CyberSecurity MALAYSIA

ANNUAL REPORT 2025

SECURING TRUST . SHAPING TOMORROW

COVER RATIONALE

Securing Trust. Shaping Tomorrow

This cover visualises a connected and secure digital future, aligned with the theme “Securing Trust. Shaping Tomorrow”. The composition places a modern cityscape—anchored by iconic national landmarks—emerging from a smartphone, symbolising how technology has become the foundation of everyday life and national development. The integration of elements such as smart transportation, robotics, cloud computing, and renewable energy reflects the technological landscape of 2025, where innovations like artificial intelligence (AI), the Internet of Things (IoT), and automation are embedded seamlessly into society. The flowing digital pathways leading into the city represent the continuous movement of data, while the central security shield reinforces the importance of safeguarding this interconnected ecosystem.

By positioning the future within the palm of a hand, the design conveys both accessibility and responsibility—highlighting how individuals, organisations, and nations collectively shape a secure digital environment. The clean and balanced visual style underscores professionalism and trust, reinforcing CyberSecurity Malaysia’s role in driving a resilient, forward-looking cybersecurity landscape.

Disclaimer
Some illustrations and visual assets in this Annual Report were generated using artificial intelligence (AI) to enhance storytelling and visual communication. These images are for illustrative purposes only and do not depict actual events, individuals, or locations.

Advancing cybersecurity, strengthening resilience, and enabling trusted digital innovation

INTRODUCTION

- Design & Cover Rationale.....2
- About CyberSecurity Malaysia.....5
- History.....6
- Our Products & Services.....8

CORPORATE GOVERNANCE

- The Board Of Directors.....18
- Corporate Governance.....20
- Notice of Annual General Meeting.....25
- Form Of Proxy.....27

OPERATIONAL REVIEW

- Foreword from the CEO.....30
- The Management Committee.....32
- Review of Corporate Performance.....33
- 2025 Calendar of Activities.....35
- Digital Voices.....50
- Achievement and Awards 2025.....56
- Professional Certifications.....60
- Editorial Committee.....66
- Social Media.....67

CyberSecurity Malaysia is the national cybersecurity specialist agency under the purview of the Ministry of Digital.

ABOUT CYBERSECURITY MALAYSIA

With effect from 10 January 2024, CyberSecurity Malaysia is placed under the Ministry of Digital. 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:

Cyber Security Responsive Services

CyberSecurity Malaysia provides responsive services to help organisations manage and recover from cyber incidents effectively. These services include incident response, digital forensics, malware analysis, and technical advisory to minimise the impact of cyber threats and ensure business continuity.

Cyber Security Proactive Services

CyberSecurity Malaysia helps organisations strengthen their cybersecurity readiness through proactive services such as security assessments, penetration testing, and threat monitoring. These efforts help identify vulnerabilities early and reduce exposure to cyber risks.

Pre-Emptive Technology & Services

CyberSecurity Malaysia develops and supports advanced cybersecurity technologies and solutions to address emerging cyber threats. Through innovation, research, and cyber intelligence, the agency enhances national preparedness and strengthens digital resilience.

Outreach and Capacity Building

CyberSecurity Malaysia promotes cybersecurity awareness and talent development through training programmes, awareness campaigns, and community engagement initiatives. These efforts help build a safer and more cyber-aware digital society.

Strategic Study and Engagement

CyberSecurity Malaysia conducts strategic studies and collaborates with government agencies, industry players, academia, and international partners to support national cybersecurity initiatives, policies, and long-term digital resilience.

Industry and Research Development

CyberSecurity Malaysia supports the growth of the national cybersecurity ecosystem through research, innovation, and industry collaboration. These initiatives help strengthen local expertise, encourage innovation, and advance the nation's digital economy.

An unquenchable faith to achieve more than the miracles of technology and the promise of future accomplishments

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 Reponse 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 (NSCP) led by MOSTI. NISER was mandated to provide technical support for NCSP implementation and was rebranded to CyberSecurity Malaysia reflecting its wider mandate and larger role. On 20 August 2007, the Prime Minister of Malaysia officiated CyberSecurity Malaysia and launched its new logo.

1997

13 Jan 1997

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

2001

10 April 2001

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

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)(www.mimos.my)

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

2018

19 October 2018

The Cabinet Meeting chaired by the Prime Minister of Malaysia decided CyberSecurity Malaysia to be placed under the Ministry of Communication and Multimedia Malaysia (KKMM)

2024

10 January 2024

The Cabinet Meeting chaired by the Prime Minister of Malaysia decided that CyberSecurity Malaysia to be placed under the Ministry of Digital

OUR PRODUCTS & SERVICES

With the vision to become a world-class cybersecurity specialist agency, our mission is to lead 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

CyberSecurity Malaysia pursues this mission through SiberKASA, a comprehensive framework that develops cybersecurity solutions by virtue of the three elements of People, Process, and Technology.

The SiberKASA framework is developed based on our six core services:

- Cybersecurity Responsive Services
- Cybersecurity Proactive Services
- Pre-emptive Technology & Services
- Outreach and Capacity Building
- Strategic Study and Engagement
- Industry and Research Development

The following is a distilled overview of our six core services and some examples of the services and products that are offered.

Cybersecurity Responsive Services

Compromise Assessment - Host Assessment

A focused security evaluation conducted on individual computing systems (hosts) within a network. These hosts can include servers, workstations, laptops, or any other network-connected devices with an operating system. The assessment aims to identify security vulnerabilities and misconfigurations specific to each machine.

Compromise Assessment: Cyber Health Assessment (Network Compromise Assessment)

Cyber Health Assessment (CHA) is conducted using CMERP Insight (INSIGHT), a Breach Detection System (BDS) designed to detect malicious and suspicious activities within a network following a security breach. INSIGHT serves as a monitoring solution that alerts organisations to potential threats, enabling timely responses to harmful activities.

CSIRT Consultancy

Computer Security Incident Response Team (CSIRT) Consultancy offers specialised expert services to organisations in the areas of people, processes, and technology. This consultancy creates tailored implementation plans to help develop and establish a CSIRT within organisations. Additionally, the service provides Incident Handling and Network Security training, job attachments, and professional memberships with the Forum of Incident Response and Security Teams (FIRST), Asia Pacific Computer Emergency Response Team (APCERT), and the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OICCERT) OIC-CERT.

Cyber Incident Response Plan Consultancy

Consultancy service to help organisations build or enhance their cyber incident response plan and strategy.

2nd and 3rd Level Incident Response Support

Deep-dive technical support for complex or escalated incidents.

System and Network Log Analysis

Analysis of system/network logs to detect anomalies and the root cause of incidents.

Cybersecurity Proactive Services

CyberDEF (Defense, Eradication & Forensics)

To assist organisation by providing solution, proactive and responsive steps to eradicate and remediate security threats and vulnerabilities (Root Cause Analysis).

Expert Development & Consultation

Digital Forensics Quality Management System Expert Consultation.

CyberDISCOVERY

Specialised cyber forensics service offered to both individuals and private organisations. It is designed to address concerns related to Electronically Stored Information (ESI) as digital evidence, particularly within the context of civil litigation. The service focuses on uncovering critical information and provide clear, defensible answers to support legal proceedings.

CyberDiscovery offers the following services:

1. **Onsite Evidence Collection and Preservation** Secure acquisition and safeguarding of digital evidence from electronic devices and storage media, ensuring chain-of-custody compliance.

2. **Evidence Examination and Analysis** In-depth forensic analysis of collected data to identify, interpret, and reconstruct relevant digital activities.

3. **Expert Witness Testimony** - Provision of qualified forensic experts to present findings and opinions in court, supporting legal arguments with professional credibility.

CyberDiscovery upholds the highest standards of integrity, confidentiality, and forensic best practices, delivering reliable and court-admissible results.

ISMS Guidance Series

Information Security Management Consulting provides expert guidance to organisations in protecting and preserving the confidentiality, integrity, and availability of their information and information systems through the implementation of an Information Security Management System (ISMS) in accordance with the ISO/IEC 27001 standard.

Customised Information Security Management Services

Tailored Information Security Management related services designed to address ISO/IEC 27001 requirements e.g., determination of ISMS scope, risk assessment, implementation of controls and general information security assessment.

DPMA – Data Privacy Management Assessment

A web-based assessment tool that helps organisations assess their data privacy governance, readiness, and compliance,

and identify implementation gaps, based on the ISO/IEC 27701 Privacy Information Management System (PIMS).

DPGP - Data Privacy Guard Pro

is an evaluation and testing for ICT / IoT product or application, based on data protection requirements outlined in Malaysia's Personal Data Protection Act (PDPA) and international best practices. It is also aligned with relevant ISO data privacy standards. DPGP evaluates how a product manages personally identifiable information (PII) throughout its lifecycle, including the functional roles involved, to guarantee strong privacy protection for the product.

