MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

ANNUAL REPORT 2021

COVER RATIONALE

"Keluarga CSM" is inspired by the government's concept of "Keluarga Malaysia" and aligned with "Pelan Antirasuah Organisasi (OACP) 2021-2023 CyberSecurity Malaysia". It aims to enrich noble values and culture of integrity among employees within the organisation.

"Keluarga CSM" strengthens employees integration through the adoption of "Keluarga Malaysia" framework and implementation of its three main characteristics, that are inclusivity, common ground and contentment. Its holistic and comprehensive approach foster a harmonious and conducive work environment, enhancing employees cognitive performance and physical well-being towards accomplishing organisational goals.

TABLE OF CONTENT

1 INTRODUCTION

2 CORPORATE GOVERNANCE

3 OPERATION'S REVIEW

INTRODUCTION

About CyberSecurity Malaysia

CyberSecurity Malaysia is the national cybersecurity specialist agency under the purview of the Ministry of Communications and Multimedia Malaysia (K-KOMM).

Pursuant to the Federal Government Ministerial Order 2019, with effect from 21 May 2018, CyberSecurity Malaysia is placed under Minister of Communications and Multimedia Malaysia.

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

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 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 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.

HISTORY

19 OCTOBER 2018

2018

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

30 MARCH 2007

2007

NISER was officially registered as CyberSecurity Malaysia

20 AUGUST 2007

CyberSecurity Malaysia was officially launched by the Prime Minister of Malaysia

28 SEPTEMBER 2005

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

13 JANUARY 1997

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

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 produce Malaysia Threat Landscape report, technical findings and analysis based on the incidents reported by Internet users.

LebahNET.MY
CyberSecurity Honeynet Project

Lebahnet
(Honeynet Project)

Lebahnet is based on Honeypot technology. It provides supporting information on network trends and malicious activities for MyCERT to handle incident as well as advisory activities. Honeypots 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.

Cyber Health Assessment
(Network Compromise Assessment)

Cyber Health Assessment (CHA) was conducted using CMERP Insight (INSIGHT). INSIGHT is a Breach Detection System (BDS) to detect malicious and suspicious activities of malware inside a network after a breach occurred. It is a solution designed to identify signs of threats and alert the organization on potentially dangerous activity.

INSIGHT is deployed using method out of band system which scan data mirrored from network switch activities. Advanced Persistent Threats (APT) employ various exploits on a target, depending on the type of vulnerable Internet applications used over the network. INSIGHT assist IT personnel to detects unknown, advanced and adaptive threats.

Managed Security Services

Advanced Security Operation Center (ASOC) monitor, track and response to security incidents such as Malware attacks, Intrusions, DDoS to protect organization's data and IT infrastructures especially Small Medium Enterprise (SME's) using the technology developed by local experts, Coordinated Malware Eradication & Remediation Platform Technology (CMERP).

CSIRT Consultancy

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

Phishing Exercise (Social Engineering)

Phishing assessment assess awareness among staff within an organization by sending malicious emails. It aims is to analyse staff's responsiveness towards phishing attempt and directly measure staff compliance against internal policies and procedures.

Cyber Drill Exercise

CyberDrill is an activity conducted by MyCERT to assess organization's cyber capacity by measuring its ability to detect and respond to a security incident. This project utilize various tools and infrastructure in CSM to perform simulated cyber drill exercise that aim to identify organisations' readiness based on existing cyber security incident response procedures.

Host Malware Scanning (Host Compromise Assessment)

Host Compromise Assessment is a service to identify evidence of malicious activity within the IT assets, through analysed data retrieved from internal scanning and 3rd-party tools. This assessment includes several stages, planning, preparation, execute, identify and reporting, to identify malware activities.

2. Digital Forensics (DF)

CyberDISCOVERY

Cyber Discovery

Digital Forensics (DF) Case Management (CyberDiscovery)

Incident Handling Case Management (CyberDiscovery)

CyberDiscovery is a professional cyber forensics service for public, individual or private organization. It addresses concerns on Electronic Stored Information (ESI) as digital evidence, in order to provide answers for questions raised in a civil litigation. It provides the following services:

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

x-Forensik 2.0

X-Forensics Tools

X-Forensik: Evidence Preservation Tools is a series of digital forensic tools developed for digital data preservation ensuring its integrity and admissibility as evidence in judicial proceeding.

PenDua x-Forensik 2.0

PenDua Tool

Pendua is a forensically sound portable digital file duplicator. It is used to duplicate digital document from a computer and its hashing function complies to forensics and evidence admissibility requirements. It also provides activity log critical in an investigation.

Pendua tool is developed under X-Forensik initiative.

Kloner x-Forensik 2.0

Kloner

Kloner is a forensically sound data acquisition tool embedded with Cloning, Imaging and Wiping capabilities. Its write-protect and hashing functions comply to forensics and evidence admissibility requirements. Kloner assist investigators to preserve digital evidence at crime scene.

Kloner tool is developed under X-Forensik initiative.

DataHapus

x-Forensic DataHapus is a high-powered and user-friendly data sanitization device with a GUI touch display. x-Forensic Data Sanitization sanitize hard disk thoroughly to ensure all confidential files are permanently deleted before disposal.

DataHapus tool is developed under X-Forensik initiative.

CamMuka 2.0

CamMuka

CamMuka is a forensically sound facial recognition system to perform facial recognition of the unknown face with the known face. It is utilized in investigation of criminal cases, where the result of the recognition analysis is accepted by the court.

The Artificial Intelligence (AI) behind CamMuka is proven and backed up by scientific journals. CamMuka system applications are supported with SOPs and methodologies comply with digital forensic international standards.

Digital Forensics Quality Management System Expert Consultation

Digital Forensics Quality Management System Expert Consultation service assist digital forensics lab to develop digital forensics policy and procedures based on international standard ISO 17025 requirements. It enable organisations to develop competent staff, provide controlled environment and equipments, to produce high quality digital forensics results, admissible in court of law and fulfill customers expectation.

3. Cryptography Development

MyKripto Validation

MyKripto Validation is a security validation and analysis service that include the following:

1. Cryptanalysis of a cryptographic algorithm to gauge its security strength
2. Cryptographic algorithm conformance testing against a standard document
3. Determine randomness characteristics of a random generator

MyCEL
CyberSecurity Malaysia Crytographic Evaluation Lab

CyberSecurity Malaysia Cryptographic Evaluation Lab (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 conduct evaluation and validation activities of cryptographic modules contained in a security product based on FIPS140 security requirements. This enhance user's security and develop trust in using cryptographic module in security products.

Apart from FIPS140, MyCEL also conduct cryptographic module validation based on ISO/ IEC19790 requirements and cryptographic algorithm validation based on MySEAL

MySEAL
Senarai Algoritma Kriptografi Terpercaya Negara

Blockchain Security Assessment

Blockchain Security Assessment is a service to validate and verify security properties in a blockchain and smart contract. Businesses gain insight on its overall blockchain and smart contract security posture, and improve the ability to address potential flaws in their blockchain-based solutions or applications.

4. MalaysianSecurity Evaluation Facility

Malaysian Security Evaluation Facility

ICT Product Security Assessment (IPSA)

IPSA is a security functional testing and/or vulnerability assessment and penetration testing adapting ISO/IEC 15408 Common Criteria (CC) and ISO/IEC 18045 Common Methodology for Information Technology Security Evaluation (CEM) referring (but not limited to) Malaysian Standards (MS) and best practices.

Common Criteria Laboratory Development and Advisory Services

Based on our experience providing Common Criteria Evaluation to our clients, we provide technical services & advisory to existing and potential CC laboratories. It mainly consists of Standard Operating Procedure (SOP) development, accreditations preparations, laboratory facilities check and audit session/s. Our technical expert will offer in-depth industry experience in many areas including up-to-date information and regulatory on Common Criteria service.

ISO 17025 Professional Laboratory Service and Specialized Equipment

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 offer this service based on the Scope of Work (SOW) agreed by both Test Labs including security evaluations, security functional testing or penetration testing.

Cloud Security Services (Cloud Security Readiness Assessment)

The scope of **Cloud Security Readiness Assessment** requirements focus on cloud security audit on IaaS, PaaS and SaaS platform for Cloud Service Subscribers (CSS), Cloud Service Providers (CSP) and Cloud Service Brokers.

Cloud Security Readiness Assessment may be conducted independently for none ISMS complying Cloud Service Subscribers (CSS), Cloud Service Providers and Cloud Service Brokers.

