid SCADA System	IEEE Xplore Digital Library	7th International Conference on Smart Computing & Communications	June 2019
14	Terrorism Indoctrination via Social Media: A Malaysian Case Study		6th European Conference on Social Media 2019	June 2019
15	Instilling Digital Citizenship Skills Through Education: A Malaysian Perspective		Proceeding of the 18th European Conference on Cyber Warfare and Security	July 2019
16	Smart Energy Monitoring System for Residential in Malaysia		3rd International Conference on Big Data and Internet of Things	August 2019

17	A New Cryptojacking Malware Classifier Model Based on Dendritic Cell Algorithm		1st European Conference on Frontiers of Computer Science and Information Technology	September 2019
18	Android Malware Classification Using XGBoost on Data Image Pattern	IEEE Xplore Digital Library	IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)	October 2019
19	Enhanced Statistical Analysis Evaluation Using CSM Randomness Test Tool	International Journal of Cryptology Research Volume 9 Issue 1	N/A	October 2019
20	Malware Classification based on Phylogenetics	International Journal of Engineering and Advanced Technology Volume 9 Issue 1	N/A	October 2019
21	Malware Classification for Cyber Physical System (CPS) Based on Phylogenetics	International Journal of Engineering and Advanced Technology Volume 9 Issue 1	N/A	October 2019
22	Design Consideration of Malay Text Stemmer Using Structured Approach		3rd International Conference on Smart Trends for Computing and Communications, Smart Innovation, System and Technology	December 2019
23	Endpoint Detection and Response: Why Use Machine Learning	IEEE Xplore Digital Library	10th International Conference on ICT Convergence	December 2019
24	Enhanced Text Stemmer with Noisy Text Normalization for Malay Texts		3rd International Conference on Smart Trends for Computing and Communications, Smart Innovation, System and Technology	December 2019
25	Crypto Ransomware Detection on Windows Operating System	International Journal of Engineering and Advanced Technology Volume 9 Issue 2	N/A	December 2019

EDITORIAL TEAM

TS. DR. ZAHRI BIN YUNOS
Chief Operating Officer

MUSTAFFA BIN AHMAD
Senior Vice President

MOHD SHAMIL BIN MOHD YUSOFF
Head of Department

ZUL AKMAL ABD MANAN
Executive

AZLIN BINTI SAMSUDIN
Senior Executive

NUR HASLAILY BINTI MOHD NASIR
Senior Executive

AZRINA BT MD SAAD
Senior Executive

ERNIEZA BINTI ISMAIL
Senior Executive

MOHD ROHAIZAD BIN MOHD GHAZALI
Senior Executive

NURUL 'AIN BINTI ZAKARIAH
Executive

NORHUZAIMI BIN MOHAMED
Senior Executive

NUR ATHIRAH BINTI ABDULLAH
Executive

SOCIAL MEDIA

CyberSecurity MALAYSIA

@CyberSecurityMalaysia

@cybersecurity_malaysia

@cybersecuritymy

@CyberSecurityMy

@cybersecurity-malaysia

MyCERT
Malaysia Computer Emergency Response Team

@mycert.org.my

@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
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

© CyberSecurity Malaysia 2020 – All Rights Reserved

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : ISM 00114

MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

ACB ISMS 02

Status Company