DPIA- Data -Protection Impact Assessment

assists organisations in assessing the potential impacts on privacy of processes, information systems, programmes, software modules, devices, or other initiatives that handle Personally Identifiable Information (PII). It also identifies necessary actions in order to treat privacy risk. The DPIA is developed based on ISO/IEC 29134 Guidelines for Privacy Impact Assessment.

PJuRA – Privacy Jurisdiction Risk Assessment

helps organisations assess their data protection practices against both local and international privacy laws. This structured assessment identifies risk exposure across different legal jurisdictions and highlightis potential compliance gaps. By understanding these risks, organisations can strengthen their data protection measures and build greater customer trust by demonstrating their commitment to data security and privacy.

MyKripto Validation

A security validation and analysis service that includes:

- Cryptanalysis of cryptographic algorithms to assess their security strength.
- Conformance testing of cryptographic algorithms against a standard document.
- Evaluation of the randomness characteristics of a random number generator.
- Cryptographic S-Box Testing checks the strength of encryption's core to ensure they resist codebreaking.

Malaysia's National Trusted Cryptographic Algorithm List (MySEAL)

MySEAL establishes requirements and guidelines for trusted cryptography products in Malaysia, aligning with the National Cryptography Policy to achieve cryptographic sovereignty and support cryptographic science; it provides a list categorising algorithms into AKSA (Existing Cryptographic Algorithms) and AKBA (New Cryptographic Algorithms), with comprehensive evaluation criteria overseen by a committee led by CyberSecurity Malaysia, marking a significant milestone since Malaysia's National IT Agenda in pursuing information security fundamentals.

Blockchain Security Verification

A service that validates and verifies the security properties of a blockchain and smart contract applications. With this, businesses gain insight into their overall blockchain and smart contract security posture, as well as the ability to address any potential flaws in their blockchain based solutions or applications.

FIPS 140-3 Cryptographic Module Validation

CyberSecurity Malaysia operates a Federal Information Processing Standard (FIPS) Publication 140 testing laboratory that provides independent technical services in the field of cryptographic algorithm testing and verification testing of cryptographic module software and hardware.

FIPS 140-3 Cryptographic Training

Gain a competitive edge with our FIPS 140-3 Cryptographic Training, designed to provide in-depth knowledge of cryptographic module validation in alignment with ISO/IEC 19790 and ISO/IEC 24759 standards.

Cybersecurity Evaluation and Testing

Conduct the evaluation and testing of ICT products and Protection Profiles (PP) using the Common Criteria Methodology (based on ISO/IEC 15408 and ISO/IEC 18045) for certification under the MyCC scheme.

ICT Product Security Assessment (IPSA)

A security functional testing and/or vulnerability assessment and penetration testing service for ICT products.

Cloud Security Evaluation

Evaluation and testing of products developed and operated on cloud computing platforms, managed by Cloud Service Providers (CSP) for Platform as a Service (PaaS) and Software as a Service (SaaS).

Expert Consultancy

We provide expert consultancy services for the development of ISO/IEC 17025 laboratories to offer Common Criteria evaluation services.

Cloud Security Audit

Cloud Security Audit services for cloud computing platforms, managed by Cloud Service Providers (CSP) for Platform as a Service (PaaS) and Software as a Service (SaaS), based on the security requirements stated in ISO/IEC 27017 and ISO/IEC 27002.

Facility Rental

Rental of ISO 17025 Accredited testing facilities, equipment and resource to the public and private organisations to conduct cybersecurity evaluations or testing in a controlled environment.

CyberSOC

Provides Manage, Detect & Response (MDR) services that monitor, analyse, detect, and protect against potential cyberattacks. The service covers endpoints such as servers, workstations and laptops.

Lebahnet

Lebahnet, based on Honeypot technology, provides valuable insights into network trends and malicious activities, supporting MyCERT in incident handling and advisory services. Honeypots are systems designed to simulate legitimate sites, luring malicious software by appearing vulnerable. This approach allows cybersecurity researchers to detect, monitor, and counteract malicious activities by analysing actions during the intrusion phase and examining attack payloads.

Cyber Drill Exercise

CyberDrill is an activity conducted to assess an organisation's cyber capacity by evaluating its ability to detect and respond to security incidents. This follows a defined methodology and is executed using various tools and infrastructure provided by CyberSecurity Malaysia. During the simulated cyber drill exercise, organisation's readiness is tested based on their existing cyber security incident response procedures, allowing for the identification of areas for improvement.

Incident Response Playbook Development

Creation of tailored response procedures for various incident types.

Vulnerability Assessment and Penetration Testing (VAPT)

A critical service provided to both public and private organisations to identify and address security weaknesses within their IT environment. This comprehensive service involves a detailed assessment of the system to uncover vulnerabilities and potential entry points that could be exploited by cyber threats.

Security Posture Assessment (SPA)

Identifies security vulnerabilities within an organisation based on internationally recognised standards, including the Open Worldwide Application Security Project (OWASP), Open Worldwide Application Security Project (OSSTMM), and PCI Security Standards Council (PCI-DSS) to help prevent breaches, reduce the impact of any incidents, and protect organisational reputation.

Mobile App Security Assessment

Identifies security weaknesses in mobile applications, devices, and operating systems and evaluates risks such as data leaks, insecure Application Programming Interface (APIs), weak authentication, and malware.

Technology Security Assurance (TSA)

A national scheme initiated by CyberSecurity Malaysia. It is an assurance where ICT products are evaluated based on Mandatory Security Functional Requirements (MSFRs) developed by the Information Security Certification Body (ISCB).

MyCC Certification

MyCC Scheme assists in raising the quality and competitiveness level of Malaysian ICT products, benchmarked against global Common Criteria requirements.

Business Continuity Management System (BCMS) Certification

The scheme is based on the ISO 22301 international standard for organisation that envisions for resiliency. It helps to plan an effective business continuity management to protect against, reduce the likelihood of, and ensure business recovers from disruptive incidents. This is in line with the national requirement towards creating a resilient National Critical Information Infrastructure (NCII).

Penetration Test Service Provider Scheme (PTSP)

PTSP ensures penetration testing service is delivered by local cyber security consulting companies that are meeting the requirement set by CyberSecurity Malaysia.

Malaysian Cryptography Validation (MyCV) Scheme

MyCV is a national scheme for validating and certifying the Cryptographic Module Validation (CMV) and the Cryptographic Algorithm Validation (CAV) services based on ISO/IEC 19790 and ISO/IEC 24759 standard and also to supports Dasar Kriptografi Nagara (DKN) or National Cryptography Policy (NCP) implementation.

Mobile Application Certification (MAC)

Mobile application assessment to ensure mobile applications meet the established required cybersecurity criteria.

Information Security Privacy Management System (ISPMS)

ISO/IEC 27701:2019 is a privacy extension to ISO/IEC 27001. The goal is to enhance the existing Information Security Management System with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System. The standard outlines a framework for Personally Identifiable Information Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals. ISO/IEC 27701 is intended to be a certifiable extension to ISO/IEC 27001 certifications.

ISMS Certification

The CSM27001 Scheme supports the National Security and Public Safety pillar under the Economic Transformation Programme (ETP) by enhancing the resilience of both the National Critical Information Infrastructure (NCII) and the broader industry. Additionally, the scheme contributes to the Catalyst for Industry Growth pillar by enabling ISO/IEC 27001-certified organisations to benchmark themselves against global standards, thereby enhancing their competitiveness in the international market.

Pre-emptive Technology & Services

Offensive Security Surface Risk Intelligence

Evaluates exposed assets of an organisation, including networks, systems, and applications, to identify and prioritise vulnerabilities that could be exploited by attackers. This proactive approach helps mitigate risks by addressing weaknesses before they are exploited.

Offensive Intelligence - Digital Exposure Monitoring

Continuously tracks online footprint of an organisation, including publicly accessible systems, leaked data, and potential vulnerabilities, to understand how adversaries might target them. It enables organisations to stay ahead of threats by monitoring and mitigating exposures in real-time.

SiberBlok / Automated Threat Prevention

Detects, analyses, and responds to cybersecurity threats in real-time by monitoring network traffic for malicious activities. It quickly blocks or mitigates threats, reducing response time, minimizing human error, and strengthening overall security resilience.

Offensive Security - Vulnerabilities Exploitation Analysis

Identify vulnerabilities and test their exploitability to assess potential impact of an attack. This analysis provides actionable insights to address weaknesses and strengthen overall security posture.

Behavioural Competency Assessment (BCA)

Information security personnel is an instrument that assess the behavioural elements that contribute to a culture of high performance, which can be observed through people's actions and behaviours. Utilising psychometric science and methods, BCA can effectively complement.