The scope of Cloud Security Readiness Assessment for ISMS requirements focus on cloud security audit on IaaS, PaaS and SaaS platform for Cloud Service Subscribers (CSS), Cloud Service Providers (CSP) and Cloud Service Brokers.

Cloud Security Readiness Assessment for ISMS can be conducted as an extension on Cloud scope on top of Information Security Management System (ISMS) Certification.

Cloud Security Services (Cloud Security Vulnerability Assessment)

The scope of **Cloud Security Vulnerability Assessment** involve Vulnerability Assessment & Penetration Testing on Cloud SaaS and/or PaaS for Cloud Service Provider (CSP).

- Vulnerability Assessment (VA) is performed by assessors in determining common threats, loopholes and weakness of cloud solution deployed in the forms of PaaS and/or SaaS.
- Penetration Testing is an activity to exploit weaknesses of the cloud solution deployed in the form of PaaS and/or SaaS.

5. Malaysia Vulnerabilities Assessment Centre (MyVAC)

Security Posture Assessment (SPA)

1. Security Posture Assessment is an exercise to identify security loopholes in an organization
2. Include service process diagram (if possible/ necessary)
3. Method and approach based on international standard OWASP, OSSTMM, and PCI-DSS
4. Effective security risk assessment to prevent breaches, reduce impact of realized breaches, and protect company's reputation

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 vulnerabilities in order to reduce risk of security breach.

6. CyberSecurity Industry Engagement and Collaboration (CIEC)

CyberSecurity Malaysia Award, Conference and Exhibition (CSM-ACE)
www.csm-ace.my

Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE) is a public-private-partnership driven platform for knowledge sharing and cybersecurity professional development. It serves as a forum for cybersecurity experts to discourse on cybersecurity current issues, trends, technology and innovations and to recognize contribution of individuals and organizations in the field of cyber security. CSM-ACE overview the following:

- To act as a catalyst in driving innovation and growth for the cyber security industry.
- To inculcate cyber security culture and awareness at national level.
- To gather industry experts and communities on the latest cyber security trends.
- To provide a platform for industry discourse on Malaysia's cybersecurity development and innovation towards national economic growth.
- To create greater awareness and educate small and medium-sized enterprises (SME) to nurture a culture of protecting against cyber threats

MyCyberSecurity Clinic (MyCSC)- Data Recovery and Data Sanitization Services
www.cybersecurityclinic.my

MyCyberSecurity Clinic provide 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.

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

CyberSecurity Malaysia Collaboration Program (CCP) serve 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 provide 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.

7. Information Security Certification Body (ISCB)

Information Security Management System (ISMS) Certification

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

MyTrustSEAL

MyTrustSEAL is a web seal issued to company's website after it fulfils MyTrustSEAL principles based on the scope being identified - 1. Secured website and online transaction 2. Compliance to Malaysian Communications & Multimedia Content Code 3. Compliance to personal data protection - PDPA 2010

Penetration Testing Service Provider(PTSP) Certification

Penetration Test Service Provider (PTSP) is a national scheme provided to 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.

Behavioural Competency Assessment

A psychometric test designed to measure behavioural competency that contributes to professional excellence in information security roles, providing a scientific method and performance feedback in a structured consistent and systematic way.

Privacy Information Management System (PIMS) Scheme

The ISO/IEC 27701 standard assists organisations to establish, maintain & improve a **Privacy Information Management System (PIMS)** by enhancing an ISMS based on the requirements of ISO/IEC 27001 and guidance of ISO/IEC 27002.

Technology Security Assurance (TSA)

Technology Security Assurance (TSA) is a national scheme developed for product evaluation and certification. It is MyCC fast-track which include 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.

Malaysian Common Criteria Scheme (MyCC)

Malaysian Common Criteria Evaluation and Certification (MyCC) is an ICT products or Protection Profile (PP) security evaluation based on Common Criteria (CC), an international standard based on ISO/IEC 15408 Common Criteria (CC) and ISO/IEC 18045 Common Evaluation Methodology. Information Communication and Technology (ICT) products or/and Protection Profile (PP) are evaluated against CC requirements to determine its security fulfil certain assurance level.

Business Continuity Management System (BCMS) Certification

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

8. Outreach & Corporate Communications (OCC)

CyberSAFE™ L.I.V.E. Galeri

CyberSAFE™ L.I.V.E. Galeri was built as one of the initiatives under CyberSAFE™ Program, aims to foster awareness and disseminate information on cyber security and safety as well as to increase understanding and interest in the cyber security field. The concept is to display and showcase hands-on product and information besides futuristic view on our daily routine involving Internet of Things, data as well as information exchange and gathering in today's cyber world. These information are expected to raise public awareness on the importance of cyber security including CyberSecurity Malaysia roles and functions. Students are exposed on critical subjects in cyber security field such as Science, Technology, Engineering and Mathematics (STEMS), for instance, description on Mathematics algorithm role in Cryptography. CyberSAFE™ L.I.V.E Galeri 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 cyber security. 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 gain new experience and learn cybersecurity knowledge, advancement and guidelines)

Cyber Security Awareness For Everyone (CyberSAFE) Program
www.cybersafe.my

Cyber Security 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.

9. Cyber Security Professional Development (CSPD)

Cybersecurity Competency & Certification Training (CyberGuru)
www.cyberguru.my

CyberGURU is a platform to nurture Information Security practitioners and cybersecurity professional developments through various competency training courses and certifications. It promotes knowledge sharing with leading industry experts, as well as academicians and policy makers by fostering local and international collaborations.

CyberGURU has over a decade of experience in Information Security Competency and Specialized Training in Malaysia. We deliver diverse lineup of competency and professional certification courses aimed at meeting accelerating needs of today's cyber landscape; from fundamental to certified training of various tracks such as Incident Handlings, Digital Forensics, Security Assessment, Cryptography, Common Criteria and Security Management.

Global Accredited Cybersecurity Education (ACE) Scheme
https://globalace.org/home

The Global ACE Certification is a holistic framework of professional certification scheme in the area of cyber security that outlines the overall approach - independent assessments, impartiality of examinations, identification and classification of cybersecurity domains, the requirements of professional memberships and code of conduct of cyber security professionals. 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 by Board of Technologist (MBOT), professional body through a Technologists & Technicians Act 2015 - Act 768 and Jabatan Pembangunan Kemahiran (JPK) under Ministry of Human Resources; and globally by The Organisation of Islamic Cooperation (OIC) and the OIC- Computer Emergency Response Team (OIC-CERT).

10. Information Security Management & Assurance (ISMA)

Information Security Governance, Risk & Compliance Health Check Assessment (ISGRiC)

A service to assist organisations to determine current level of readiness and initiatives in information security governance, risk management and compliance thus, ensure management make informed decisions based on ISGRiC results, justify the information security investment and support business case for managing information security.

ISMS Guidance Series

A service that provides expert guidance to organisations for the protection and preservation of confidentiality, integrity and availability of information and information systems through implementation of information security management in accordance to ISO/IEC 27001 Information Security Management System (ISMS) requirements.

Privacy Information Assessment

A service to conduct compliance and impact assessment on organisations that collect, store and process personal identifiable information (PII) covering technology, process and people. This is to ensure data privacy protection is uphold in accordance to relevant acts and international standards (Malaysia PDPA Act709 and ISO/IEC 27701).

- Data Privacy Jurisdiction Risk Assessment (PJuRA)
- Data Privacy Impact Assessment (DPIA) (*development is in progress, to be completed in 2022)

11. Government Engagement (GE)

Government Engagement
ciip.cybersecurity.my

Government Engagement offers strategic engagement services with stakeholders within the Malaysian Government. It aims to identify and lead various national cybersecurity initiatives, programmes, collaborations, and activities to advocate and enhance the prominence of cybersecurity agenda for the nation. This service also provides administration for the Critical Information Infrastructure Protection (CIIP) portal.

12. International Engagement (IE)

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.

13. Strategic Study

Strategic Study

- Strategic advice
- Feedback to stakeholders'
- Collaborations with relevant local and international parties
- mplementation of cyber security technologies

14. Research

Research

- Cyber Security Responsive Services
- Cyber Security Acculturation & Capacity Building
- Information Security Certification
- Cyber Security Governance, Risk Management & Compliance
- Cyber Security Assessment & Assurance
- Cyber Rapid Action & Intelligence
- Cyber Security Strategic Studies
- Digital Forensic

CORPORATE GOVERNANCE

CHAIRMAN STATEMENT

> I am pleased to report that CyberSecurity Malaysia continued to be the pillar of strength for our nation's cybersecurity in 2021 by spearheading the development of a safer and more resilient cyber ecosystem through provision of quality and impactful services, imparting cyber knowledge and technical supremacy as well as nurturing Malaysia's talent and expertise.