Outreach & Capacity Building

CyberSAFE®

CyberSAFE® (Cyber Safety Awareness for Everyone) is a public awareness programme developed by CyberSecurity Malaysia to educate and empower the general public on the importance of cybersecurity and to promote a safer digital environment for all.

CyberGURU

CyberGURU is a dedicated platform for nurturing information security practitioners and advancing cyber security professional development through a wide range of competency based training programmes and certifications. The platform also promotes knowledge sharing by engaging leading industry experts, academicians, and policymakers, while fostering both local and international collaborations.

CyberGURU offers a diverse portfolio of competency and professional certification courses tailored to meet the evolving demands of the cyber security landscape. These include training tracks ranging from fundamentals to advanced certifications in areas such as Incident Handling, Digital Forensics, Security Assessment, Cryptography, Common Criteria, and Security Management.

Global ACE Certification

A national certification scheme designed to strengthen Malaysia's cyber security capacity and capability by recognising and certifying qualified personnel. The framework is aligned with international standards, including ISO/IEC 17024 for personnel certification, ISO/IEC 9000 for quality management processes, and ISO/ IEC 27001 for information security management.

Strategic Study & Engagement

Strategic Study

Strategic study provides:

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

Government Engagement

Government Engagement provides:

- Strategic engagement services with stakeholders within the Malaysian Government.
- Administrator for the Critical National Information Infrastructure (CNII) portal.

International Engagement

International Engagement provides:

- Multilateral relations service to enhance cyber security corporation globally
- To establish and support cross border collaboration, bilateral and multilateral platforms in the effort to achieve a safe and secured cyber space.
- Corporation globally among the Computer Emergency Response Teams (CERTs), World Trustmark Alliance (WTA) and other information security organisations

Industry & Research Development

CyberSecurity Malaysia Collaboration Program (CSM-CP)

A strategic initiative designed to foster collaboration between CyberSecurity Malaysia and the local cyber security industry, as well as other government entities. The programme aims to encourage the development and innovation of Malaysia's cyber security products and services. Through CSM-CP, participants gain access to potential collaborations and synergies not only with CyberSecurity Malaysia, but also with relevant government agencies and fellow collaborators. The programme leverages partners' strengths and helps bridge market gaps by supporting the creation of high-quality, locally relevant cyber security solutions.

MyCyberSecurity Clinic (MyCSC)- Data Recovery and Data Sanitisation Services offers trustworthy and convenient data recovery and data sanitisation services, ensuring that all data is handled in a safe, secure, and confidential manner.

- **Data Recovery Services:** Designed to retrieve data from digital storage media that are damaged, failed, corrupted, or otherwise inaccessible. Our expert team uses advanced techniques to maximise the chances of successful recovery while maintaining data integrity.
- **Data Sanitisation Services:** Provide organisations with a reliable solution for the secure and permanent deletion of data from storage devices that are being retired, upgraded, or repurposed. This helps prevent data leakage and ensures compliance with data protection policies.

Our services are aligned with industry best practices to support your organisation's data lifecycle management needs with confidence and peace of mind.

BOARD OF DIRECTORS

The Board of Directors of CyberSecurity Malaysia helps lead the organisation by providing guidance and making key decisions. Their leadership has played an important role in keeping the agency focused on its mission to protect Malaysia's digital space and ensure a safer online environment for everyone.

Al-Ishsal Bin Prof. Dato' Ishak T. Kechik

Chairman

Tuan Fabian Bigar

Secretary General,
Ministry of Digital

Director

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab FASc

Chief Executive Officer

Director

Derek John Fernandez

Director

Norhayati binti Masah

Director

Dato' Sri Mohd Kamarudin bin Md Din

Director

Datuk Hj Rostam Affendi bin Dato' Hj Salleh

Director

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.

The Human Resources and Remuneration Committees (HRRC)

Objectives

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

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 organisational structure for the Company.
- To review potential candidates for hiring and promotion for the Top Management positions of the Company.

Members:

- YBhg. Datuk Fabian Bigar (Chairman).
- YBhg. Dato' Sri Mohd Kamarudin bin Md Din (Member).
- YBhg. Datuk Haji Rostam Affendi bin Dato' Haji Salleh (Member).

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.

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.

Audit, Governance and Integrity Committee (AGI)

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.

Governance and Integrity

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

Members:

- YBrs. Puan Norhayati Binti Masah (Chairman)
- YBrs. Encik Derek John Fernandez
- YBhg. Datuk Ts. Dr. Fazidah binti Abu Bakar (cessation of appointment with effect from 5 June 2025)
- YBrs. Encik Shaifubahrim bin Mohd Saleh (cessation of appointment with effect from 25 June 2025)
- YBhg. Dato' Sri Mohd Kamarudin bin Md Din (appointment effective from 19 December 2025)

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 organisation. 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.

In accordance with the Constitution of CyberSecurity Malaysia, the Board comprises Government Directors representing ministries or agencies of the Government of Malaysia and Other Directors who possess relevant industry expertise, professional competence, or distinguished public service experience. The composition of the Board, including the ratio of Government Directors to Other Directors, is determined by the Supervising Ministry from time to time. All Board appointments are subject to the prior consent of the Supervising Ministry and the approval of the Registrar of Companies, Companies Commission of Malaysia (SSM). Currently, the Board of CyberSecurity Malaysia comprised six (6) members, consisting of two (2) Government Directors and four (4) Other Directors, including the Chairman.

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.

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

NOTIS MESYUARAT AGUNG TAHUNAN KE-20

DENGAN INI DIMAKLUMKAN BAHAWA Mesyuarat Agung Tahunan kali ke-20 CyberSecurity Malaysia (CSM) Tahun 2026 akan diadakan secara maya melalui penstriman langsung dari lokasi siaran di CyberSecurity Malaysia, Bilik Jati, Level 10, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor pada hari Isnin, 22 Jun 2026, jam 11.30 pagi untuk membincangkan urusan-urusan berikut

URUSAN BIASA		
1.	Untuk menerima Penyata Kewangan Beraudit bagi tahun kewangan berakhir 31 Disember 2025 berserta laporan 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 RM240,000 dan manfaat lain bermula dari tarikh AGM ke-20 sehingga AGM CyberSecurity Malaysia bagi tahun yang berikutnya. (Rujuk nota keterangan 2)	Resolusi 1
3.	Untuk melantik semula Pengarah-pengarah berikut yang akan bersara mengikut giliran menurut Artikel 54 Perlembagaan CyberSecurity Malaysia, dan oleh kerana layak, menawarkan diri mereka untuk dilantik semula; 3.1 YBhg. Dato' Sri Mohd Kamarudin bin Md Din; dan 3.2 YBhg. Datuk Haji Rostam Affendi bin Dato' Haji Salleh. (Rujuk nota keterangan 3)	Resolusi 2
NOTIS MESYUARAT AGUNG TAHUNAN KE-20		
4.	Untuk melantik Tetuan MHA Associates (Dahulunya dikenali sebagai Tetuan Atarek Kamil Ibrahim & Co.) sebagai Juruaudit CyberSecurity Malaysia bagi tahun kewangan berakhir 31 Disember 2026 dan memberi kuasa kepada Lembaga Pengarah untuk menetapkan imbuhan mereka. (Rujuk nota keterangan 4)	Resolusi 4
5.	Untuk melaksanakan apa-apa urusan lain yang mana notis sewajarnya telah diberikan mengikut Akta Syarikat 2016 dan Perlembagaan CyberSecurity Malaysia.	

MENURUT PERINTAH LEMBAGA PENGARAH

JAILANY BIN JAAFAR
LS0008843
SSM PC No. 201908002687
Setiausaha Syarikat

Selangor Darul Ehsan
Tarikh: 29 Mei 2026

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 vang 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 it menurut Seksen 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 Berdaftar 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 2025

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 Anggota syarikat.

2. Bayaran elaun bulanan

Bayaran elaun bulanan Pengerusi bukan Eksekutif dan Pengarah bukan Eksekutif berjumlah sehingga RM240,000 dan manfaat lain yang perlu dibayar kepada Pengerusi dan Pengarah Bukan Eksekutif di bawah perkara 2.

3. Pemilihan semula Pengarah yang akan bersara menurut Artikel 54

YBhg. Dato' Sri Mohd Kamarudin bin Md Din dan YBhg. Datuk Haji Rostam Affendi bin Dato' Haji Salleh, telah dilantik menjadi Pengarah pada 10 Oktober 2025. Kedua-dua Pengarah tersebut hanya akan menjawat jawatan sebagai Pengarah untuk tempoh sehingga AGM ke-20 ini dan selepas itu menurut Artikel 54 Perlembagaan CyberSecurity Malaysia, kedua-dua Pengarah boleh dilantik semula sebagai Pengarah dan Pengerusi CyberSecurity Malaysia.

Berdasarkan Artikel 54 Perlembagaan CyberSecurity Malaysia, Pengarah-pengarah tersebut adalah layak untuk dilantik semula melalui resolusi AGM 2026 ini.

Kedua-dua Pengarah tersebut telah bersetuju untuk dilantik semula sebagai Pengarah CyberSecurity Malaysia.

4. Pelantikan Juruaudit Kewangan Luar

Lembaga Pengarah CyberSecurity Malaysia di mesyuaratnya pada 14 Mei 2026 telah meluluskan untuk mengesyorkan pelantikan Tetuan MHA Associates (Dahulunya dikenali sebagai Tetuan Atarek, Kamil & Co.) sebagai juruaudit kewangan luar CyberSecurity Malaysia untuk kelulusan Anggota 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 kali ke-20 CyberSecurity Malaysia Tahun 2026 yang akan berlangsung secara maya melalui penstriman langsung dari lokasi siaran di Bilik Jati, Level 10 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor pada hari Isnin, 22 Jun 2026 jam 11.30 pagi atau pada sebarang penangguhan, seperti yang tertera di bawah :

RESOLUSI	BERSETUJU	TIDAK SETUJU
PERKARA 1 Menerima Penyata Kewangan yang telah diaudit bagi tahun kewangan berakhir 31 Disember 2025, berserta laporan-laporan Pengarah dan Juruaudit.		
RESOLUSI 1 Meluluskan pembayaran elaun bulanan Pengerusi Bukan Eksekutif dan Pengarah bukan Eksekutif berjumlah sehingga RM240,000 dan manfaat lain bermula dari tarikh AGM ke-19 sehingga AGM CyberSecurity Malaysia bagi yang berikutnya.		
RESOLUSI 2 Melantik semula Pengarah berikut, yang akan bersara mengikut giliran menurut Artikel 54 Perlembagaan CyberSecurity Malaysia dan oleh kerana layak, telah menawarkan diri untuk dilantik semula; a) YBrs. Tuan Al-Ishsal bin Ishak b) YBrs. Encik Derek John Fernandez c) YBrs. Puan Norhayati binti Masah		
RESOLUSI 3 Melantik Tetuan Atarek Kamil Ibrahim & Co. sebagai Juruaudit CyberSecurity Malaysia bagi tahun kewangan berakhir pada 31 Disember 2025 dan memberi kuasa kepada Pengarah bagi menetapkan imbuhan mereka.		
PERKARA 2 Melaksanakan apa-apa urusan lain yang mana notis sewajarnya telah diberikan mengikut Akta Syarikat 2016 dan Perlembagaan CyberSecurity Malaysia.		

Sila tandakan “X” dalam ruang yang disediakan di atas untuk menandakan pilihan anda. Jika tiada arahan tertentu, proksi akan mengundi atau tidak mengundi mengikut budi bicaranya.

Bertarikh ..... haribulan 2025

.....
Tandatangan Anggota/Meterai

OPERATIONAL REVIEW

As a trusted enabler of digital security and innovation, our operational journey throughout the year reflects the collective efforts of our leadership, people and technology in delivering value to stakeholders. Guided by our commitment to securing trust and shaping tomorrow, we continued to strengthen organisational performance, foster meaningful engagement, drive innovation and build future-ready capabilities.

This section highlights the key milestones, achievements and initiatives that defined our year — from strategic leadership and operational performance to stakeholder engagement, industry recognition and professional development. Together, these efforts reinforce our role in advancing a secure, resilient and trusted digital ecosystem.

FOREWORD FROM THE CEO

Every innovation creates new possibilities. Every possibility demands trust. At CyberSecurity Malaysia, we are committed to safeguarding both.

The year 2025 marked another defining chapter in Malaysia's digital transformation journey. As artificial intelligence, cloud computing, digital platforms, and interconnected technologies became increasingly embedded across government, industry, and society, cybersecurity evolved from a technical necessity into a strategic enabler of national progress. In this rapidly changing environment, trust, security, and resilience have become fundamental pillars underpinning sustainable digital growth and economic prosperity.

The accelerating adoption of generative artificial intelligence (AI), intelligent automation, and data-driven services has unlocked unprecedented opportunities to enhance productivity, strengthen competitiveness, and drive innovation across all sectors. Yet these advancements have also introduced new complexities and vulnerabilities. Cyber threats today are more sophisticated, persistent, and far-reaching than ever before, targeting not only networks and information systems but also digital identities, critical infrastructure, supply chains, operational technologies, and AI-enabled ecosystems. The rise of ransomware operations, AI-assisted cybercrime, and increasingly sophisticated disinformation campaigns underscores the need for continuous vigilance, adaptive governance, and stronger collective resilience.

Against this backdrop, CyberSecurity Malaysia continued to play a pivotal role in advancing the nation's cybersecurity agenda. As the national cybersecurity specialist agency under the Ministry of Digital, we remained steadfast in strengthening cyber resilience, enhancing digital trust, protecting critical information infrastructures, and supporting the secure adoption of emerging technologies. Through our technical expertise, advisory services, digital forensics capabilities, capacity-building initiatives, and public awareness programmes, we continued to support the nation's aspiration to build a secure, resilient, and trusted digital ecosystem.

Building a secure digital future, however, extends beyond technology alone. It requires a cyber-aware society, a highly skilled workforce, robust governance frameworks, and strong partnership across sectors. Throughout the year, we intensified efforts to strengthen national capabilities through cybersecurity awareness initiatives, professional development programmes, research and innovation activities, strategic collaborations, and industry engagement. These efforts are essential in fostering a culture of shared responsibility and ensuring that cybersecurity remains embedded within Malaysia's broader digital transformation agenda.

Malaysia's ASEAN Chairmanship in 2025 further reinforced the importance of regional and international cooperation in addressing shared cyber challenges. As cyber threats continue to transcend geographical boundaries, no nation can tackle them in isolation. The Chairmanship provided valuable opportunities to advance regional dialogue and collaboration on cybersecurity, digital trust, artificial intelligence governance, and emerging technology risks. Strengthening partnerships, advancing information-sharing programmes, and fostering collective action remain critical to building a more secure and resilient digital future for the region.

The theme of this Annual Report, "Securing Trust. Shaping Tomorrow.", reflects a conviction that has guided our work throughout the year. Trust is the foundation upon which digital transformation succeeds. It empowers individuals to embrace technology with confidence, enables organisations to innovate responsibly, and allows nations to realise the full potential of the digital economy. As technology continues to evolve at an unprecedented pace, safeguarding that trust becomes both a strategic imperative and a shared responsibility.

As we reflect on the achievements of 2025, I would like to express my sincere appreciation to our stakeholders, strategic partners, industry collaborators, government agencies, academia, international counterparts, and the dedicated team at CyberSecurity Malaysia. Your unwavering support, commitment, and collaboration have been instrumental in advancing our mission and strengthening the nation's cybersecurity landscape.

Looking ahead, emerging technologies will continue to reshape the way we live, work, and connect. Realising their full potential safely and responsibly will require sustained commitment, forward-looking policies, strong institutional capabilities, and continued collaboration among all stakeholders. Guided by our mandate and purpose, CyberSecurity Malaysia will continue to champion cybersecurity as a catalyst for innovation, trust, and national resilience.

Together, we are not only securing today's digital landscape—we are shaping a future where trust enables progress, resilience strengthens prosperity, and innovation benefits all.

Note: *YBhg. Dato' Ts. Dr. Haji Amirudin Abdul Wahab retired from CyberSecurity Malaysia on 13 January 2026. The above message was prepared in his capacity as Chief Executive Officer during the reporting period ended 31 December 2025.*

MANAGEMENT COMMITTEE MEMBERS

Fazlan Bin Abdullah
General Manager,
Pre-emptive Technology
& Services Division

Zulfeka Bin Zainal Abidin
General Manager,
Business Development
& Industry Affairs Division

Hamidun Bin Katemin
General Manager,
Corporate Planning
& Strategy Division

Mohd Adlyn Mughni Bin Shamsudin
General Manager,
Chief Executive Officer's Office

Jailany Bin Jaafar
Head, Legal & Secretarial/
Company Secretary

Sabariah Binti Ahmad
Principal Specialist,
Pro-active Technology
& Services Division

Azman Bin Ismail
Senior General Manager,
Management Services
Division

Roshdi Bin Hj Ahmad
Chief Operating Officer
(COO)

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

Ts. Wan Roshaimi Bin Wan Abdullah
Chief Technology Officer
(CTO)

REVIEW OF CORPORATE PERFORMANCE

This performance report presents an overview of the organisation's achievements, progress, and key milestones throughout 2025 across various strategic, operational, and development initiatives. It highlights the collective efforts undertaken to strengthen organisational performance, enhance service delivery, and drive continuous improvement in line with the organisation's goals and long-term aspirations.

TOTAL KPIs
13

OVERALL ACHIEVEMENT
85%

NO	BSC	KPI	TARGET	ACHIEVEMENT
1.	Stakeholders / Customers	Number of Strategic Papers Received by Stakeholders / Interested Parties	1	60%
2.		Number of Digital Trust Policy Frameworks Approved	1	100%
3.		Percentage of Organising Forums / Conferences in the Cybersecurity Field in Conjunction with ASEAN 2025	100	100%
4.		Percentage of Operations of CyberSecurity Malaysia's Subsidiary Company	100	70%
5.		Percentage of Implementation of the Industry Collaboration 2.0 Programme	100	90%
6.		Number of Compliance Support and Act 854 Implementation Initiatives Provided to NCII Sector Leads	3	79%
7.		Number of ICT Products / Applications / Systems and Organisations Assessed and/or Certified by CyberSecurity Malaysia	80	100%
8.		Percentage of Operations of the National Personal Data Monitoring and Protection Laboratory (Joint KPI with JPDP) – Supporting Act 709	100	100%
9.		Percentage of Training and Certification Programmes Implemented for Data Protection Officers (DPO) (Joint KPI with JPDP) – Supporting Act 709	100	100%
10.		Percentage of Artificial Intelligence (AI) Safety Initiatives Implemented with the National AI Office (NAIO)	100	100%
11.	Financial	RM Net Profit Before Tax	RM10 million	37.5%
12.	Internal Process	Percentage of CyberSecurity Malaysia Cyber Case / Incident Resolution at Organisational Level	92	100%
13.	Growth and Learning	Percentage of Research, Development and Commercialisation (RD&C) Collaborations with Technology Companies (Domestic and International)	100	66%

2025 CALENDAR OF ACTIVITIES

Throughout the year, CyberSecurity Malaysia undertook and participated in a diverse range of activities, programmes, and engagements in support of its mission to strengthen cybersecurity resilience and foster greater awareness of cybersecurity issues.

These initiatives reinforced the organisation's position as Malaysia's national cybersecurity specialist agency, strengthened stakeholder engagement, and contributed towards building a safer and more trusted digital environment. The collective impact of these efforts is reflected in the milestones achieved and the value delivered to stakeholders throughout 2025.

12
JANUARY 2025

CyberSecurity Malaysia participated in the Crime Prevention and Cybersecurity Programme organised by MCPF at Dewan Wadi Budi, International Islamic University Malaysia (IIUM), to raise cybersecurity awareness among students and the campus community.

5
MARCH 2025

CyberSecurity Malaysia received a visit from CommerceDotCom Sdn Bhd at Menara Cyber Axis, Cyberjaya, to discuss potential collaboration in digital and cybersecurity initiatives.

20
MARCH 2025

CyberSecurity Malaysia received a visit from the Office of the Deputy Minister of Digital at Menara Cyber Axis, Cyberjaya, further strengthening ties between the agency and the Ministry of Digital's leadership.

26
FEBRUARY 2025

Ahead of CyberDSA 2025, a Pre-Launch Ceremony was held at M Resort Hotel, Kuala Lumpur, officiated by the Deputy Minister of Digital, YB Datuk Wilson Ugak Anak Kumbong, marking another year of strengthening the nation's digital security agenda on the regional stage.

23
MARCH 2025

Through the 2025 CSR Programme, CyberSecurity Malaysia brought "Kembara Amal CyberSAFE®" to orphans from Bait Al Amin, Parit, Perak Darul Ridzuan — combining community outreach with cybersecurity awareness education for the younger generation.

17
APRIL 2025

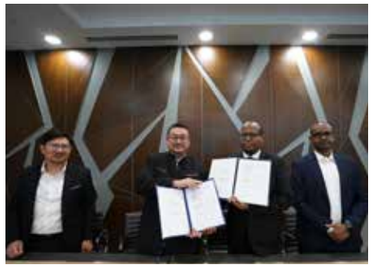
CyberSecurity Malaysia received a visit from the Defence Cyber and Electromagnetic Division (BSEP) at Menara Cyber Axis, Cyberjaya, to explore collaboration opportunities in national defence cybersecurity.

18
APRIL 2025

CyberSecurity Malaysia received a visit from a Chinese delegation at Menara Cyber Axis, Cyberjaya, in conjunction with the "Future of Cybersecurity Summit 2025" organised by PIKOM, strengthening bilateral ties in regional cybersecurity.

6
MAY 2025

CyberSecurity Malaysia and the National Communications Authority (NCA) of Somalia signed a Memorandum of Understanding (MoU), opening a new chapter of cybersecurity cooperation between the two nations.



6
MAY 2025

The "Open Day CyberSecurity Malaysia" CSR programme was held at the CyberSAFE® L.I.V.E Gallery, Cyber Axis Tower 2, Cyberjaya, opening its doors to the public for an interactive exploration of the world of cybersecurity.

9-11
MAY 2025

CyberSecurity Malaysia took part in the 2025 Program MADANI Rakyat (PMR) at Dataran Majlis Perbandaran Tawau, Sabah, bringing cybersecurity awareness directly to the local community.

13
MAY 2025

The Malaysian Highway Authority (LLM) and CyberSecurity Malaysia signed an MoU at LLM's office, strengthening cooperation to protect the nation's digital infrastructure.

25
MAY 2025

In conjunction with University College TATI's Open Day 2025 in Kemaman, Terengganu, CyberSecurity Malaysia signed a Memorandum of Agreement (MoA) to expand academic and research collaboration in cybersecurity.

26
MAY 2025

CyberSecurity Malaysia received an official visit from the Royal Malaysian Navy's Cyber and Electromagnetic Division at Menara Cyber Axis, Cyberjaya, to share expertise in maritime defence cybersecurity.

3
JUNE 2025

CyberSecurity Malaysia launched the Cybersecurity Programme — Certified Chief Information Security Officer (C|CISO) Capability Development for Ministries and Agencies at Doubletree by Hilton Kuala Lumpur, an initiative to strengthen cybersecurity leadership in the public sector.

12
JUNE 2025

CyberSecurity Malaysia launched the CyberSAFE® In Schools programme for Indian students at SJK(T) and SMK schools, introduced by the Minister in the Prime Minister's Department (Federal Territories) at SJK (T) Thamboosamy Pillai, Kuala Lumpur — nurturing a culture of cyber safety from school age.

13-15
JUNE 2025

The 2025 Program MADANI Rakyat (PMR) roadshow continued at Lumut Waterfront, Perak, bringing the cybersecurity message closer to the people.

18
JUNE 2025

The first webinar in the SID-ASEAN 2025 series, themed "Digital Trust", brought together regional experts to discuss challenges and directions for digital trust in the ASEAN region.

18-19
JUNE 2025

The 2025 National Anti-Scam Roadshow (JASK) made a stop at Universiti Malaysia Terengganu (UMT), educating the campus community on recognising and avoiding the latest cyber scam tactics.

25-26
JUNE 2025

Leading cryptology researchers and academics gathered at Cyberview Resort & Spa, Cyberjaya, for the 6th Malaysian Cryptology and Information Security Lecture Series (MCISLS 2025), celebrating 40 years of number theory and cryptology development in Malaysia.

1-3
JULY 2025

CYDES 2025 at the Putrajaya International Convention Centre (PICC) brought together industry players and government agencies to explore the latest developments in digital cybersecurity.

4
JULY 2025

CyberSecurity Malaysia and Tenaga Nasional Berhad (TNB) signed a cooperation MoU, joining forces to strengthen the cybersecurity of the nation's critical infrastructure.

4
JULY 2025

CyberSecurity Malaysia received a visit from the Army Communications and Electromagnetic Institute (BSEP), Malaysian Armed Forces, at Menara Cyber Axis, Cyberjaya, to strengthen cooperation in defence cybersecurity.

15
JULY 2025

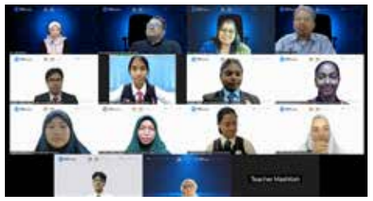
The ASEAN 5G & OT Security Summit at the Kuala Lumpur Convention Centre (KLCC), jointly organised by DNB and CyberSecurity Malaysia, brought together regional experts to discuss 5G network and operational technology (OT) security.

5-7
AUGUST 2025

The Octofinal and Quarterfinal rounds of the National ICT Security Discourse — CyberSAFE® Challenge Trophy 2025 (NICTSeD 2025) uncovered young talent in the field of cybersecurity.

12
AUGUST 2025

The Quarterfinal round of the National ICT Security Discourse — CyberSAFE® Challenge Trophy 2025 (NICTSeD 2025) was held online at the Media Centre, Menara Cyber Axis, Cyberjaya.



19-21
AUGUST 2025

The Malaysian Technical Cooperation Programme (MTCP) 2025 organised the Digital Security & Lifelong Learning Program (DLSP) at Hotel Moxy, Putrajaya, sharing Malaysia's cybersecurity expertise with international participants.

21
AUGUST 2025

CyberSecurity Malaysia received an academic visit from participants of the Digital Forensics Symposium, organised by the United Nations Office on Drugs and Crime (UNODC) together with the Royal Malaysia Police, at Menara Cyber Axis, Cyberjaya, to explore the latest digital forensics practices.

22-24
AUGUST 2025

The 2025 Program MADANI Rakyat (PMR) roadshow arrived at Dataran Nilai, Negeri Sembilan, continuing its mission of bringing cybersecurity awareness closer to the people.

27
AUGUST 2025

The Semifinal round of the National ICT Security Discourse — CyberSAFE® Challenge Trophy 2025 (NICTSeD 2025) took place at the Education Sector & Technology Resource Centre (SSTP), Penang, bringing participants closer to the Final of the National ICT Security Discourse — CyberSAFE® Challenge Trophy 2025.

AUGUST 2025

CyberSecurity Malaysia, through its MySEF Department, collaborated with Universiti Sains Malaysia (USM) to organise Biometric Technology Security Assessment training, enhancing technical expertise in the security evaluation of biometric technologies.

8
SEPTEMBER 2025

The Ministry of Digital's Monthly Assembly, hosted by CyberSecurity Malaysia at Menara Cyber Axis, Cyberjaya, was themed "Kemerdekaan" (Independence), fostering patriotic spirit among staff.

8
SEPTEMBER 2025

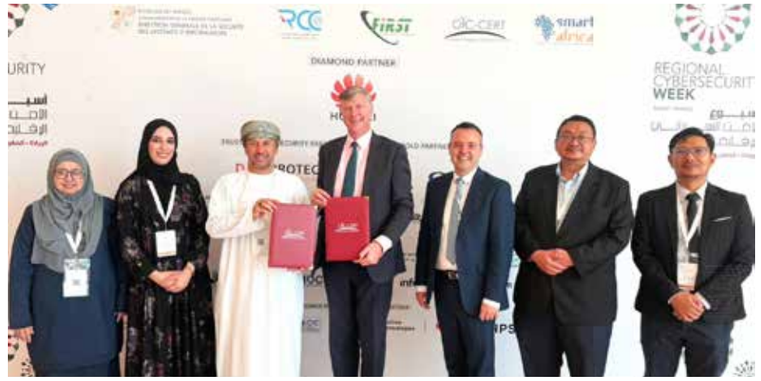
CyberSecurity Malaysia's Vehicle Forensic Laboratory was officially launched by YB the Minister of Digital at the Multipurpose Hall, Menara Cyber Axis — the first laboratory of its kind in Malaysia, strengthening the nation's digital vehicle forensics capability.

10
SEPTEMBER 2025

The Final of the National ICT Security Discourse — CyberSAFE® Challenge Trophy 2024 (NICTSeD 2024) reached its climax at Dewan BSTP, Bukit Kiara, Kuala Lumpur, crowning this year's champion.

15-19
SEPTEMBER 2025

CyberSecurity Malaysia represented the nation at the OIC-CERT 17th Annual Conference 2025 in Rabat, Morocco, strengthening cybersecurity cooperation among OIC member states.



23
SEPTEMBER 2025

CyberSecurity Malaysia received an academic visit from participants of the International Narcotics Enforcement Course 2025, organised by the Royal Malaysia Police, at Menara Cyber Axis, Cyberjaya, to understand the role of digital forensics in cross-border criminal investigations.

23
SEPTEMBER 2025

CyberSecurity Malaysia organised the 2025 Program Galakan Pemerkasaan Siber Kepada Perusahaan Kecil dan Sederhana (PGPKS) at The Light Hotel, Seberang Jaya, strengthening cybersecurity awareness among SME entrepreneurs in Penang.

29
SEPTEMBER 2025

The glittering Malaysia Cybersecurity Awards 2025 ceremony at MITEC, Kuala Lumpur, celebrated outstanding achievements within the nation's cybersecurity ecosystem.

30
SEPTEMBER 2025

The Digital Trust Forum at Cyber Stage, MITEC, held in conjunction with CyberDSA 2025, brought together thought leaders and industry leaders to discuss the future of digital trust.

30
SEPTEMBER 2025

CyberDSA 2025 was officiated by YB the Minister of Digital at MITEC, Kuala Lumpur, marking the official start of one of the region's largest cybersecurity events.

30
SEPTEMBER 2025

The book "The Society of Online Superheroes (S.O.S)" was launched at the Cloud Room, MITEC, Kuala Lumpur — a creative effort to instil cybersecurity awareness among the younger generation through storytelling.

1
OCTOBER 2025

The ISCB Certification Appreciation Ceremony at the Cloud Room, MITEC, held in conjunction with CyberDSA 2025, honoured certified professionals contributing to the nation's cybersecurity industry.

1
OCTOBER 2025

The Quantum Safe Migration (QSM) Forum discussed the strategy of "Securing ASEAN's Digital Future," preparing the region for the security challenges of the quantum computing era.

1
OCTOBER 2025

The Pre-Launch of the Data Protection and Privacy Service Suite and the ISMAD Certificate Presentation Ceremony at Flash Talk, MITEC, introduced new services to strengthen national data protection and privacy.

1
OCTOBER 2025

A closed-door ASEAN discussion on crypto assets at MITEC, Kuala Lumpur, brought together regional policymakers to discuss the direction of regional crypto governance.

2
OCTOBER 2025

The China-ASEAN Digital Trust Cooperation Forum at the Flash Talk Stage, MITEC, sealed cross-regional cooperation in strengthening digital trust.

2
OCTOBER 2025

An invitation-only session on "Building Resilient Cyber Defence: Empowering the Government Sector through Threat Intelligence Integration Awareness" at MITEC, Kuala Lumpur, examined strategies for strengthening public sector cyber defence.

6
OCTOBER 2025

CyberSecurity Malaysia's Vehicle Forensic Laboratory received a certificate of recognition from the Malaysia Book of Records, making history as the nation's first vehicle forensic laboratory.

11
OCTOBER 2025

The 2025 National Anti-Scam Roadshow (JASK) made a stop at UIA Kuantan Campus, Pahang, bringing the #JanganJadiMangsa (Don't Be A Victim) message to the local community.

15
OCTOBER 2025

SID-ASEAN 2025 addressed the issue of scams in conjunction with The Global Islamic Finance Forum (GIFF) at Sasana Kijang, Kuala Lumpur, highlighting the threat of cross-border digital financial fraud.

16
OCTOBER 2025

CyberSecurity Malaysia organised the 2025 Program Galakan Pemerkasaan Siber Kepada Perusahaan Kecil dan Sederhana (PGPKS) at AC Hotel, Kuantan, strengthening cybersecurity among SME entrepreneurs in Pahang.

22
OCTOBER 2025

CyberSecurity Malaysia and Universiti Utara Malaysia (UUM) signed a Memorandum of Agreement (MOA), expanding collaboration in cybersecurity education and research.

23
OCTOBER 2025

CyberSecurity Malaysia organised the 2025 Program Galakan Pemerkasaan Siber Kepada Perusahaan Kecil dan Sederhana (PGPKS) at Hatten Hotel, Bandar Hilir, bringing cybersecurity awareness to SME entrepreneurs in Melaka.

28
OCTOBER 2025

The 2025 National Anti-Scam Roadshow (JASK) made a stop at Universiti Sains Malaysia (USM), Penang, educating the campus community on recognising the latest cyber scam tactics.

30
OCTOBER 2025

CyberSecurity Malaysia signed an MoU with the Electronic Security Service under the Ministry of Digital Development and Transport of the Republic of Azerbaijan, strengthening cybersecurity cooperation between the two nations.

30
OCTOBER 2025

CyberSecurity Malaysia organised the 2025 Program Galakan Pemerkasaan Siber Kepada Perusahaan Kecil dan Sederhana (PGPKS) at Capri by Fraser Hotel, Johor Bahru, strengthening cybersecurity awareness among SME entrepreneurs in Johor.

5
NOVEMBER 2025

CyberSecurity Malaysia received a visit from the Commercial Crime Investigation Department, Bukit Aman, at Menara Cyber Axis, Cyberjaya, to strengthen cooperation in combating cyber and commercial crime.

8
NOVEMBER 2025

The International Battle of Hackers 2025 (IBOH 2025) at Asia Pacific University (APU), Bukit Jalil, tested the skill and expertise of cyber challengers from around the world.

12
NOVEMBER 2025

CyberSecurity Malaysia received an official working visit from a Bangladeshi government delegation, comprising representatives from the Cabinet Division and Finance Division, at Menara Cyber Axis, Cyberjaya, to share national cybersecurity experience and best practices.

13
NOVEMBER 2025

CyberSecurity Malaysia organised the 2025 Program Galakan Pemerkasaan Siber Kepada Perusahaan Kecil dan Sederhana (PGPKS) at Hilton Hotel, Kuching, extending cybersecurity awareness outreach to SME entrepreneurs in Sarawak.

20
NOVEMBER 2025

CyberSecurity Malaysia organised the 2025 Program Galakan Pemerkasaan Siber Kepada Perusahaan Kecil dan Sederhana (PGPKS) at Hyatt Regency Kinabalu Hotel, Kota Kinabalu, continuing its mission to strengthen cybersecurity among SME entrepreneurs in Sabah.

25-27
NOVEMBER 2025

CyberSecurity Malaysia represented the nation at the APCERT Annual General Meeting 2025 in Sydney, Australia, strengthening regional Asia-Pacific cyber incident response cooperation.

26
NOVEMBER 2025

CyberSecurity Malaysia received a visit from the Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA (UiTM), together with 30 distinguished delegates from OIC-COMSTECH member countries, at Menara Cyber Axis, Cyberjaya, showcasing the nation's expertise in big data and artificial intelligence.

2
DECEMBER 2025

CyberSecurity Malaysia signed an MOA with Binary University College at Bilik Jati, Level 10, Menara Cyber Axis, expanding its network of academic cybersecurity collaboration.

5-7
DECEMBER 2025

CyberSecurity Malaysia took part in the Program Rancakkan MADANI Bersama Malaysiaku and the 2025 Civil Service Reform Convention at Dataran Putrajaya, spreading cybersecurity awareness among civil servants and the public.

11
DECEMBER 2025

CyberSecurity Malaysia and Epi Academy Sdn Bhd signed a cooperation agreement at Hotel Seri Pacific, Kuala Lumpur, opening a new chapter of collaboration in cybersecurity training and talent development.

12
DECEMBER 2025

The Ministry of Digital's Two-Year Appreciation and Anniversary Ceremony was celebrated at Hotel Pavilion, Kuala Lumpur, honouring the achievements and transformation journey of the nation's digital ministry since its establishment.

20-21
DECEMBER 2025

The 2025 Karnival CAKNA Digital in Lenggong, Perak Darul Ridzuan, was officiated together with the YAB Menteri Besar of Perak and the Secretary-General of the Ministry of Digital, bringing digital and cyber literacy awareness to rural areas of the state.

29
DECEMBER 2025

The Siber Satria Programme at Menara Cyber Axis closed out 2025's activities with the spirit of chivalry in defending the nation's cyberspace.

DIGITAL VOICES

Digital Voices showcases the collection of posters, infographics, and digital awareness materials produced throughout 2025. Published across CyberSecurity Malaysia's social media platforms, these visual communications were designed to educate, inform, and raise public awareness on cybersecurity issues, digital safety, and emerging cyber threats. Through engaging and accessible content, Digital Voices serves as an important channel for delivering timely messages, promoting cyber resilience, and fostering a more informed and security-conscious digital community.

The Ramadan Cyber Security Infographic Series

The Ramadan Cyber Security Infographic Series was developed to enhance public awareness of cyber fraud threats during the Ramadan month and festive season. The infographics covered topics such as fake donation schemes, fraudulent iftar promotions, social media scams, and online duit raya scams. The materials were disseminated through social media platforms to effectively communicate cyber security messages to the public.

Online Safety During School Holidays Campaign

To raise awareness of digital safety during the school holiday season, CyberSecurity Malaysia introduced the Online Safety During School Holidays campaign. Through a series of informative infographics published on social media, the campaign provided parents and guardians with practical tips on managing children's online activities, promoting responsible digital behaviour, and protecting them from cyber threats. The initiative aimed to foster a safer and more secure online environment for young digital users.

6 Peraturan Keselamatan Siber di Rumah

This infographic was developed as a practical guide for parents to help ensure their children's digital safety during the school holiday period. It highlights six key areas, including the use of parental controls, protection of personal privacy, responsible online behaviour, and eye health practices through the 20-20-20 rule. The initiative aims to empower families in creating a safe, balanced, and secure digital environment at home.

"Digital Selamat, Cuti Sekolah Ceria"

Designed to support parents in managing their children's online activities during school holidays, this infographic provides simple guidance on maintaining a healthy digital lifestyle. Key topics include screen time management, the use of safety features such as SafeSearch and Parental Controls, and the promotion of positive digital etiquette to prevent cyberbullying. The campaign encourages open communication between parents and children to foster a safer and more balanced online experience.

Digital Safety Checklist for Parents

This infographic presents a simple and practical checklist for parents to help keep their children safe online during school holidays. Covering essential cybersecurity measures, online privacy protection, and safe digital habits, it serves as a quick reference for families to create a secure online environment while enabling children to enjoy the benefits of technology responsibly.

Ransomware Best Practices

The "Ransomware Best Practices" Infographic Series was developed as a proactive initiative to strengthen awareness and preparedness against the growing threat of ransomware attacks. The infographics provided comprehensive guidance categorised into two main groups: System Administrators and Internet Users. Shared through social media platforms, this initiative aimed to strengthen digital security and promote safe cyber practices among organisations and the general public.

Merdeka Cyber Awareness

The Cyber Awareness Poster Series in conjunction with National Month celebrations was developed to promote a culture of ethical and safe digital practices among the public. The posters highlighted messages related to social media communication ethics, personal data protection, information security, and the importance of cyber awareness as part of Malaysians' digital responsibility. The campaign materials were disseminated through social media platforms to enhance public awareness of responsible cyber practices in line with the aspirations of Malaysia MADANI.

Digital Literacy

The Digital Literacy Infographic Series was developed to raise public awareness on the importance of using technology safely, wisely, and responsibly. The campaign content was tailored to various target groups, including students, parents, senior citizens, business owners, and civil servants.

Panggilan Senyap

This infographic series aimed to increase public awareness of scam tactics and suspicious phone activities. The campaign provided practical guidance to help individuals recognise potential threats and adopt safer practices when dealing with unknown callers.

ACHIEVEMENT AND AWARDS 2025

The awards and recognitions received during the year reflect CyberSecurity Malaysia's continued pursuit of excellence and innovation in cybersecurity. These accolades acknowledge the organisation's significant contributions towards strengthening national cyber resilience, fostering digital trust, and delivering impactful cybersecurity initiatives. They also serve as a recognition of the dedication and professionalism of CyberSecurity Malaysia's people in supporting the nation's digital transformation journey and advancing a secure digital future.

15 July 2025

CyberSecurity Malaysia, in collaboration with Digital Nasional Berhad (DNB), has successfully organised the ASEAN 5G & Operational Technology Security Summit 2025 (5GOT25) at the Kuala Lumpur Convention Centre, aimed at strengthening cybersecurity cooperation and enhancing digital trust across the Southeast Asian region.

8 September 2025

CyberSecurity Malaysia has successfully established Malaysia's first Vehicle Forensic Laboratory as an effort to strengthen the nation's digital forensic capabilities in investigations, particularly those involving accidents and criminal cases.

3 June 2025

Professional Cybersecurity Capability Development Programme – Certified Chief Information Security Officer (CCSIO) for officers in ministries and government agencies has been successfully introduced as a strategic initiative to develop highly skilled information security leaders within the public sector, particularly in the management of the nation's critical infrastructure.

29 September 2025

The launch of the new CyberSecurity Malaysia Collaboration Programme (CSM-CP) aims to strengthen strategic collaboration between the government and the local cybersecurity industry to develop and innovate products and services.

1 October 2025

The launch of the Data Privacy Services aimed at strengthening national data protection capabilities. This initiative introduces three new services, namely the Certified Data Protection Officer training programme, the Data Privacy Guard Pro (DPGP) assessment and testing service, and the Data Privacy Management Assessment (DPMA).

20 November 2025

The 2025 SME ICONS Tokoh Recognition Award was conferred by the ASEAN International Fair for Trade in Services (AIFTIS 2025) to the Chief Executive Officer of CyberSecurity Malaysia, YBhg. Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab.

5 December 2025

The Path Finder Awards 2025, presented by the Association of Anti-Virus Asia Researchers (AVAR), was conferred on the Chief Executive Officer of CyberSecurity Malaysia, YBhg. Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab.

6 October 2025

CyberSecurity Malaysia has been recognised by the Malaysia Book of Records as the first Vehicle Forensic Laboratory in Malaysia.

PROFESSIONAL CERTIFICATIONS

As the national cybersecurity specialist agency, CyberSecurity Malaysia is deeply committed to fostering a skilled and resilient cybersecurity workforce. In line with our mission to strengthen Malaysia's cybersecurity capabilities, we take pride in recognising individuals who have achieved professional certifications over the past year. These certifications demonstrate not only personal commitment to excellence but also contribute to our national agenda of building a secure and trusted cyber environment.

This section highlights the names of CyberSecurity Malaysia personnel who have obtained industry-recognised certifications. Their achievements reflect a strong foundation of expertise, professionalism, and continuous improvement. We commend these individuals for their dedication and thank them for their role in advancing Malaysia's cybersecurity readiness and resilience.

CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO)

- Ts. Wan Roshaimi Bin Wan Abdullah
- Fazlan Bin Abdullah
- Mohd Azlan Bin Mohd Nor
- Mohammad Zaharudin Bin Ahmad Darus
- Rushidan Bin Ghazali
- Dr. Sarah Khadijah Taylor

CERTIFIED MICROSOFT POWER BI DATA ANALYST

- Ahmad Hisyamudin Bin Salleh
- Faridatul Hanim Binti Abdul Hamid
- Muhammad Kovin Bin Abdul Kohar

COMPTIA SECURITY+

- Shahrin Bin Baharom
- Nur Iylia Binti Roslan
- Mohd Muslim Bin Mohd Aruwa
- Farhan Arif Bin Mohamad
- Mohammad Asyran Fitri Bin Dunya
- Muhammad Ikhwan Bin Mohammad Faisal
- Muhammad Fahmi Bin Zainuddin
- Nik Haziq Iman Bin Nazaruddin
- Shawn Slyvester AL Damotharam
- Hareesh Kumar AL Raman
- Vimalan AL Gunaseelan
- Danish Aisar Bin Mohd Fazrul

CERTIFIED MICROSOFT AZURE FUNDAMENTALS (AZ-900)

- Ahmad Azizul Iqram Bin Musa
- Muhammad 'Allam Bin Omar
- Muhammad Imran Bin Mohamad Fauzi
- Ahmad Osman Bin Ahmad
- Shaikh Abdul Fikri Bin Shaikh Abdul Hamid
- Mohammad Zailani Bin Shato
- Mohd Faisal Bin Abdullah
- Mohd Nor Akashah Bin Mohd Kamal
- Mohammad Amir Syahmi Bin Sharunizak

CERTIFIED ETHICAL HACKER (CEH)

- Noraqilah Binti Azlan
- Vimalan AL Gunaseelan
- Ahmad Al Aqsa Iskandar Bin Ahmmad Bohari
- Muhammad Ikhwan Bin Mohammad Faisal
- Syafiq Iskandar Bin Sham Suri
- Shaikh Abdul Fikri Bin Shaikh Abdul Hamid
- Kilausuria Binti Abdullah
- Ahmad Rabbani Bin Omar

CERTIFIED ISO/IEC 27001:2022 INFORMATION SECURITY MANAGEMENT

- Ahmad Zulfakar Bin Abd Aziz

CERTIFIED ASSOCIATE PROJECT MANAGEMENT (CAPM)

- Nik Azura Bt Nik Abdullah
- Faridatul Akhma Binti Ishak
- Mohammad Zaharudin Bin Ahmad Darus

Muhammad Amirul Bukhari Bin Razak

Suraya Hani Binti Ahmad Zaki

Faridatul Hanim Binti Abdul Hamid

Farah Harnum Bt Gulam Haidir

Ida Rajemee Binti Ramlee

Noor Azwa Azreen Binti Abd Aziz

CERTIFIED MICROSOFT 365 FUNDAMENTALS

Ahmad Hisyamudin Bin Salleh

Muhammad 'Allam Bin Omar

Nur Liyana Binti Zahid Safian

Hareesh Kumar AL Raman

Nur Fazila Binti Selamat

Mohd Faisal Bin Abdullah

Mohd Nor Akashah Bin Mohd Kamal

Muhammad Kovin Bin Abdul Kohar

Abdul Hakim Bin Mohd Raidzoh

Wan Shafiuddin Zainudin

Nur Nadira Bt Mohamad Jafar

Madihah Zulfa Binti Mohamad

Zailin Binti Marjuni

Aliya Farhana Binti Mohd Nasran

SIRIM LEAD ASSESSOR ISO/IEC 17025:2017 LABORATORY QMS

Syarifah Nabilah Syahirah Binti Syed Abd Wahab

Roshenna AP Durairajoo

Mohammad Azree Bin Yahaya

ISO 37001:2025 ANTI-BRIBERY MANAGEMENT SYSTEM (ABMS) LEAD AUDITOR

Adlil Ammal Bin Mohd Kharul Apendi

Noor Aida Binti Idris

Hasnida Binti Zainuddin

Nahzatulshima Binti Zainuddin

Razana Bt Md Salleh

CERTIFIED PROCUREMENT PROFESSIONALS

Syahran Bin Abdul Halim

CERTIFIED INFORMATION SECURITY AWARENESS MANAGER (CISAM)

Nurhafidzah Binti Abdul Halim

Rozila Binti Ramli

Mohd Adlan Bin Ahmad

Mohd Faizal Bin Abdullah

Nur Khairunisa Binti Mohd Nazri

Nur Athirah Binti Abdullah

CERTIFIED CLOUD PRACTITIONER

Muhammad Haziq Aiman Bin Fakhrudin

CERTIFIED PENETRATION TESTER ENGINEER

Ahmad Azizul Iqram Bin Musa

Zul Hafiy Ikmal Bin Mohd Marzuki

Nurul Asha Binti Jeffridin

CERTIFIED PENETRATION TESTER (CPT)

Aiman Aizzat Bin Mohd Yusof

COMPTIA CYSA+

Alfin Najeehah Binti Zahid

Zul Hafiy Ikmal Bin Mohd Marzuki

Nurul Asha Binti Jeffridin

Muhammad Ikhwan Bin Mohammad Faisal

Noraqilah Binti Azlan

Syafiq Iskandar Bin Sham Suri

Hareesh Kumar AL Raman

Zafreida Binti Zahrullayali

Vimalan AL Gunaseelan

COMPTIA PROJECT+

Muhammad Sufi Syiddiq Bin Rosdi

CERTIFIED WEB APPSEC EXPERT

Danish Aisar Bin Mohd Fazrul

PROFESSIONAL AGILE LEADERSHIP-ESSENTIAL (PAL-E)

Atikah Binti Baharudin

Azatulsheera Binti Mohd Azman

MyCC CERTIFIED EVALUATOR

Mohd Muslim Bin Mohd Aruwa

Wan Ahmad Fadli Bin Wan Mohd Yusri

TRAIN THE TRAINER

Syafiqa Anneisa Leng Binti Abdullah

Nurfaezah Hanis Binti Halim

Muhammad Syahreen Bin Zulkifli

Abdul Alif Bin Zakaria

Nur Qurratu 'Aini Binti Rohizan

Sharifah Nurul Asyikin Binti Syed Abdullah

Hanania Aida Binti Mohd Hilmi

Muhammad Rasyid Redha Bin Mohd Tahir

Wira Zanoramy Ansiry Bin Zakaria

Mohammad Zaharudin Bin Ahmad Darus

Mohamad Hafiz Bin Rahman

Nurshahira Binti Mohd

Mohamed Iqbal Bin Tajol Azmi

Nurul Husna Binti Mohd Nor Hazalin

Fatahillah Bin Hashim

CERTIFIED FINANCIAL INVESTIGATOR PROGRAM (CFIP)

Dr. Sarah Khadijah Taylor

Alifa Ilyana Chong Binti Abdullah

Zulkifli Musnman

CERTIFIED HACKING FORENSIC INVESTIGATOR

Mohammad Azree Bin Yahaya

Muhamad Zuhairi Bin Abdullah

Muhammad Afrizal Bin Abd Ghani

CERTIFIED CYBERDEFENDER (CCD)

Shaikh Abdul Fikri Bin Shaikh Abdul Hamid

CERTIFIED IN CYBERSECURITY

Kilausuria Binti Abdullah

Noor Azwa Azreen Binti Abd Aziz

Yuzida Binti Md Yazid

CERTIFIED INTEGRITY OFFICER

Nur Haslaily Binti Mohd Nasir

EDITORIAL COMMITTEE

CONTENT CONTRIBUTOR

1. Azlin Samsudin
2. Ernieza Ismail
3. Alifa Ilyana Chong Abdullah
4. Abdul Hakim Mohd Raidzoh

DIGITAL TEAM

5. Zaihasrul Ariffin
6. Zul Akmal Abd Manan
7. Nurul 'Ain Zakariah
8. Farhana Natasha Mazlan
9. Nurrul Syafina Md Yahaya

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

MINISTRY OF DIGITAL