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

According to a research survey by Cisco Systems on Asia, 2021 proved to be yet another difficult year as nations across the globe, including Malaysia, scramble to contain the resurgence in COVID-19 infections due to the more transmissible Omicron variant. The pandemic posed an enormous challenge for businesses in Malaysia to continue operating despite massive shutdowns of offices and other facilities. Employees were mostly confined to virtual and digital platforms for work and social interaction. Consequently, the physical and digital worlds continued to merge, making it a fertile ground for cyber criminals and actors to launch sophisticated cyber-attacks against those working remotely from home.

According to Oppotus Research Group, approximately 48% of Malaysia's workforce, especially among Professionals, Managers, Executives and Businessowners (PMEBs) could not return to office in 2021 and were compelled to work from home. Today, working from home become a gateway to new forms of data theft as companies also faced increased cyber risk.

Globally, 2021 saw 50% more cyber-attacks per week on corporate networks compared to 2020. Check Point Research also indicated that cyber-attacks reached an all-time high at the end of 2021 after revelations of the Log4J exploit. The year also saw several high profile breaches such as the SolarWinds hack and Colonial Pipeline ransomware attack in the US that had major economic and security impact. From January to December 2021, a total of 10,016 cases of cyber incidents were reported to Cyber999 in Malaysia.

On the back of escalating challenges and cyber threats, 2021 saw the unveiling of **MyDigital – Malaysia's Digital Economy Blueprint** that sets out a strategic roadmap for Malaysia to position the country as a digital content and cyber security leader in the regional market by 2030. It promotes Malaysia to the forefront of cybersecurity innovation and create economic opportunities for the country.

The five key thrusts in **MyDigital** reflect CyberSecurity Malaysia's mission and our key strategies to raise cybersecurity awareness; equip students with knowledge and skills on acceptable ways of using the Internet; strengthen data protection and related regulatory framework; reinforce cross-border data transfer mechanisms and protection to facilitate seamless data flow; and to cultivate investment in cybersecurity to create a safe, secure and trusted digital ecosystem.

I am pleased to inform that CyberSecurity Malaysia continued to be the pillar of strength for our nation's cybersecurity in 2021 by spearheading the development of a safer and more resilient cyber ecosystem through provision of quality and impactful

services, imparting cyber knowledge and technical supremacy as well as nurturing Malaysia's talent and expertise.

On technology service offerings, CyberSecurity Malaysia unveiled **CamMuka 2.0** – a new and improved version powered by artificial intelligence (AI) to increase depth to CyberSecurity Malaysia's digital forensics services. This latest edition enable CamMuka to be deployed on various computing devices from personal computers, laptops and devices.

At the forefront of 5G technology adoption, CyberSecurity Malaysia signed a landmark MoU with Huawei Technologies and Celcom Axiata Berhad in March 2021 to jointly develop the region's first 5G Cyber Security Test Lab. The lab conduct test cases related to Internet of Things (IoT) and telecommunication security, as well as to improve the country's preparation in responding to 5G-related cyber-attacks. We will establish test-lab accreditation from NESAS Security Test Laboratories and Common Criteria. The facility put Malaysia firmly on the world map as a regional cyber security hub.

CyberSecurity Malaysia also inked a MoU with Cisco Systems, a world-class leader in cybersecurity, to establish cooperation in research, development and sharing of information and knowledge. This collaboration strengthen cybersecurity capabilities, enhance Malaysia's global threat intelligence and contribute towards upskilling and development of our cybersecurity workforce.

Another significant milestone for CyberSecurity Malaysia was the official launch of **SiberKASA**, an initiative aimed at developing, empowering, sustaining and strengthening cybersecurity infrastructure and ecosystem in Malaysia to ensure network security preparedness. It is a holistic ecosystem approach that leverages people, process, and technology to create a highly adaptive and cooperative cybersecurity framework. Under SiberKASA initiative, CyberSAFE™ L.I.V.E Galeri was also unveiled as Malaysia's first cybersecurity gallery, a hub for learning and teaching, as well as dissemination of information on cybersecurity.

One of the key highlights of 2021 was undoubtedly Malaysia's sterling performance in the Global Cybersecurity Index (GCI) ranking. The International Telecommunication Union (ITU) scored and ranked Malaysia as No. 5 in the Global Cybersecurity Index 2020. This was a remarkable improvement from the 8th spot in the previous index in 2018. At the Asia Pacific level, Malaysia was ranked second after joint leaders South Korea and Singapore.

Through various outreach initiatives and capacity building strategies undertaken by CyberSecurity Malaysia, Malaysia achieved top score in three of five ITU categories, namely legal framework for handling security and crime, capacity measures based on R&D, education and training, as well as international partnerships and information-sharing. It is also heartening to note that Malaysia has been consistently ranked top 10 since the first report was released in 2014.

On the international collaboration front, CyberSecurity Malaysia was re-elected chair for Asia Pacific Computer Emergency Response Team (APCERT) 2021-2022, marking its fourth term. The re-election for three consecutive terms underscored confidence bestowed upon Malaysia's leadership in enhancing Asia Pacific regional and international cooperation on information security. As joint co- founders of APCERT since 2002, CyberSecurity Malaysia remains on its steering committee for 2021 - 2023.

Looking ahead

In today's volatile digital environment, companies must anticipate and be prepared to recover from potential impact of major cyber incident. Cybersecurity is a collective responsibility requiring government and various industry stakeholders to work closely together.

As Malaysia slowly transitions to post-pandemic life with more industries and consumers embracing digitalisation, cybersecurity literacy and resilience become highly critical. That said, CyberSecurity Malaysia remains firmly committed in our mission towards strengthening our nation's cyber resilience with renewed optimism.

Lastly, I would like to thank the management team, staff, our partners and associates for their support and hard work which has enabled us to come this far. I am confident, CyberSecurity Malaysia is in a strong position to overcome new challenges and continue to keep our country cyber safe.

BOARD OF DIRECTORS

General Tan Sri Dato' Sri Panglima Mohd Azumi bin Mohamed (Retired)

Chairman, Board of Directors, CyberSecurity Malaysia,

Dato' Sri Haji Mohammad Bin Mentek

Secretary General of the Ministry of Communications and Multimedia Malaysia

Director, CyberSecurity Malaysia

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

Mohd Sori Bin Husain

Director, CyberSecurity Malaysia

Shaifubahrim Bin Mohd Saleh

Director, CyberSecurity Malaysia

Azih Bin Yusof

Director, CyberSecurity Malaysia

Dato' Dr. Suhazimah binti Dzazali

Director, CyberSecurity Malaysia

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 map out and review 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 consider in depth, and if thought fit, approve 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 review action plans implemented by the management to achieve business and operational targets. It oversees the operations and business of CyberSecurity Malaysia by requiring regular periodic operational and financial reporting from 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 to ensure infrastructure, internal controls and risk management processes are well in place.

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

1. The Human Resources and Remuneration Committees (HRRC)

i. Objectives:

- Develop and periodically review overall remuneration policy and human resource strategies of CyberSecurity Malaysia to ensure it is contributing effectively to the success of the company.
- Ensure 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 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 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 rewards and remunerations of company staff to demonstrate rewards and remunerations considered by a committee without personal interest in the outcome of its advice and 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' Sri Haji Mohammad Bin Mentek
2. YBhg. Dato' Dr. Suhazimah binti Dzazali
3. YBrs. Tuan Mohd Sori bin Husain
4. YBrs. Tuan Shaifubahrim bin Mohd Saleh

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.

iv. 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) 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. YBrs. Encik Mohd Sori bin Husain
3. YBrs. Encik Shaifubahrim bin Mohd Saleh

Terms of Reference of the AGI

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.

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.

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 programme and seminars to update themselves on new development 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 are sent out to the members of CyberSecurity Malaysia at least 21 days before the date of the meeting in accordance with the Constitution of CyberSecurity Malaysia.

KEMENTERIAN KOMUNIKASI
DAN MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

PELAN ANTIRASUAH ORGANISASI (OACP) CYBERSECURITY MALAYSIA 2021-2023

Pelan Antirasuah Organisasi (OACP) merupakan salah satu inisiatif mandatori dalam Arahan YAB Perdana Menteri No. 1 Tahun 2018, Siri 2 No. 1 Tahun 2019 – Perkara 6.1.2 - Strategi 6: Memupuk Tadbir Urus Baik Dalam Entiti Korporat Di Dalam NACP.

Manakala Pelan Antirasuah Nasional (NACP) 2019-2023 dilancarkan pada 29 Januari 2019 oleh YAB Perdana Menteri Tun Dr. Mahathir bin Mohamad dengan matlamat mewujudkan negara bebas rasuah. Ia menjadi dasar antirasuah, rujukan utama serta panduan bagi agensi Kerajaan dan entiti berkaitan dalam membangunkan Pelan Antirasuah Organisasi (OACP) masing-masing.

Intipati OACP mencakupi risiko, senario dan punca masalah rasuah di setiap jabatan dari aspek dalaman serta luaran, dan menggariskan 23 inisiatif sebagai mekanisma pengurusan pemantapan tadbir urus (governans), integriti dan antirasuah yang akan dilaksanakan oleh CyberSecurity Malaysia. Seluruh organisasi komited dalam melaksanakan inisiatif-inisiatif tersebut demi mencapai visi 'CyberSecurity Malaysia Sebagai Peneraju Bidang Keselamatan Siber Dengan Warga Kerja Berintegriti Dan Bebas Rasuah'.

PELAN ANTIRASUAH ORGANISASI (OACP) 2021-2023 CYBERSECURITY MALAYSIA telah disahkan dan dipersetujui oleh Pengurusan Tertinggi pada 21 Disember 2021. Ia dihasilkan dengan tunjuk ajar, panduan dan sokongan daripada Suruhanjaya Pencegahan Rasuah Malaysia (SPRM).

NOTICE OF ANNUAL GENERAL MEETING

DENGAN INI DIMAKLUMKAN BAHAWA Mesyuarat Agung Tahunan ("AGM") ke-16 CyberSecurity Malaysia ("Syarikat") akan diadakan di Bilik Jati, Level 10, Tower 1 Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor pada hari Isnin, 27 Jun 2022 pada jam 11.00 pagi untuk pelaksanaan urusan-urusan berikut :

URUSAN BIASA

1.	Untuk menerima Penyata Kewangan yang telah diaudit bagi tahun kewangan berakhir 31 Disember 2021, berserta laporan-laporan Lembaga Pengarah dan Juruaudit yang berkaitan dengannya. *(Rujuk nota keterangan 1)*	
2.	Untuk meluluskan pembayaran elaun bulanan Pengerusi bukan Eksekutif dan Pengarah bukan Eksekutif berjumlah sehingga RM204,000 dan manfaat lain bermula dari tarikh AGM ke-16 hingga AGM Syarikat bagi tahun yang berikutnya. *(Rujuk nota keterangan 2)*	Resolusi 1
3.	Untuk melantik semula Pengarah berikut, yang akan bersara mengikut giliran menurut Artikel 52 Perlembagaan Syarikat dan oleh kerana layak, telah menawarkan diri untuk dilantik semula; 3.1 YBrs. Encik Mohd Sori bin Husain; *(Rujuk nota keterangan 3)*	Resolusi 2
4.	Untuk melantik semula Pengarah berikut, yang akan bersara menurut Artikel 54 Perlembagaan Syarikat dan oleh kerana layak, telah menawarkan diri untuk dilantik semula; 4.1 YABhg. Jeneral Tan Sri Dato' Sri (Dr.) Haji Zulkifeli bin Mohd Zin (Bersara) *(Rujuk nota keterangan 4)*	Resolusi 3
5.	Untuk melantik Tetuan Atarek Kamil Ibrahim & Co (ATAREK) sebagai Juruaudit Luar Syarikat yang baharu bagi tahun kewangan berakhir 31 Disember 2022 dan memberi kuasa kepada Lembaga Pengarah bagi menetapkan imbuhan mereka. *(Rujuk nota keterangan 5)*	Resolusi 4
6.	Untuk melaksanakan urusan-urusan lain yang mana notis yang sewajarnya telah diberikan menurut Akta Syarikat 2016 dan Perlembagaan Syarikat.	

MENURUT PERINTAH LEMBAGA PENGARAH

JAILANY BIN JAAFAR
LS0008843
SSM PC No. 201908002687
Setiausaha Syarikat

Selangor Darul Ehsan
Date : 3 Jun 2022

A) NOTA

1. Anggota Syarikat yang berhak untuk hadir dan mengundi di Mesyuarat Agung Tahunan ("AGM") adalah berhak untuk melantik proksi untuk hadir dan mengundi sebagai pengganti beliau. Seorang proksi tidak perlu menjadi anggota Syarikat. Tiada sekatan mengenai kelayakan proksi. Proksi yang dilantik untuk hadir dan mengundi pada AGM akan mempunyai hak yang sama seperti anggota Syarikat untuk bersuara di AGM.
2. Sebagai pengganti kepada pelantikan proksi, anggota korporat boleh melantik wakil korporatnya untuk menghadiri mesyuarat itu menurut Seksyen 333 Akta Syarikat 2016 ("Akta"). Untuk tujuan ini dan menurut Seksyen 333(5) Akta, anggota korporat hendaklah menyediakan perakuan/sijil di bawah meterai perbadanannya sebagai bukti prima facie mengenai pelantikan wakil korporat.
3. Suratcara pelantikan proksi bagi individu mestilah ditandatangani oleh pelantik atau wakil yang diberi kuasa sewajarnya secara bertulis atau, bagi sebuah perbadanan, suratcara pelantikan proksi atau proksi-proksi hendaklah di bawah meterai atau ditandatangani oleh pegawai atau wakil yang diberi kuasa sewajarnya.
4. Suratcara pelantikan proksi atau perakuan/sijil wakil korporat mestilah didepositkan di Pejabat Pendaftar CyberSecurity Malaysia, Level 7 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia tidak kurang daripada 48 jam sebelum masa yang ditetapkan untuk mengadakan AGM atau pada mana-mana penangguhannya.

B) NOTA PENERANGAN

1. Penyata Kewangan Beraudit bagi tahun kewangan berakhir 31 Disember 2021

Perkara ini bertujuan untuk perbincangan sahaja. Peruntukan Seksyen 340(1) Akta Syarikat 2016 memerlukan Penyata Kewangan Beraudit dan Laporan Lembaga Pengarah dan Juruaudit mengenainya dibentangkan di AGM. Oleh itu, perkara ini bukanlah urusan yang memerlukan resolusi untuk diundi oleh ahli Syarikat. Penyata Kewangan Beraudit tersebut dan Laporan Lembaga Pengarah dan Juruaudit dilampirkan sebagai LAMPIRAN 1.

2. Bayaran elaun bulanan

Bayaran elaun bulanan Pengerusi Bukan Eksekutif dan Pengarah Bukan Eksekutif berjumlah sehingga RM204,000 dan manfaat lain yang perlu dibayar kepada Pengerusi dan Pengarah Bukan Eksekutif di bawah perkara 2 ini adalah seperti yang dinyatakan dalam LAMPIRAN 2.

3. Pemilihan semula Pengarah yang akan bersara menurut Artikel 52

Encik Mohd Sori bin Husain yang dilantik menjadi Pengarah pada AGM ke-14 yang lalu akan menamatkan perkhidmatan setelah berkhidmat untuk tempoh merangkumi dua (2) AGM menurut Artikel 52 Perlembagaan Syarikat dan beliau telah bersetuju untuk dilantik semula sebagai Pengarah Syarikat.

Biodata dilampirkan sebagai LAMPIRAN 3.

4. Pelantikan semula Pengarah yang akan bersara menurut Artikel 54

YABhg. Jeneral Tan Sri Dato' Sri (Dr.) Haji Zulkifeli bin Mohd Zin (Bersara) yang dilantik oleh Lembaga Pengarah sebagai ahli Lembaga Pengarah baharu berkuatkuasa pada 26 April 2022 akan menamatkan perkhidmatan menurut Artikel 54 Perlembagaan Syarikat dan beliau telah bersetuju untuk dilantik semula sebagai Pengarah Syarikat.

Biodata dilampirkan sebagai LAMPIRAN 4.

5. Pelantikan Juruaudit Luar

Lembaga Pengarah Syarikat di mesyuaratnya pada 10 Mac 2022 telah meluluskan untuk mengesyorkan pelantikan Tetuan Atarek Kamil Ibrahim & Co (ATAREK) sebagai juruaudit kewangan luar CyberSecurity Malaysia yang baharu untuk kelulusan ahli-ahli Syarikat pada AGM yang akan datang.

FORM OF PROXY

(COMPANY NO. 200601006881 (726630-U)

Saya/Kami.....(nama penuh dalam huruf besar)

No. Kad Pengenalan/No. Syarikat.....

beralamat di .....

.....sebagai

anggota CyberSecurity Malaysia, dengan ini melantik .....

.....(nama penuh dalam huruf besar)

No. Kad Pengenalan/No. Syarikat .....

beralamat di .....

.....

.atau jika tidak kehadiran beliau .....

.....(nama penuh dalam huruf besar)

No. Kad Pengenalan/No. Syarikat .....

beralamat di .....

sebagai proksi saya/kami untuk mengundi bagi pihak saya/kami di Mesyuarat Agung Tahunan ke-16 CyberSecurity Malaysia yang akan berlangsung di Bilik Jati, Level 10 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor pada hari Isnin, 27 Jun 2022 jam 11.00 pagi atau pada sebarang penangguhan, seperti yang tertera di bawah :

.....

Tandatangan Anggota/Meterai

OPERATION'S REVIEW

FOREWORD FROM THE CEO

The cybersecurity landscape has changed drastically since the pandemic struck. We have witnessed how adversaries can harness the power of good to do harm. Cyber criminals attempting to steal corporate data and intellectual property are certainly not the only threat to businesses. Employees who are not well-versed in cybersecurity knowledge and information will continue to be a weak link in corporate IT security systems. It is critical that each and every stakeholder in our cybersecurity ecosystem must ensure that smart, resilient defenses are put in place to protect against evolving cyber threats.

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

2021 was a year when industries, businesses, communities and ordinary Malaysians came to grips of the post COVID-19 reality and a gradual acceptance of a 'new normal'. It became clear the pandemic had caused a 'tectonic-shift' in the way businesses operate from remote working, virtual meetings and collaboration to explosive growth in e-commerce. In today's world that is becoming more digitally connected and fraught with ever-evolving cyber threats, cybersecurity practices and knowledge must be prioritized in all domains of society.

CyberSecurity Malaysia kicked off the year with a CyberSAFE workshop with the Ministry of Education Malaysia (MOE) through the Education Resources and Technology Division (BSTP). At the end of the workshop, CyberSecurity Malaysia completed its deliberation on the annual nationwide cyber safety activity programmes and handed over the National Cyber Security Awareness Module (MKKSN) to the Ministry of Education as an online teaching and learning module on cyber security awareness for primary and secondary schools.

For higher institutions of learning, a series of Memorandum of Understanding (MoUs) were signed with local universities including Management & Science University (MSU) and Universiti Malaysia Terengganu (UMK) to strengthen partner collaboration in delivering cybersecurity courses, research and testing.

One of the significant milestones for CyberSecurity Malaysia came in March 2021 when **SiberKASA** - a cyber security empowerment program to build, motivate, sustain, and improve Malaysia's cyber security infrastructure and ecosystem was officially launched. Several CyberSecurity Malaysia products and services were also showcased - namely CyberSAFE™ L.I.V.E Galeri, Global Accredited Cybersecurity Education Certification's Upskilling Program (Global ACE), Cyber Security Industry Guidelines, CamMuka 2.0, xForensik, MASSA (Mobile Assessment Security Scanning Application), as well as CMERP ADF (Coordinated Malware Eradication & Remediation Project Advanced DNS Firewall).

Q2 in 2021 saw CyberSecurity Malaysia not only actively participating in cybersecurity awareness programs and action plans to educate industry sectors on new cyber threats but also assisting Malaysia's workforce affected by the COVID-19 pandemic. In April, we launched **Hari Kerjaya Malaysia 2021** with strict standard operating procedures (SOPs) and attended by more than 1,400 participants. The 2-day career fair received strong support from over 16 cybersecurity companies offering over 1,000 job openings in the field of cybersecurity.

In our continuous effort to educate Internet users and foster a more positive cyber environment, particularly women, a Cyber

Ethics webinar **"Empowering Your Mindset with Cyber Ethics"** was organised through YouTube Live in conjunction with 'International Girls in ICT Day'. The webinar was well attended by women activists, educationists, mental health practitioners, entrepreneurs as well as and non-governmental organisations (NGOs).

Despite limitations on physical face-to-face meetings, CyberSecurity Malaysia continued our capacity building and training programs on the virtual platform. In collaboration with the Ministry of Foreign Affairs through Malaysian Technical Cooperation Program (MTCP) a **'Certified Penetration Tester'** 8-day training program was conducted online for 12 regional participants from five (5) ASEAN and OIC-CERT member countries.

CyberSecurity Malaysia also made significant strides in strengthening our nation's infrastructure with stronger cyber resilience for cryptocurrency services. In August 2021, a Memorandum of Cooperation (MoC) was signed with the National Financial Crime Prevention Center (NFCC) that defined cooperation between the two entities in the field of cyber security involving financial security, where CyberSecurity Malaysia provide exclusive support services to NFCC.

Despite a lack of physical event opportunity due to RMCO, the annual National ICT Security Discourse Competition (NICTSeD) was a major success. The preliminary rounds of the 8th edition of NICTSeD CyberSAFE™ Challenge Trophy (Virtual Discourse) were keenly participated by 75 schools nationwide on YouTube LIVE platform. The competition benefited students in developing their communication and research skills as well as ability to address ICT security. The grand finals, held in hybrid mode in December 2021, saw SMK Sultan Abu Bakar from Pahang emerge as champion for the second time.

I am pleased to report that CyberSecurity Malaysia's pinnacle event – **Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE)** made a grand return in 2021 in hybrid format with a theme **'#Cyber Transform'.** The highlight of the 12th annual edition, in addition to the Malaysian Cyber Security Awards, Conferences and Sector Specific and Career Exhibitions, was the official launch of **5G Cyber Security Test Lab (My5G)** in collaboration with Huawei Technologies and Celcom Axiata. The launch of 5G Cyber Security Test Lab marked a giant step towards reinforcing our nation's cybersecurity capabilities in preparation for the 5G launch. My5G will be Southeast Asia's first specialist security evaluation and test facility for 5G products, devices and applications.

During CSM-ACE 2021, CyberSecurity Malaysia also unveiled two major initiatives to strengthen cyber resilience of 'Keluarga Malaysia' and business sectors. **The National Cyber Security Awareness Module (MKKSN),** which was jointly developed with MOE help in nurturing good cyber ethics in school children through increased cybersecurity awareness. Meanwhile, the **Cyber Security Enhancement Project for SME (PGPKS)**, set to benefit over 300 organisations, offer comprehensive cybersecurity health check to prevent Small and Medium Enterprise (SME) from cyber security threats.

Four (4) sector-specific events were also held in conjunction with **CSM-ACE 2021**, including Business Continuity & Disaster Recovery Symposium, Cisco Cyber Combat Session and BlockTech Forum 2021.

The cybersecurity landscape has changed drastically since the pandemic struck. We have witnessed how adversaries can harness the power of good to do harm. Cyber criminals attempting to steal corporate data and intellectual property are certainly not the only threat to businesses. Employees who are not well-versed in cyber security knowledge and information will continue to be a weak link in corporate IT security systems. It is critical that each and every stakeholder in our cybersecurity ecosystem must ensure that smart, resilient defenses are put in place to protect against evolving cyber threats.

Going forward, we have identified emerging cybersecurity challenges which will become major areas of focus for cybersecurity professionals across every sector from Industrial Internet of Things (IIoT) to 5G Networks and Artificial Intelligence (AI).

I would like to express my appreciation and gratitude to all my colleagues for their dedication and unwavering support in 2021. While I am hopeful that the worst of the pandemic is behind us, we must remain vigilant and steadfast in our duties to address rising cyber threats.

Let's continue to work together for a safer cyber space!

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

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

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

Azman Bin Ismail
Vice President,
Corporate Services Division

Jailany Bin Jaafar
Head, Legal & Secretarial/Company Secretary

REVIEW OF CORPORATE PERFORMANCE

There are 2 CyberSecurity Malaysia KPIs contributed to Ministry of Communication and Multimedia Malaysia (K-KOMM)

Deputy Secretary General Key Performance Indicator (TELECOMMUNICATION INFRASTRUCTURE AND DIGITAL ECONOMY)

ITEM	TARGET	ACHIEVEMENT	% ACHIEVED
1 Ensuring the Organization Undergoes Cyber Security Assessment / Certification According to Set Standards	33	33	100%

OUTCOME BASED BUDGETING (OBB) (PROGRAM PERFORMANCE MANAGEMENT FRAMEWORK- PPMF)

ITEM	TARGET	ACHIEVEMENT	% ACHIEVED
1 Percentage of incident/complaint resolution	90	91.84	100%

How We Performed Based on Corporate Key Performance Indicators (2021 KPI)

The following table are about the 2021 KPI – what were the indicators, and how we performed in relations to the targets.

KPI	Target	Achievement	%
SG 1 **Create Visible Contribution to Strategic Outcomes**			
1. # Trained knowledge workers	1,200	1,568	100
2. # Peoples reach out in Digital Economy community on Cyber Security Awareness Talk	20,000	32,412	100
3. # Visibility of program through events/programs	30	34	100
SG 2 **Provide Thought Leadership in Domain Expertise Areas**			
4. # Articles published in domain of cybersecurity	50	62	100
5. # Testing, accreditation, and certification	33	33	100
6. National and / or international recognition and awards	1	1	100
SG 3 **Deliver Quality and Impactful Services**			
7. % Customer satisfaction Leve	88	90	100
8. % Corporate website accessible	100	100	100
SG 4 **Grow Commercial Revenue**			
9. $ Mil Net Profit for Operation	16,000,000	13,856,779	86.60
SG 5 **Strengthen Solutioning and Innovation**			
10. # New products / services / applications	3	3	100
SG 6 **Improve Project and Client Management**			
11. % Digital Forensic Case Completed at CSM's end	90	70.20	78.00
12. % Cyber Incident Case Completed at CSM's end	90	92.70	100
13. % ISMS Compliance	90	96.04	100
SG 7 **Enhance Strategic and Industry Engagement**			
# Companies benefited from Cyber Security Industry Collaboration Program	3	3	100
SG 8 **Improve Project and Client Management**			
14. % Employee Engagement Satisfaction Level	78	76	97.44
15. % Staff aware on integrity Program	80	93.48	100

2020 Corporate KPI Achievement as of 31 December 2020 is: 97.63%

2021 CALENDER OF ACTIVITIES

JANUARY 2021

8 - 10 January 2021

CYBERSAFE™ IN SCHOOLS WORKSHOP - 2021 COLLABORATION PROJECT BETWEEN CYBERSECURITY MALAYSIA AND THE MINISTRY OF EDUCATION MALAYSIA

13 January 2021

18TH INTERNATIONAL BHURBAN CONFERENCE ON APPLIED SCIENCES & TECHNOLOGY (IBCAST-2021)

FEBRUARY 2021

3 February 2021

'TEMU MINDA' PROGRAM ON TV1 IN CONJUNCTION WITH SAFER INTERNET DAY (SID) 2021

27 February 2021

CYBER ETHICS TALK "TERLAJAK PERAHU BOLEH DIUNDUR, TERLAJAK POSTING'..... KAWALAN KENDIRI JADI PEGANGAN"

MARCH 2021

2 March 2021

MEMORANDUM OF UNDERSTANDING SIGNING CEREMONY BETWEEN CYBERSECURITY MALAYSIA AND AGENCY COUNSELING & MANAGEMENT CREDIT (AKPK), CYBERJAYA

5 March 2021

VISIT BY CHIEF EXECUTIVE OFFICER OF MALAYSIA DIGITAL ECONOMY CORPORATION (MDEC) TO CYBERSECURITY MALAYSIA

21 March 2021

MEMORANDUM OF UNDERSTANDING SIGNING CEREMONY BETWEEN CYBERSECURITY MALAYSIA AND UNIVERSITI MALAYSIA TERENGGANU (UMK), CYBERJAYA

22 March 2021

MEMORANDUM OF UNDERSTANDING SIGNING CEREMONY BETWEEN CYBERSECURITY MALAYSIA (CSM) AND MANAGEMENT & SCIENCE UNIVERSITY (MSU), CYBERJAYA

23 March 2021

SIBERKASA LAUNCHING CEREMONY, CYBERJAYA

23 March 2021

CYBER SECURITY COLLABORATION PROGRAMME (CCP) - "CYBER SECURITY DIALOGUE WITH INDUSTRY", CYBERJAYA

23 March 2021

CYBERSAFE™ L.I.V.E GALERI LAUNCHING CEREMONY , CYBERJAYA

30 March 2021

MEMORANDUM OF UNDERSTANDING SIGNING CEREMONY BETWEEN CYBERSECURITY MALAYSIA, CELCOM AXIATA, AND HUAWEI MALAYSIA

31 March 2020

'CYBER SECURITY ESSENTIAL' TRAINING COURSE

2 - 3 April 2021

CYBERSECURITY MALAYSIA JOB FAIR

24 April 2021

WEBINAR "EMPOWERING YOUR MINDSET WITH CYBER ETHICS" SEMPENA GIRL IN ICT (GICT) 2021

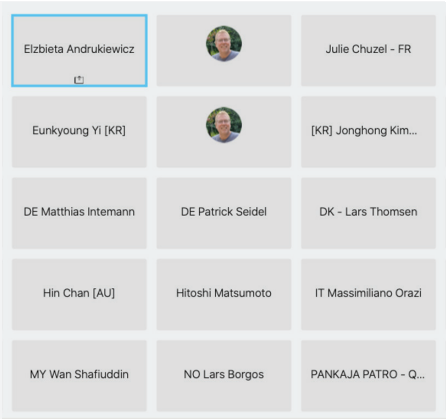
30 April 2021

PROGRAM CYBERSAFE™ BERSAMA MEDIA

MAY 2021

4 May 2021

MOCK COMPETITION OF NATIONAL ICT SECURITY DISCOURSE CYBERSAFE™ CHALLENGE TROPHY 2021 (VIRTUAL DISCOURSE)

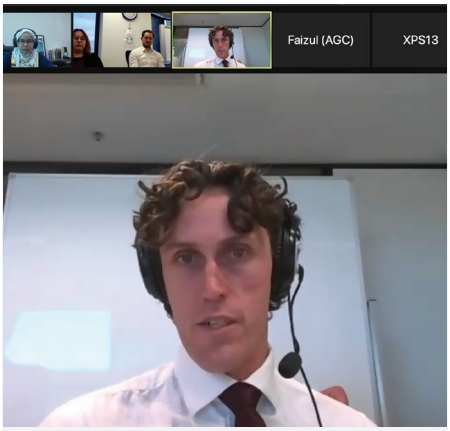


10 - 12 May 2021

COMMON CRITERIA ARRANGEMENT (CCRA) MEETING 2021

27 May 2021

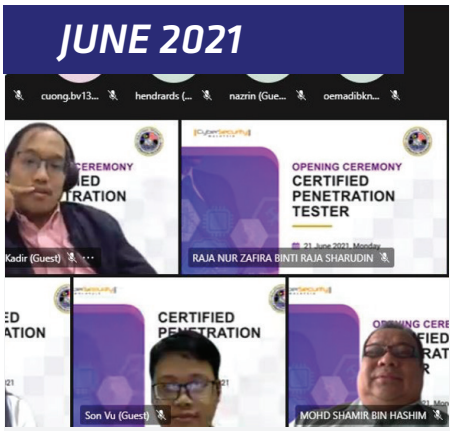
THE LAUNCHING CEREMONY OF NATIONAL ICT SECURITY DISCOURSE CYBERSAFE TM CHALLENGE CUP (VIRTUAL DISCOURSE)



31 May 2021

'CRYPTOCURRENCIES INVESTIGATION FROM AUSTRALIA'S PERSPECTIVE' SEMINAR

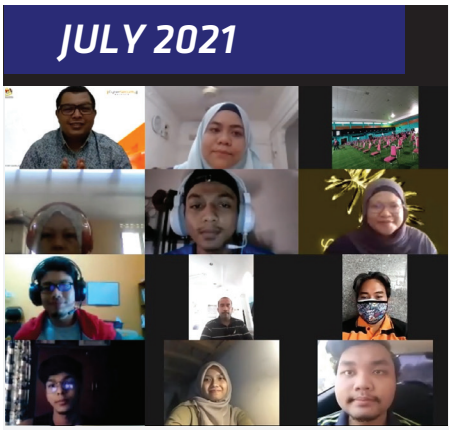
JUNE 2021



21 - 30 June 2021

MALAYSIAN TECHNICAL COOPERATION PROGRAMME 'CERTIFIED PENETRATION TESTER' TECHNICAL TRAINING

JULY 2021



14 - 15 July 2021

CYBER SECURITY AWARENESS PROGRAM FOR ENTREPRENUERS

29 July 2021

"CYBER SECURITY READINESS" ROUNDTABLE DISCUSSION WITH SOPHOS MALAYSIA

AUGUST 2021

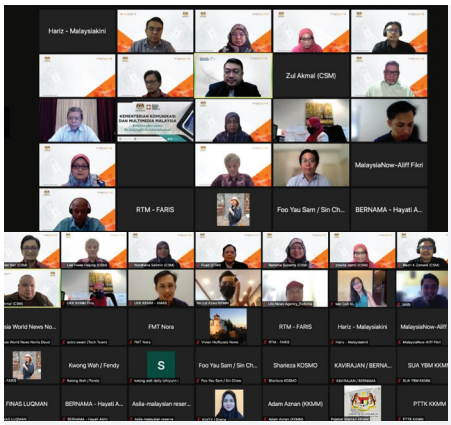
4 August 2021

CYBERTRONIUM FIRMWARE SECURITY WEBINAR - THREATS BELOW THE SURFACE IN HIGH RISK DEVICES WITH CYBERTRONIUM SDN BHD

AUGUST 2021

9 - 12 August 2021

CYBER FORENSIC TRAINING PROGRAM TO ASIA PACIFIC UNIVERSITY (APU)

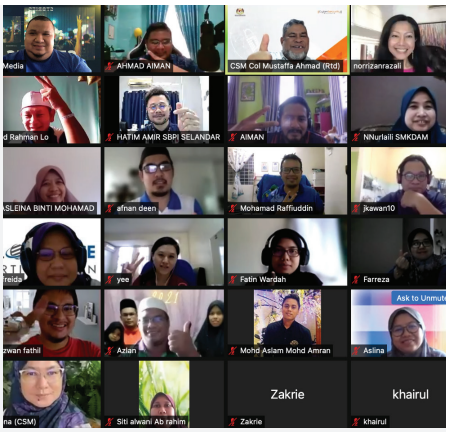


12 August 2021

"TURUN PADANG" PROGRAM, THE HONOURABLE DATO' SAIFUDDIN BIN ABDULLAH, MINISTER OF COMMUNICATIONS AND MULTIMEDIA WITH CYBERSECURITY MALAYSIA

27 August 2021

MEMORANDUM OF COOPERATION CEREMONY SIGNING BETWEEN CYBERSECURITY MALAYSIA AND NATIONAL FINANCIAL CRIME CENTRE (NFCC)



28 - 29 August 2021

CERTIFIED CYBERSECURITY AWARENESS EDUCATOR (CCASE) TRAINING PROGRAM

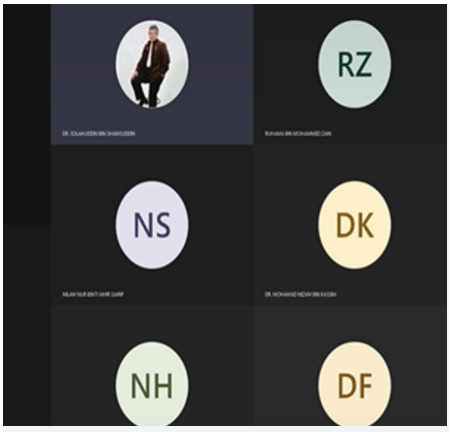
SEPTEMBER 2021

1 - 7 September 2021

CYBER FORENSIC TRAINING PROGRAM TO MANAGEMENT AND SCIENCE UNIVERSITY (MSU)

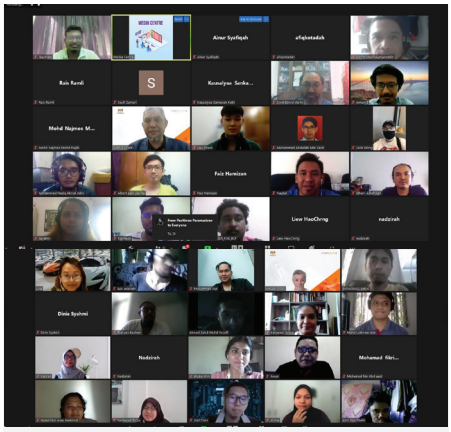
9 September 2021

VISIT BY THE HONOURABLE TAN SRI DATUK SERI PANGLIMA TPR ANNUAR HAJI MUSA MINISTER OF COMMUNICATION AND MULTIMEDIA TO CYBERSECURITY MALAYSIA



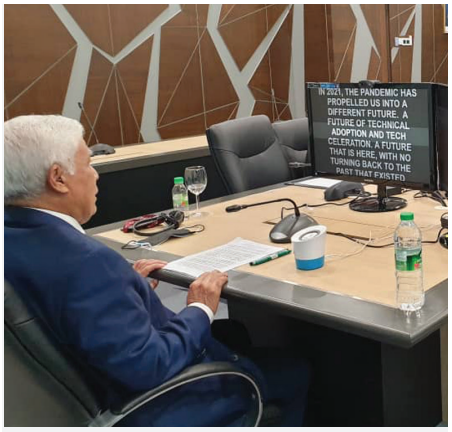
10 September 2021

KSA DESCRIPTOR REVIEW WORKSHOP



20 - 23 September 2021

PEMULIH SIBERKASA - CYBER SECURITY ESSENTIAL TRAINING



29 September 2021

ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM (APCERT) 2020 ANNUAL GENERAL MEETING

OCTOBER 2021

6 - 29 October 2021

NATIONAL ICT SECURITY DISCOURSE CYBERSAFE™ CHALLENGE TROPHY 2021 (NICTSeD) 2021 - VIRTUAL DISCOURSE, MENARA CYBER AXIS, CYBERJAYA

NOVEMBER 2021

1 November 2021

SIBERKASA OJT KICK-OFF DAY LAUNCHING CEREMONY, CYBER AXIS TOWER, CYBERJAYA

8 November 2021

MEMORANDUM SIGNING CEREMONY OF AGREEMENT BETWEEN CYBERSECURITY MALAYSIA & UNIVERSITI TEKNOLOGI MARA (UiTM), MENARA CYBER AXIS, CYBERJAYA

15 November 2021

GLOBAL ACE CERTIFICATION PROGRAM COLLABORATION DISCUSSION AND DELL NOTEBOOK PRESENTATION CEREMONY, CYBER AXIS TOWER, CYBERJAYA

15 - 17 November 2021

MALAYSIA FINANCIAL CRIME PREVENTION CONFERENCE 2021 (MFCPC'21), HOTEL EVERLY, PUTRAJAYA

17 November 2021

WORKING VISIT AND DISCUSSION ON COOPERATION BETWEEN CYBER SECURITY MALAYSIA AND UNIVERSITI TEKNIKAL MALAYSIA MELAKA (UTeM), MENARA CYBER AXIS, CYBERJAYA

22 November 2021

DIGITAL FORENSICS WORKING GROUP WORKSHOP, PUTRAJAYA

23 - 24 November 2021

13TH ANNUAL CONFERENCE OF THE ORGANISATION OF ISLAMIC COOPERATION - COMPUTER EMERGENCY RESPONSE TEAM (OIC-CERT)

23 November 2021

CYBER FORENSIC COLLOQUIUM 2021, HOTEL EVERLY, PUTRAJAYA

DECEMBER 2021

6 December 2021

GLOBAL ACE CERTIFICATION BOARD OF GOVERNANCE MEETING 1/2020, CYBERJAYA

7 December 2021

GRAND FINAL OF NATIONAL ICT SECURITY DISCOURSE – CYBERSAFE™ CHALLENGE TROPHY (NICTSED)2021, KUALA LUMPUR

9 - 12 December 2021

SOFT LAUNCH OF SIBERKASA TELEMOVIE AT ASPIRASI KELUARGA MALAYSIA 2021, KUALA LUMPUR

14 December 2021

CYBER SECURITY MALAYSIA – AWARDS, CONFERENCE & EXHIBITION (CSM-ACE) 2021, MENARA CYBER AXIS, CYBERJAYA

23 December 2021

CERTIFICATION REQUIREMENTS- "PEOPLE, PROCESS AND TECHNOLOGY CERTIFICATION: AN INSTRUMENT OF COMPLIANCE" WEBINAR, MENARA CYBER AXIS, CYBERJAYA

22 December 2021

GLOBAL ACE CERTIFICATION MEETING FOR THE FORMATION OF COUNTRY CHAPTERS WITH REPRESENTATIVES OF CIRT E-GOV BGD (BANGLADESH), CYBER AXIS TOWER, CYBERJAYA

ACHIEVEMENTS & AWARDS 2021

23 March 2021

CyberSecurity Malaysia launched SiberKASA,]an initiative to develop, empower, sustain and strengthen cyber security infrastructure and ecosystem in Malaysia to combat] complex and sophisticated cyber threats and cyber attacks.

29 September 2021

CyberSecurity Malaysia re-elected as a Steering Committee member (2021-2023) and the Chair of the Asia Pacific Computer Emergency Response Team (APCERT) for 2021-2022.

23 March 2021

CyberSAFE™ L.I.V.E. Galeri was recognised by The Malaysia Book of Records as "The First Cyber Security Gallery in Malaysia", a hub for research, training and disseminate cyber security knowledge in Malaysia as part of CyberSAFE Programme.

PROFESSIONAL CERTIFICATION

No	Name	Department	Certification
1	HAZLIN ABDUL RANI	CD	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
2	SUHAIRI MOHD JAWI	CD	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
3	NIK AZURA NIK ABDULLAH	CD	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
4	NORUL HIDAYAH LOT	CD	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
5	LIYANA CHEW NIZAM CHEW	CD	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
6	FARIDATUL AKHMA ISHAK	CD	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
7	ISMA NORSHAHILA MOHAMAD SHAH	CD	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
8	ZARINA MUSA	MYSEF	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
9	ALIFA ILYANA CHONG ABDULLAH	CAGI	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
10	NUR HASLAILY MOHD NASIR	CAGI	LEAD ASSESSOR, LABORATORY QUALITY MANAGEMENT SYSTEM: ISO/IEC 17025:2017
11	FAKHRUL AFIQ ABD AZIZ	DF	EC-COUNCIL CERTIFIED SECURITY ANALYST (ECSA)
12	FAISZATULNASRO MOHD MAKSOM	MYCERT	CompTIA CYBERSECURITY ANALYST (CYSA+)
13	KILAUSURIA ABDULLAH	MYCERT	CompTIA CYBERSECURITY ANALYST (CYSA+)
14	FARAH RAMLEE	MYCERT	CompTIA CYBERSECURITY ANALYST (CYSA+)
15	NUR QURRATU'AINI ROHIZAN	MYCERT	CompTIA CYBERSECURITY ANALYST (CYSA+)
16	LUKMAN HAKIM ABD RAHMAN	MYCERT	CompTIA CYBERSECURITY ANALYST (CYSA+)
17	FAKHRUL AFIQ ABD AZIZ	DF	CompTIA CYBERSECURITY ANALYST (CYSA+)
18	MUHAMMAD MUZAMMIL ABDUL RASHID	DF	CERTIFIED DIGITAL FORENSICS FIRST RESPONDER (CDFFR)
19	MUHAMMAD ISKANDAR SHAH ABDUL AZIZ	DF	CERTIFIED DIGITAL FORENSICS FIRST RESPONDER (CDFFR)
20	BALAMURUGAN S/O NALLAPAN	MD	CERTIFIED DIGITAL MARKETING SPECIALIST (CDMS)
21	MOHAMMAD FAHDZLI ABDUL RAUF	MD	CERTIFIED DIGITAL MARKETING SPECIALIST (CDMS)
22	ANISYAH SYAZWANI AHMAD SUPARMIN	MD	CERTIFIED DIGITAL MARKETING SPECIALIST (CDMS)

23	MOHD RIZAL BIN ABU BAKAR	ISCB	CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) AUDITOR/LEAD AUDITOR (BS ISO/IEC 27001:2013) (PR320)
24	OM NASHILA BINTI RAMLI	ISCB	CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) AUDITOR/LEAD AUDITOR (BS ISO/IEC 27001:2013) (PR320)
25	AMIROUL FARHAN ROSLAINI	ISCB	CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) AUDITOR/LEAD AUDITOR (BS ISO/IEC 27001:2013) (PR320)
26	SABARIAH AHMAD	ISMA	CERTIFIED INFORMATION SECURITY MANAGER (CISM)
27	MUHAMAD ZAIM MOHD ROZI	SRA	CERTIFIED INFORMATION SECURITY AWARENESS MANAGER (CISAM)

TECHNICAL PAPERS AND JOURNALS

No	Paper Title	Journal/ Conference Proceeding	Country	Date
1	A Study on Privacy Issues in Internet of Things (IoT)	Proceedings of the 5th International Conference on Cryptography, Security & Privacy 2021	USA	January 2021
2	Modifications of Key Schedule Algorithm on RECTANGLE Block Cipher	Proceedings of the International Conference on Advances in Cyber Security	Germany	February 2021
3	Lightweight Denial of Service (DoS) Detection System Algorithm (LIDSA)	Proceedings of the International Conference on Advanced Communications Technology	USA	February 2021
4	People, Process and Technology for Cryptocurrencies Forensics: A Malaysia Case Study	Proceedings of the International Conference on Advances in Cyber Security	Germany	February 2021
5	Compromising the Data Integrity of an Electrical Power Grid SCADA System	Proceedings of the International Conference on Advances in Cyber Security	Germany	March 2021
6	Developing Cyber Resilience Strategy for The Critical National Information Infrastructure Sectors in Malaysia	The University of Warwick, United Kingdom	United Kingdom	March 2021
7	Practical Guideline for Digital Forensics Laboratory Accreditation – A Case Study	OIC-CERT Journal of Cyber Security Volume 3 Issue 1	Malaysia	April 2021
8	The Integration of Cyber Warfare and Information Warfare	OIC-CERT Journal of Cyber Security Volume 3 Issue 1	Malaysia	April 2021
9	Cyberbullying via Social Media: Case Studies in Malaysia	OIC-CERT Journal of Cyber Security Volume 3 Issue 1	Malaysia	April 2021
10	Establishment of a Method to Measure the Awareness of OIC-CERT Members	OIC-CERT Journal of Cyber Security Volume 3 Issue 1	Malaysia	April 2021
11	Development of Examination Framework for Cyber Security Professional Competency Certification	OIC-CERT Journal of Cyber Security Volume 3 Issue 1	Malaysia	April 2021
12	New Vulnerabilities upon Grain v0 Boolean Function through Fault Injection Analysis	OIC-CERT Journal of Cyber Security Volume 3 Issue 1	Malaysia	April 2021
13	Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets	Proceedings of the 3rd International Cyber Resilience Conference	USA	April 2021
14	Comparison Multi Transfer Learning Models for Deep Fake Image Recognizer	Proceedings of the 3rd International Cyber Resilience Conference	USA	April 2021
15	A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology	Proceedings of the 3rd International Cyber Resilience Conference	USA	April 2021

16	Application of Knowledge-Oriented Convolutional Neural Network for Causal Relation Extraction in South China Sea Conflict Issues	Proceedings of the 3rd International Cyber Resilience Conference	USA	April 2021
17	News Event Prediction using Causality Approach on South China Sea Conflict	Proceedings of the 3rd International Cyber Resilience Conference	USA	April 2021
18	Formulation of Association Rule Mining (ARM) for an effective Cyber Attack Attribution in Cyber Threat Intelligence (CTI)	International Journal of Advanced Computer Science and Applications (IJACSA) - Volume 12 No 4 April 2021.	United Kingdom	April 2021
19	Security and Threats in the Internet of Things Based Smart Home	Book Chapter – Innovative Systems for Intelligent Health Informatics, Data Science, Health Informatics, Intelligent System, Smart Computing	Germany	May 2021
20	KSA for Digital Forensic First Responder: A job Analysis Approach	Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021	United Kingdom	June 2021
21	The Implementation of Hardware Security Based Zymkey 4i in HDVA	Proceedings of 2021 International Congress of Advanced Technology and Engineering (ICOTEN)	USA	July 2021
22	M-Health Digital Evidence Taxonomy System (MDETS): Enabling Digital Forensics Readiness with Knowledge Sharing Approach	Proceedings of International Conference on Information Technology and Digital Applications (ICITDA) 2021	Indonesia	November 2021
23	Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework	2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)-ICRAIE 2021	Malaysia	December 2021
24	Cyber Range Platform: Applications and Challenges	2nd International Recent Trends in Engineering, Advanced Computing and Technology, Perth, Australia (VIRTUAL CONFERENCE)	Australia	December 2021

EDITORIAL TEAM

SENIOR EDITORIAL TEAM
Roshdi Hj Ahmad , Lt. Col. Mustafa Ahmad, Mohd Shamil Mohd Yusoff

CONTENT CONTRIBUTOR
Yuzida Md Yazid, Azlin Samsudin, Norhuzaimi Mohamed, Ernieza Ismail, Mohd Rohaizad Mohd Ghazali, Alifa Ilyana Chong Abdullah, Azrina Md Saad

DIGITAL TEAM
Zul Akmal Abd Manan, Nurul 'Ain Zakariah, Zaihasrul Ariffin

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

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA