CyberSecurity MALAYSIA

ANNUAL REPORT 2013

ABOUT CYBERSECURITY MALAYSIA

PROFILE

CyberSecurity Malaysia is the national cyber security specialist center under the purview of the Ministry of Science, Technology and Innovation (MOSTI).

Our mission is to create and sustain a safer cyberspace to promote national sustainability, social well-being and wealth creation.

This mission together with our core values – Trust, Impartiality, Proactive - will guide us to achieve our vision to be a globally recognised national cyber security reference and specialist centre by 2020.

MANDATES

▶ 2005

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 the National ICT Security and Emergency Response Centre (now known as CyberSecurity Malaysia) as a National Body to monitor the National e-Security aspect, spun off from MIMOS to become a separate agency and incorporated as a Company Limited-by-Guarantee, under the supervision of MOSTI.

▶ 2009 & 2013

The Malaysian Government gazetted the role of CyberSecurity Malaysia by Order of the Ministers of Federal Government Vol.53, No.13, dated 22 June 2009 (revised and gazetted on 26 June 2013 [P.U. (A) 184] by identifying CyberSecurity Malaysia as an agency that provides specialised cyber security services and continuously identifies possible areas that may be detrimental to national security and public safety.

▶ 2013

As a specialist agency, CyberSecurity Malaysia is also required to support as well as provide technical assistance and training services for national cyber crisis management, as stated in Paragraph 16.1, Order No. 24 of the *Dasar dan Mekanisme Pengurusan Krisis Siber Negara* (Policy and Mechanism for National Cyber Crisis Management) by the National Security Council.

For more information, visit our website www.cybersecurity.my

DESIGN AND COVER RATIONALE

The design and layout of the 2013 Annual Report is based on the concept of "Securing Cyber Space for Economic Growth", inline with the theme of the Cyber Security Malaysia – Awards, Conference & Exhibition 2013 (CSM-ACE2013).

The theme was also aligned with the National Transformation Program, in which cyber security was identified as a new source of economic growth.

When the national cyberspace is secured, there are tremendous potential for economic activities, creation of knowledge-based jobs and business opportunities.

HOW THE REPORT IS ORGANIZED

The introduction part of the Annual Report 2013 is brief, given that the corporate information is available online, where we have published a Corporate Profile booklet at the website of CyberSecurity Malaysia.

The main contents are divided into two parts:

(I) Corporate Governance – at Board level
(II) Operation's Review – at Management Level

The latter part of the report contains information about the editorial team and the organization's contact information.

(For details, see the Table of Contents on the next page)

TABLE OF CONTENTS

INTRODUCTION

About CyberSecurity Malaysia 02

Design and Cover Rationale 03

Table of Contents 04

CORPORATE GOVERNANCE

Chairman's Statement 06

The Board of Directors 09

Corporate Governance Report 11

Notice of Annual General Meeting 15

OPERATION'S REVIEW

Foreword from the CEO 17

The Management Committee 20

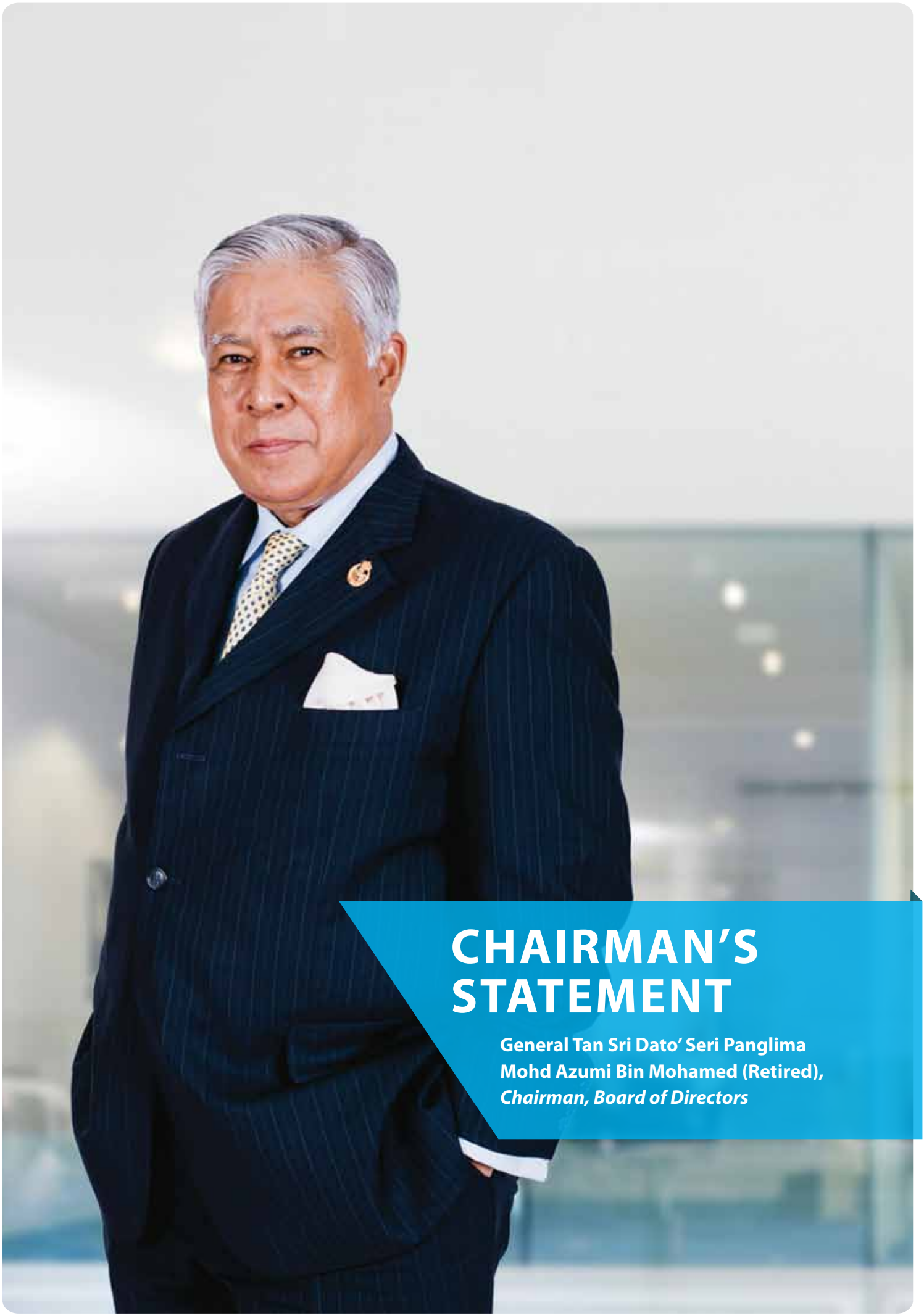
1. Review of Corporate Performance - 2013 23
2. Outlook for 2014 & 2015 29
3. Financial Report 30
4. Products and Services 33
5. 2013 Calender of Activities 36
6. CyberSecurity Malaysia in the News 43
7. List of Achievements and Events 47
   - A. Key Events Organised or Co-organised at National Level 47
   - B. Supported Seminars/Conferences at National Level 49
   - C. Key Events Co-Organised at International Level 50
   - D. Local and International Visits Received 52
   - E. Professional Certifications 53
   - F. Published Technical Papers and Articles 55
   - G. List of Presentations at International Level 56
   - H. List of Presentations at National Level 57

Editorial Committee 60

Form of Proxy 61

Contact Information 63

CORPORATE GOVERNANCE



CHAIRMAN'S STATEMENT

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

CHAIRMAN'S STATEMENT

The 'Cyber Security Market - Global Advancements, Forecasts & Analysis (2014-2019)' published in April 2014 by Research and Markets, reported that "The total market for cyber security is expected to grow from US$95.60 billion in 2014 to 155.74 billion by 2019, at a Compound Annual Growth Rate (CAGR) of 10.3%."

This clearly shows that as the world experiences rapid growth in Internet usage, cyber security also grows correspondingly. A global market value of USD155.74 billion by 2019 is a huge market and opportunities for the local cyber security industry players. To penetrate the global cyber security market, Malaysian companies could get their ICT products certified by CyberSecurity Malaysia under the MyCC Scheme, which is based on international standard known as the Common Criteria MS-ISO/IEC 15408 and MS-ISO/IEC 18045. ICT products certified under the Common Criteria standard by CyberSecurity Malaysia are recognized and accepted in the global market.

Furthermore, Malaysian companies could leverage on CyberSecurity Malaysia's high standing in the two mainstream regional cyber security organizations, the Asia Pacific Computer Emergency Response Team (APCERT) and the Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) to market their products.

These are part of the reasons why we chose "Securing Cyber Space for Economic Growth" as the theme of the Cyber Security Malaysia – Awards, Conference & Exhibition 2013 (CSM-ACE2013) and for this annual report 2013. In fact, among the key achievements in 2013 for CyberSecurity Malaysia is helping to boost the Local Cyber Security Industry Competitiveness by having 11 ICT products evaluated for certification on the product security features against Common Criteria standard.

CyberSecurity Malaysia also helped to increase the numbers and capabilities of local developers to produce and develop secure products based on the Common Criteria standard, which is competitive internationally, by giving incentives to five (5) companies that met the requirements.

Regionally, CyberSecurity Malaysia was once again appointed as a steering committee of the APCERT during the Annual Conference of APCERT, a body of 30 Computer Security Incident Response Teams (CSIRTs) members from 20 countries across the Asia Pacific region.

CyberSecurity Malaysia was also appointed as the permanent secretariat of the OIC-CERT during the OIC-CERT's Annual General Meeting in Bandung, Indonesia in November 2013.

In addition, the Chairman of CyberSecurity Malaysia was appointed as special advisor to the new Chair of the OIC-CERT, recognizing CyberSecurity Malaysia's experience as Chairman of OIC-CERT for the first two terms, from January 2009 until October 2013.

As a centre of technical expertise in the area of cyber security in Malaysia, CyberSecurity Malaysia carries the roles and responsibilities of ensuring the safety and security of the Nation's cyber space.

For the year under review, The Board is pleased with the overall performance of CyberSecurity Malaysia, as the organization attained 89.8% of the target for its Corporate Key Performance Indicators (Corporate KPI).

CyberSecurity Malaysia made us proud when it received a Certificate of Appreciation from the Ministry of Science, Technology and Innovation (MOSTI) for being one of the top four contributors to MOSTI in terms of the number of Key Performance Indicators (KPI) attained with 90% or higher achievement above the target set for the Ministry's KPI (MKPI) for 2013.

When the World Bank released its annual Doing Business Report on 29 October 2013, Malaysia was ranked sixth (6th) among 189 economies globally for 2014. It was a big improvement from 12th position in 2013 and 18th position in 2012.

The improvement in World Bank ranking kept us on a positive spirit. We are hopeful that in 2014 -- we will be able to achieve more -- in securing the Malaysian cyberspace.

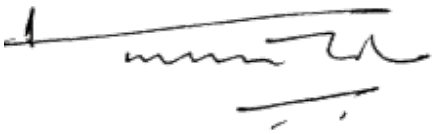
On behalf of the Board of Directors, I wish to welcome the new Chief Executive Officer (CEO) of CyberSecurity Malaysia, Dr. Amirudin Abdul Wahab

who assumed the position in January 2013.

It is a great pleasure to pledge our full support as we wish to continue to see greater initiatives and successful outcome from CyberSecurity Malaysia.

Congratulations to CyberSecurity Malaysia for the excellent performance in 2013!

Thank you.



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

BOARD OF DIRECTORS

Datuk Haji Abang Abdul Wahap Bin Haji Abang Julai
Director

Datuk Dr. Abdul Raman Bin Saad
Director

Ir. Md. Shah Nuri Bin Md. Zain
Director

Rohani Binti Mohamad
Director

Dr. Amirudin bin Abdul Wahab
Director & Chief Executive Officer

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

Dato' Dr. Rosli bin Mohamed
Director

BOARD OF DIRECTORS

1. **General Tan Sri Dato' Seri Panglima Mohd Azumi Bin Mohamed (Retired)**
   Chairman, Board of Directors
   - *Member, Governance and Integrity Committee**
   - *Member, Audit Committee*

2. **Dato' Dr. Rosli bin Mohamed**
   Director
   - *Chairman, Human Resources and Remuneration Committee*

3. **Dr. Amirudin bin Abdul Wahab**
   Director
   - *Chief Executive Officer*

4. **Datuk Dr. Abdul Raman Bin Saad**
   Director
   - *Chairman, Audit Committee*
   - *Member, Governance and Integrity Committee**

5. **Datuk Haji Abang Abdul Wahap Bin Haji Abang Julai**
   Director
   - *Chairman, Governance and Integrity Committee**

6. **Ir. Md. Shah Nuri Bin Md. Zain**
   Director
   - *Member, Human Resources and Remuneration Committee*

7. **Rohani Binti Mohamad**
   Director
   - *Member, Audit Committee*
   - *Member, Human Resources and Remuneration Committee*

Company Secretary
- Jailany Bin Jaafar

Internal Auditor
- Abd Rouf Bin Mohammed Sayuti

Note:
**Governance and Integrity Committee* is a new committee formed in 2014, effective from 14 March 2014.*

CORPORATE GOVERNANCE

STATEMENT OF CORPORATE GOVERNANCE

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

BOARD RESPONSIBILITIES

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

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

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

1. The Human Resources and Remuneration Committees (HRRC)

Duties :

i. 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.

ii. 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 undertake, consider and act on other human resource related issues or tasks as the committee consider appropriate or as may be referred to by the Board.
- To periodically review and participate in determining the organizational structure for the Company.

iii. To review potential candidates for hiring and promotion for the Top Management positions of the Company.

Chairman:

i. YBhg. Dato' Dr. Rosli bin Mohamed

Members:

ii. Encik Ir Shah Nuri bin Md Zain
iii. Puan Rohani bin Mohamad

Terms of Reference of the HRRC

Size and Composition

i. 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.

ii. The Board may from time to time appoint additional members to the HRRC from among

its members and such other persons as the board deem fit.

iii. 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 consider desirable to assist the HRRC in attaining its objectives.

Meetings

i. The HRRC shall have meetings at least twice a year. Additional meetings may be conducted at anytime with the consensus from all members of the Committee.

ii. 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.

iii. The quorum for HRRC meeting shall be two (2) members of the appointed members.

iv. The Head of Human Capital Department ("HCD") is the Secretary for this Committee. In the absence of the Head of HCD, a representative from HCD shall replace the Head of HCD in carrying out the secretariat function.

2. Audit Committee (AC)

Duties:

i. 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.

ii. To review the internal controls, performance and findings of the internal auditors and to recommend and implement appropriate remedial and corrective actions.

iii. To recommend to the Board the appointment of external auditors of the Company, the audit fee and any matter of resignation or dismissal.

iv. 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.

v. To review any significant audit problems that can be foreseen either as a result of the previous year's experience or because of new developments.

vi. To evaluate and review the role of the internal and external auditors from time to time.

vii. To review any significant related party transactions that may arise within the Company.

viii. To review any significant transactions which are not a normal part of the ordinary business of the Company.

ix. To place the internal auditors under the direct authority and supervision of the Audit Committee and to evaluate and approve their performance and remuneration package.

x. To recommend changes in the accounting policies to the Board of Directors.

xi. To review the assistance given by the Company's officers to the auditors.

xii. To consider any matter which the auditors may wish to bring to the attention of the Directors.

xiii. To carry out such other responsibilities as may be delegated by the Board of Directors from time to time

Chairman:

i. YBhg. Datuk Dr. Abdul Raman bin Saad

Members:

ii. YABhg. General Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired)

iii. Puan Rohani binti Mohamad

Terms of Reference of the AC

Size and Composition

The Audit Committee shall consist of at least three (3) but not more than five (5) members of whom the majority shall be independent non-executive Directors of CyberSecurity Malaysia.

The members of the Audit Committee shall select a chairman from among them who is not an executive director or employee of the Company or any related organization.

Meetings

i. 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.

ii. The quorum for Meetings shall be two (2

iii. 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.

iv. The auditors of the Company shall be the Secretary to the Audit Committee.

BOARD COMPOSITION AND BALANCE

The Board consists of members of high caliber, 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 fulfill 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. All selected members of the Board must obtain the prior approval from the Minister of Domestic Trade and Consumer Affairs (MDTCA).

At least half of the total composition of the Members of the Board must be from the government sector and are to be appointed by the Minister of Science, Technology and Innovation. The remaining members may be from the commercial or other relevant sectors that have been elected by the members of CyberSecurity Malaysia at its General Meeting. There are currently seven (7) members of the Board.

The Board is fully and effectively assisted in the day-to-day management of CyberSecurity Malaysia by the Chief Executive Officer and his management team. The profiles of the current Members of the Boards are set out on pages of the Annual Report.

SUPPLY OF INFORMATION TO THE BOARD

Board meetings are held regularly, whereby reports on the progress of CyberSecurity Malaysia's business and operations and minutes of meetings of the Board are tabled for review by the Members of the Board. At these Board meetings, the Members of the Board also evaluate business 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.

As at the end of the financial year 2013, sixteen 16) Board Meetings were held inclusive of circular resolutions passed.

APPOINTMENTS AND RE-ELECTION TO THE BOARD

Members of the Board that represents the Ministry of Science, Technology and Innovation ("MOSTI") are not subject to retirement whereas other members of the Board shall hold office for a term of two (2) years or for a term which commences at the date of appointment and spans two annual general meeting (including where applicable the annual general meeting where the appointment was made), whichever is the longer.

Dato' Dr. Rosli bin Mohamed, Director of CyberSecurity Malaysia is not subject to retirement since he is representing MOSTI.
Dr Amirudin bin Abdul Wahab, being the Chief Executive Officer is subject to retirement in accordance with his tenure of service with CyberSecurity Malaysia and the terms and conditions applicable thereto.

YABhg. Gen Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired), YBhg. Datuk Abang Abdul Wahap bin Abang Julai, YBhg. Datuk Dr Abdul Raman bin Saad, Ir Md Shah Nuri bin Md Zain and Puan Rohani binti Mohamad who are the Directors holding office for a term of two (2) year, which terms is expiring pursuant to Articles 31 of the Articles of Association of CyberSecurity Malaysia. They offer themselves for re-election as a Director and will be considered for approval by the Members of CyberSecurity Malaysia at the Seventh Annual General Meeting 2013.

DIRECTORS' TRAINING

Directors are encouraged to attend talks, training programs 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 MOSTI. 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 Articles of Association of CyberSecurity Malaysia.

INTERNAL CONTROL AND RISK MANAGEMENT

The Board is responsible for CyberSecurity Malaysia's system of internal controls and its effectiveness. However, such a system is designed to manage CyberSecurity Malaysia's risks within an acceptable risk profile, rather than eliminate the risk of failure to achieve the policies and business objective of CyberSecurity Malaysia. The prescribing and maintenance of a system of internal controls, however, provides a reasonable assurance of effective and efficient operations, and compliance with laws and regulations, as well as with internal procedures and guidelines.

The Board has, through the Management, carried out the ongoing process of identifying, evaluating and managing the key operational and financial risks confronting CyberSecurity Malaysia. The Board embarked on a review of the existing risk control and risk management, implementing and entrenching the risk management culture and functions within CyberSecurity Malaysia.

The internal risk control and management programs prescribed by the Board include policies and procedures on risks and control by identifying and assessing the risks faced, and in the design, operation and monitoring of suitable internal controls to mitigate and control these risks.

The Board is of the view that the system of internal controls in place for the year under review and up to the date of issuance of the annual report and financial statements is sufficient to safeguard the interests of the stakeholders, clients, regulators and employees, and CyberSecurity Malaysia's assets.

NOTICE OF ANNUAL GENERAL MEETING

NOTICE IS HEREBY GIVEN THAT the 8th Annual General Meeting of CYBERSECURITY MALAYSIA will be held by way of Members' Circular Resolution pursuant to Article 20 of the Company's Articles of Association on or before 18 August 2014 to transact the following business:

AS ORDINARY BUSINESS

1.	To receive the Audited Financial Statements for the financial year ended 31 December 2013 together with the Reports of the Directors and Auditors thereon;	Ordinary Resolution 1
2.	To re-elect the following who is a Director holding office for a term of two (2) years, which term is expiring pursuant to Article 31 of the Company's Articles of Association, and being eligible, offers himself for re-election;	Ordinary Resolution 2
	2.1 General Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired);	
	2.2 Datuk Abang Abdul Wahap bin Abg Julai;	
	2.3 Datuk Dr Abdul Raman bin Saad; and	
	2.4 Puan Rohani binti Mohamad.	
3.	To appoint Messrs Afrizan Tarmili Khairul Azhar & Co (AFTAAS) as Auditors of the Company and Messrs Afrizan Tarmili Khairul Azhar Taxation Services Sdn Bhd as Tax Consultant of the Company and to authorize the Directors to fix their remuneration;	Ordinary Resolution 3

AS SPECIAL BUSINESS

4.	To approve the Director's accumulated monthly allowance totaling RM171,050 for the financial year ended 31 December 2013; and	Ordinary Resolution 4
5.	To transact any other business of which due notice shall have been given in accordance with the Companies Act, 1965.	

BY ORDER OF THE BOARD

JAILANY BIN JAAFAR (LS 8843)
Company Secretary

Selangor Darul Ehsan
Date :

NOTES :

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

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

To be valid the proxy form duly completed must be deposited at the Registered office of the CyberSecurity Malaysia at Level 5, Sapura@Mines, No. 7 Jalan Tasik, The Mines Resort City, Seri Kembangan, 43300 Selangor Darul Ehsan, Malaysia not less than forty-eight (48) hours before the time for holding the meeting.

OPERATION'S REVIEW

FOREWORD FROM THE CEO

Dr. Amirudin Abdul Wahab,
Chief Executive Officer

FOREWORD FROM THE CEO

Dear Stakeholders:

"We remain committed to our mission of creating and sustaining a safer cyberspace to promote national sustainability, social well-being and wealth creation."

In this information age, we must be brave enough to challenge our formerly proven methods as well as our organizational culture. It is not enough to simply keep up with the wind of change. We have to anticipate change, and be ready either to challenge it or adapt quickly.

I was appointed as CEO of CyberSecurity Malaysia on 14th January 2013. Thanks to my predecessor, Lt Col Dato' Husin Jazri (Retired) and the dedicated staff, CyberSecurity Malaysia has gained recognition and respect from local and international counterparts.

When I came in, I found that CyberSecurity Malaysia had very strong potential. Fundamental policies and key infrastructures are well established. I believe CyberSecurity Malaysia is strong enough to move forward and face bolder challenges.

Strengthening CyberSecurity Malaysia

I will continue to lead CyberSecurity Malaysia towards the vision of making CyberSecurity Malaysia a globally recognized expert in cyber security. To achieve that vision, we must first ensure that here at home in Malaysia we are the point of reference when it comes to online security matters.

However, we could not go about this ambitious quest alone. I believe in working together with various cyber security agencies to help strengthen our knowledge in the field.

Among the most important steps are to play a more active role when working together with agencies like the National Security Council (MKN) to keep Malaysia's critical infrastructure safe from being brought down by cyber attacks. We also need to work closely with the Attorney General's Chambers (AGC) and the police force to strengthen Malaysia's laws and defenses when fighting cybercriminals. I am open to working with anyone, including independent cyber security experts.

Internally, the organisation's staff members have superb technical skills and there are a lot of untapped potential in CyberSecurity Malaysia. I hope to inspire the staff members to pursue continues learning and be more of a team player rather than working in silos.

Continues improvement, teamwork, and a more competitive attitude, would definitely help CyberSecurity Malaysia to grow stronger and become a formidable force in the industry. Given the right mindset, I am confident that CyberSecurity Malaysia will not only remain relevant in the Malaysian cyber security industry, but will continue to lead.

National Centre of Exellence

With sustainability in mind, and CyberSecurity Malaysia's vision to be a Globally Recognized, National Cyber Security Reference & Specialist Centre by 2020, I introduced a new mindset in February 2013, via the concept of National Centre of Excellence (COE).

A Centre of Excellence is a premier organization providing an exceptional product or service in an assigned sphere of expertise and within a specific field of technology, business, or government, consistent with the unique requirements and capabilities of the COE organization.

CoE is the master plan that CyberSecurity Malaysia needed to chart the strategic positioning and future direction. COE is intended to ensure that

CyberSecurity Malaysia is well positioned to play its part in supporting the national agenda as well as meeting the challenges of tomorrow, sustaining its operation in the long run and the greater needs of the business and corporate community at-large.

Based on the solid performance of CyberSecurity Malaysia in 2013 (see the Operation's Review section), I strongly believe that the concept of National Centre of Excellence (COE) can be successfully implemented.

Operation's Review

The operation's review section of the Annual Report 2013 is organized as follows:

- Foreword
- The Management Committee
- Review of Corporate Performance (Based on KPI 2013)
- Financial Report
- Products and Services
- Calendar of Activities
- CyberSecurity Malaysia in the News
- Lists of achievements, events, publications and international presentations

Gratitude

I would like to thank the Board for their valuable support, and the Management & Staff for their hard work and dedications in helping to create and sustain a safer cyberspace to promote national sustainability, social well-being and wealth creation.

I am truly grateful for the opportunity to lead CyberSecurity Malaysia. I must also say that I am proud of the CyberSecurity Malaysia Team – who is young, vibrant, and supportive, with positive attitude and genuine enthusiasm to succeed.

Thank you.

Dr. Amirudin Abdul Wahab
Chief Executive Officer

THE MANAGEMENT COMMITTEE

Zahri bin Hj Yunos
Chief Operating Officer

Dr. Amirudin bin Abdul Wahab
Chief Executive Officer

Dr. Solahuddin bin Shamsuddin
Chief Technology Officer

Mohd Roslan Bin Ahmad
Vice President, Corporate Services

Mohd Shamir Bin Hashim
Vice President, Government & International Engagement

Roshdi Bin Ahmad
Vice President, Corporate Strategy & Industry Development

Lt Col Mustaffa Bin Ahmad (Retired)
Vice President, Outreach & Capability Building

Lt. Col. Sazali bin Sukardi (Retired)
Vice President, Strategic Research

Maslina binti Daud
Vice President, Proactive Services

Dr. Aswami Fadillah bin Ariffin
Vice President, Responsive Services

Jailany Bin Jaafar
Head, Legal and Secretarial / Company Secretary

THE MANAGEMENT COMMITTEE

TOP MANAGEMENT

1. **Dr. Amirudin bin Abdul Wahab**
   Chief Executive Officer

2. **Zahri bin Hj Yunos**
   Chief Operating Officer

3. **Dr. Solahuddin bin Shamsuddin**
   Chief Technology Officer

HEAD OF DIVISIONS / VICE PRESIDENTS

1. **Mohd Roslan Bin Ahmad**
   Vice President, Corporate Services

2. **Mohd Shamir Bin Hashim**
   Vice President, Government and International Engagement

3. **Roshdi Bin Ahmad**
   Vice President, Corporate Strategy and Industry Development

4. **Lt Col Mustaffa Bin Ahmad (Retired)**
   Vice President, Outreach and Capability Building

5. **Lt Col Sazali bin Sukardi (Retired)**
   Vice President, Strategic Research

6. **Maslina binti Daud**
   Vice President, Proactive Services

7. **Dr. Aswami Fadillah bin Ariffin**
   Vice President, Responsive Services

8. **Jailany Bin Jaafar**
   Company Secretary
   Head, Legal and Secretarial

REVIEW OF CORPORATE PERFORMANCE - 2013

Various efforts, initiatives and programs have been carried out since the inception of CyberSecurity Malaysia. These efforts were essential to support the strategic direction of CyberSecurity Malaysia that has stepped into the 10th Malaysia Plan phase.

In 2013, we were at a more challenging phase with the goal to "Spearhead National Cyber Security Through Resiliency And Self-Reliance". This phase would highlight the stronger cooperation between the Government, Industry and the Community in addressing cyber security related issues that require concerted effort from all parties.

Alhamdulillah, I am pleased to report that despite the challenges that we had to overcome, we did quite well.

Among the highlights of our achievements based on Corporate Key Performance Indicators 2013 (KPI 2013) are as follows:

1. Brand recognition and visibility

CyberSecurity Malaysia's brand name remained strong and respected. Our services were sought after by our counterparts both locally and internationally.

We received acknowledgement from Ministry of Science, Technology and Innovation (MOSTI) for being in the top 7th place among 27 Departments and Agencies in generating media coverage that contributed to MOSTI's visibility in the media.

In addition, we were pursued by six (6) organizations for co-branding of conferences/seminars at national level. We were invited to co-organize 30 trainings/ conferences at national level and seven (7) at international level. We also received eight (8) visits from Malaysian institutions / organizations and four (4) from foreign organizations.

CyberSecurity Malaysia was invited to deliver presentations during conferences, seminars and meetings that were held both in Malaysia and overseas. CyberSecurity Malaysia's personnel delivered a total of 48 presentations in 2013 including 17 at international events.

2. International Accreditation

Our Cyber27001 service received accreditation based on international standard, MS ISO/IEC 17021 from Department of Standards Malaysia. Cyber27001 is a service to certify organization's Information Security Management System (ISMS) scope based on MS ISO/ IEC 27001. This accreditation allows us to implement ISMS certification service with impartiality and credibility.

More importantly, organizations that obtained ISMS certification from CyberSecurity Malaysia will enjoy tax exemptions against their certification fee.

3. National Cyber Crisis Exercise or X-MAYA

National Security Council (MKN) in collaboration with CyberSecurity Malaysia had organized the National Cyber Crisis Exercise or X-MAYA 5 on 25 November 2013.

The closing ceremony of X-MAYA 5 was officiated by the Deputy Prime Minister of Malaysia - Yang Amat Berhormat Tan Sri Dato' Hj. Muhyiddin Bin Hj. Mohd Yassin, on 26 November 2013 at the Royale Bintang Hotel, Damansara.

In line with its mandate as the national cyber security technical and specialist centre, CyberSecurity Malaysia provided the infrastructure and technical support that made X-MAYA 5 possible.

The success of X-MAYA 5 was due to vast experience gained by CyberSecurity Malaysia in organizing the previous four versions of X-MAYA and also in organizing regional cyber drills with Organization of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) and the Asia Pacific Computer Emergency Response Team (APCERT).

In addition, CyberSecurity Malaysia has also gained capabilities and expertise in handling various cyber security incidents through years of training and experience running its services namely the Cyber999 Help Centre and the Malware Research Centre.

The National Cyber Crisis Exercise 2013 or X-MAYA

5 was aimed at testing the effectiveness of procedures developed under the National Cyber Crisis Management Plan and also evaluating the preparedness and readiness to respond to cyber attacks by the participants who are from the Critical National Information Infrastructure (CNII) organizations.

X-MAYA 5 recorded the highest participation in the history of the program since its inception in 2008, with participation from 98 public and private agencies that represent 10 CNII sectors.

4. Corporate Social Responsibility (CSR)

CyberSecurity Malaysia continued to showcase a caring attitude through its Corporate Social Responsibility (CSR) initiatives through implementation of Tunas Cemerlang 2.0 Program.

As is the tradition since 2009, during the month of Ramadhan and as a part of Hari Raya Aidilfitri preparation, CyberSecurity Malaysia took the orphans and underprivileged children of Bait Al-Amin for Hari Raya Shopping followed by a simple ceremony to give away donations to the children and teachers of Bait Al-Amin, as well as to students of University Petronas who acted as mentors to the children at Bait Al-Amin.

This initiative is an opportunity for CyberSecurity Malaysia to reach out to under privileged community and at the same time instill element of positive use of the Internet and promote the cyber security culture.

5. CyberSAFE@CSM-ACE2013

- **LAUNCHING & HANDOVER CEREMONY OF 'NATIONAL SURVEY – SAFETY NET: GROWING AWARENESS AMONG MALAYSIAN SCHOOL CHILDREN ON STAYING SAFE ONLINE'**

  We conducted the closing ceremony of DiGi CyberSAFE in Schools Program (DCP) on the 14 November 2013. The DCP has been educating students and teachers in schools nationwide since November 2011.

  CyberSecurity Malaysia and its strategic partners for the CyberSAFE in Schools Program in 2013, namely DiGi Telecommunications Sdn Bhd and the Ministry of Education launched and distributed the booklet containing the result from National Survey – Safety Net: Growing Awareness among Malaysian School Children on Staying Safe Online.

  The survey gathered opinions from 9,651 students from 459 schools across all states in Malaysia from the DiGi's CyberSAFE in Schools workshops, which were carried out nationwide from 26 April to 12 October 2013.

- **FINAL ROUND OF THE NATIONAL ICT SECURITY DEBATE 2013**

  The Final round of the National ICT Security Debate: CyberSAFE Challenge Trophy 2013 was also conducted in conjunction with the CSM-ACE 2013, on 14 November 2013.

  The preliminary rounds were held months in advance in eight zones nationwide. The finalists were sponsored by the program sponsors to attend the final competition in Kuala Lumpur during the CSM-ACE 2013.

- **CYBERSAFE AMBASSADORS PROGRAM**

  The CyberSAFE Ambassadors Program in 2013 focused on collaboration with the Girl Guide Association of Malaysia and DiGi in order to be more targeted, hence, allowing more efficient utilization of resources.

  The collaboration with DiGi involved providing training to 500 teachers (part of DiGi CyberSAFE in Schools) to qualify them as CyberSAFE Ambassadors who will in turn train school children to behave ethically when they are online and make use of the Internet positively such as for communicating with family and friends and search for educational resources.

  The collaboration with the Girl Guide Association of Malaysia focuses on training 200 Brownie Malaysia leaders as CyberSAFE Ambassadors who will in turn spread the knowledge on cyber safety and best practices to their schools and communities.

CONTRIBUTIONS TO MOSTI'S KPI

As mentioned by our Chairman of the Board of Directors, we are honored to receive the Appreciation Certificate from the Ministry of Science, Technology and Innovation (MOSTI) for being one of the top four contributors to MOSTI in terms of the number of Key Performance Indicators (KPI) attained with 90% or higher achievement above the target set for 2013 Ministry KPI (MKPI).

The table below shows our performance against the target for MOSTI's Ministry KPI 2013.

CyberSecurity Malaysia's achievement compared with the target for 2013 Ministry KPI (MKPI)

1. NKEA SRI 14: **11** ICT products under evaluation. **Five (5)** products have been certified, which meet the target of **five (5)** products certified based on Common Criteria Standards.

2. MKRA 2.1: **Two (2)** new products rolled out, which meet the target of **two (2)** technologies transferred to companies/government agencies.

3. MKRA 2.2: **12** Information security papers published in journals, meeting the target of **12** publications.

4. MKRA 3.2: **41** professional certifications were obtained by CyberSecurity Malaysia's staff, 95.2% above the target of **21** k-workers trained via staff development programs.

5. MKRA 3.3: **811** trained k-workers by certification or professional qualifications. 35% above the target of **600.**

6. MKRA 4.1: **Three (3)** STI projects diffused to community, 50% above target of **two (2)** STI projects.

7. MKRA 4.2: **1006** people impacted from STI projects diffused to community, more than doubled the target of 400 people. (151.5% above target)

8. MKRA 4.3: **21** STI awareness activities, exceeding the target of 20 by 5%.

9. MKRA 4.4: **19,155** people impacted from STI awareness (outreach) activities, exceeding the target of 15,000 people by 27.7%.

HOW WE PERFORMED BASED ON CORPORATE KEY PERFORMANCE INDICATORS (2013 KPI)

For the 2013 KPI, I am pleased to report that we exceeded most of our targets and attained a score of 89.8 %. This is the most tremendous improvement in terms of KPI performance compared with the last five years (since 2009).

The following paragraphs are about the 2013 KPI – what were the indicators, and how we performed in relations to the targets.

Since 2007, we have always organized our Key Performance Indicators into three perspectives, based on the Balanced Scorecard framework introduced by Profs. Kaplan and Norton, namely:

- From the Shareholder's and Customer's Perspectives
- From the Internal Business Process Perspectives
- From the Internal Learning and Growth Perspectives

I. Our Performance as seen from our Shareholder's and Customer's Perspectives

We defined our shareholder as the Malaysian Government, represented by MOSTI and MOF Inc.; and our customers as all Internet users in Malaysia. For 2013, from the Shareholder's and Customer's Perspectives, we had five strategic goals with 50% total weight for the 2013 KPI, out of ten corporate goals in total. Our performances in meeting each of the goals are described below:

1. The first goal was to achieve brand recognition, by hosting and/or co-chairing one global event in the area of cyber security as well as to have brand partnership exercise with the industry players where CyberSecurity Malaysia would be involved as speaker and support their initiatives to raise awareness and generate interest in cyber security. To achieve this goal, the main responsibility was on the Corporate Branding and Media Relations Department.

   Performance: 200% above target as we succeeded in hosting/ co-chairing two global events (our target was one event) and co-branding.
   - We hosted and chaired two international events.

   - The international event that we hosted was the Regional Asia Information Security

Exchange (RAISE) Forum Meeting, through our Security Management & Best Practices (SMBP) Department, on 11 - 12 November 2013 as a satellite event of the CSM-ACE 2013.

- We chaired the Cyber Intelligence Asia 2013 Conference organized by Intelligence-Sec Limited, United Kingdom. With the support from MOSTI, CyberSecurity Malaysia played an active role in this conference including as the chairperson for the conference and presented papers as speaker.

2. The second goal was to increase the number of globally-recognized cyber security professionals, by assisting 800 local professionals to obtain certifications in cyber security. To achieve this goal, the main responsibility was on the Cyber Security Professional Development Department.

   Performance: For this goal, we achieved 70% of the target, through our Cyber Security Professional Development Department. The target was to assist 800 local professionals to obtain certifications in cyber security, and we assisted 561.

3. The third goal was to develop 'National Proactive & Defensive Capabilities'. To achieve this goals, there were two indicators:

   i. Two new cyber security proactive and defensive services have been developed, and fully operational by the end of 2013.
   ii. To provide incentives under the Strategic Reform Initiatives (SRI): Industry Development funds to three (3) companies to allow them to send their ICT products for Common Criteria (CC) evaluation and certification. This will encourage industry players to be involved in the Common Criteria (CC) ICT product evaluation and certification through various financial assistance and grants.

   Performance: We managed to roll out four new services, which is 200% above target; and provided incentives to five companies, which is 167% above the target.

   The four new services are:

   a. Cyber Drill Training Services
      - Training "*Latihan Krisis Siber Negara*"
      - Provide technical expertise
      - Utilized by National Security Council (MKN)

   b. Cyber Security Master Program Services
      - Module for Cyber Security Master degee Program. A Collaboration between Universiti Kebangsaan Malaysia (UKM) and CyberSecurity Malaysia

   c. Smart Card System Evaluation Services
      - Smart Cards and Smart Card-Related Devices and Systems evaluation and certification through MyCC
      - Utilized by National Registration Department (JPN)

   d. Cyber Security Industry Directory Services
      - Directory and information on Malaysian companies providing cyber security related products and services.
      - List of MyCC / ISMS / Malaysia Trustmark Certified Products and Companies
      - Utilized by cyber security industry players

4. Our fourth goal was to raise national acculturation in cyber security with 15,450 people targeted to benefit from our outreach and awareness activities. In addition, we targeted to raise RM1 million from the private sector as their contribution to the National Acculturation Program.

   Performance:
   - A total of 19, 155 Malaysians benefited from our cyber security and safety awareness activities; which was 124% above target.
   - We also earned RM935,620 contribution from private sector, or 93.6% of the RM1 million target.
   - Primarily the Outreach Unit of the Outreach & Corporate Communications Department carried out this task.

5. The fifth goal was to Boost Local Cyber Security Industry Competitiveness by having eight (8) ICT products evaluated for certification on the product security features against Common Criteria standard, a set of functional and assurance claims using MS-ISO/IEC 15408 and MS-ISO/IEC 18045; and three (3) companies given incentives in order to increase the numbers and capabilities of local developers to produce and develop secure products based on the Common Criteria standard that will be competitive internationally

   Performance:
   - We evaluated 11 products or 137.5% above target, and provided incentives to five (5) companies, which is 167% above target.
   - The MyCC Unit of Information Security

Certification Body (ISCB), the MySEF Unit of Security Assurance Department, Government Engagement Department and the Industry & Business Development Department (IBD) are primarily responsible to achieve the target for this goal.

II. Under the Internal Business Process perspectives, our strategic goals and performance indicators were as follows:

6. The sixth goal was to Deliver CyberSecurity Malaysia Core Services to Market Segments / Technology Clusters. The indicators are 70% customer satisfaction, 85% Incident Resolution for cyber incidents and digital forensics cases solved (at our end) within the Service Level Agreement (SLA) requirement and Monetization of five (5) CyberSecurity Malaysia services.

   Performance:
   - For this goal, we obtained 88.5% customer satisfaction rating, higher than the target of 70%. All departments in CyberSecurity Malaysia contributed in achieving this goal.
   - As for the second indicator, we resolved 92.17% of the 10, 636 cyber security incidents reported to the Cyber999 Help Centre and the 490 Digital Forensics cases, much higher than the target -- which was 85%
   - The main contributors are the Cyber999 Unit of the Malaysia Computer Emergency Response Team (MyCERT) Department and the Digital Forensics Department. Both departments are under the Cyber Security Responsive Services Division.

7. Our seventh goal was to Secure and Professionally Manage Funds. The indicators were the ability to earn RM 2 million net profit either from revenue of selected CyberSecurity Malaysia services and/ or sponsorship. The second indicator was the ability to utilize 100% of budget allocated to CyberSecurity Malaysia (allocation received from the Government)

   Performance: 132% above target. We managed to earn RM2, 634, 375 net profit from revenue of selected CyberSecurity Malaysia services and/or sponsorship. On top of that, we also utilized 100% of the budget allocation, thus 100% on target.

III. From the Learning and Growth Perspectives, the strategic goals and performance indicators were as follows:

8. CyberSecurity Malaysia's eighth goal was to Enhance Internal Research Capacity, Capability & Facility, by developing 2 Research Initiatives undertaken by the technical staff, to roll out 2 new cyber security related products for the use of various targeted customers, and to have 11 information security papers published in journals.

   Performance: Three (3) research initiatives (150% above target), two (2) new products rolled out (100% on target), and 13 information security papers published in journals (118% above target).

   The two new products rolled out were:

   I. Face recognition (20 November 2013) - Comparing selected facial features from the image and a facial database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

   II. CSM Block Cipher (5 December 2013)
   A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block

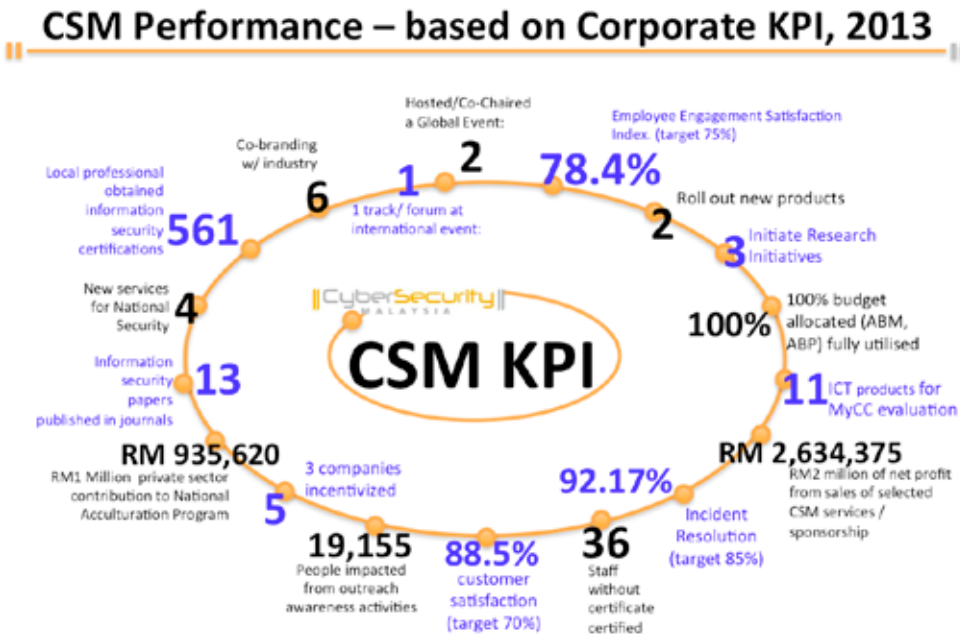
9. The ninth goal was to Increase the Number of Globally-Recognized CyberSecurity Malaysia Professionals, by having 21 staff not having any certificates yet to be certified under various programs covering both technical and non-technical.

   Performance: We did very well with a total of 54 certified staff in 2013. 41 of them are newly certified (195% above target).

10. Our 10th goal was to Build Creative & Innovative Work Processes & Environment by ensuring at least 75% Employee Engagement Satisfaction Index (EEI), based on EEI survey conducted yearly to measure the degree of an employee's positive or negative emotional attachment to their job, colleagues and organization that profoundly influences their willingness to learn and perform at work.

Performance: 78.4% Employee Engagement Satisfaction Index, or 105% above target.

The chart below graphically summarizes the results of our achievements based on the targets set for CyberSecurity Malaysia's Corporate KPI 2013:



OUTLOOK FOR 2014 & 2015

TRANSFORMING CYBERSECURITY MALAYSIA

To cope with continuous shifts and changes in market demands, we need to make fundamental changes in how we conduct business. We believe that a time will come, where there will be a need to **transform** CyberSecurity Malaysia.

Sooner or later, we will need to push ourselves beyond our comfort zone and embark on a Business Transformation Program (CSM BTP) – will it be in 2014? Or 2015? We are currently assessing our readiness for CSM BTP. For a start, we will first prepare a roadmap on how we can achieve a measured, goal-orientated response to marketplace events, or to the need to improve our performance.

The Vision of CSM BTP is to transform CyberSecurity Malaysia corporate-wide as an entity that is flexible, robust to dynamic changes in the market and sustainable.

We have big plans for CyberSecurity Malaysia. Hopefully, the future will bring more success to all of us.

CONCLUSION

CyberSecurity Malaysia organized or participated in events, programs and/or activities only if they are important initiatives or part of initiatives that would result in creating a conducive, secured eco-system or cyber environment.

Throughout the year 2013 we have achieved the KPI objectives in line with Malaysia's aspiration to become a developed nation via digital economy by 2020 through wide application of Information Technology and Communication (ICT) in every aspects.

So far, we have presented the following:

1. Review of Corporate Performance – 2013
2. Outlook for 2014 - 2015

In the subsequent part of this Operation's Review, let us share with you the report/review of the following:

3. Financial Report
4. Products and Services
5. Calendar of Activities
6. CyberSecurity Malaysia in the News

To conclude the Operation's Review, we have listed our achievements, events, publications and international presentations as follows:

A. Key Events Organized or Co-organized at National Level
B. Supported Seminars or Conferences at National Level
C. Key Events Co-organized at International Level
D. Local and International Visits Received
E. List of Staff Obtaining Professional Certifications
F. Technical Papers and Articles Authored or Co-authored by Staff
G. Presentations at International Level
H. Presentations at National Level

Last but not least, we present to you the editorial team and we have provided our contact information for your ease of reference.

Thank you.
On behalf of CyberSecurity Malaysia.

FINANCIAL REPORT

STATEMENT OF FINANCIAL POSITION AS AT 31 DECEMBER 2013

	31.12.2013	31.12.2012
	RM	RM
ASSETS		
Non Current Assets		
Property, plant and equipment	24,523,948	23,763,222
Intangible assets	2,954,726	2,398,208
	27,478,674	26,161,430
Current Assets		
Trade receivables	467,355	295,022
Other receivables	1,916,316	889,102
Short term deposit with licensed banks		72,100,750
Cash and bank balances	5,895,207	1,620,922
	8,278,878	74,905,796
Total Assets	**35,757,522**	**101,067,226**
RESERVES AND LIABILITIES		
Reserves		
Accumulated reserves	1,361,438	1,447,253
Non Current Liabilities		
Government grants	31,941,639	99,177,851
Current Liabilities		
Other payables and accruals	2,454,475	442,122
Tax payable	-	-
Total Reserves and Liabilities	**35,757,552**	**101,067,226**

STATEMENT OF COMPREHENSIVE INCOME FOR THE YEAR ENDED 31 DECEMBER 2013

	2013	2012
	RM	RM
INCOME FROM GRANTS	44,743,918	36,381,776
OPERATING REVENUE	1,887,648	1,949,594
OTHER INCOME	1,541,271	445,272
	48,172,837	**38,776,642**
STAFF COST	(26,227,143)	(21,799,220)
DIRECTOR'S EMOLUMENTS	(627,576)	(616,606)
DEPRECIATION AND AMORTISATION	(5,132,121)	(5,009,693)
RENTAL	(4,163,400)	(4,057,221)
OTHER OPERATING EXPENSES	(12,097,864)	(7,295,862)
DEFICIT OF INCOME BEFORE TAXATION	**(75,267)**	**(1,960)**
TAXATION	(10,548)	13,844
TOTAL COMPREHENSIVE INCOME / (DEFICIT) FOR THE YEAR	**(85,815)**	**11,884**

STATEMENT OF CHANGES IN RESERVES FOR THE YEAR ENDED 31 DECEMBER 2013

	ACCUMULATED RESERVES
	RM
As at 1 January 2012	1,435,369
Total Comprehensive deficit for the year	11,884
Balance at 31 December 2011	1,447,253
Total comprehensive income for the year	(85,815)
Balance at 31 December 2012	**1,361,438**

STATEMENT OF CASH FLOWS FOR THE YEAR ENDED 31 DECEMBER 2013

	31.12.2013	31.12.2012
	RM	RM
CASH FLOWS FROM OPERATING ACTIVITIES		
Deficit of income before tax	(75,267)	(1,960)
Adjustments for:		
Depreciation of property, plant and equipment	3,947,132	3,921,591
Amortisation of intangible assets	1,184,988	1,088,102
Property, plant and equipment write off	194,046	21,979
Interest income	(418,316)	(266,730)
Grant income recognised	(44,743,918)	(36,381,776)
Operating loss before working capital changes	(39,836,068)	(31,616,834)
Changes is working capital :		
(Increase) / decrease in trade receivables	(172,332)	(177,283)
(Increase) / decrease in other receivables	(1,027,214)	(58,881)
(Decrease) / increase in other payables	2,012,353	(903,651)
Increase in governmnet grants	(70,000,000)	(70,000,000)
	(109,023,261)	(102,756,649)
Operating government grants	19,380,000	20,400,000
Interest received	418,316	266,730
Tax Paid	- 10,548.00	-
Net cash used in operating activities	(89,310,760)	(82,091,897)
CASH FLOWS FORM INVESTING ACTIVITIES		
Purchase of property, plant and equipment	(4,925,905)	(788,623)
Purchase of intengible assets	(1,741,506)	(1,014,165)
Proceed from disposal of PPE	24,000	-
Net cash used in investing activities	(6,643,411)	(1,802,788)
CASH FLOWS FROM FINANCE ACTIVITY		
Development government grant received	28,127,706	155,235,855
NET INCREASE / (DECREASE) IN CASH AND CASH EQUIVALENTS DURING THE YEAR	(67,826,465)	71,341,188
CASH AND CASH EQUIVALENTS AT BEGINNING OF THE YEAR	73,721,672	2,380,484
CASH AND CASH EQUIVALNETS AT END OF YEAR	**5,895,207**	**73,721,672**
CASH AND CASH EQUIVALNTS COMPRISE:-		
Fixed Deposit	-	72,100,750
Cash and bank balances	5,895,207	1,620,922
	5,895,207	**73,721,672**

PRODUCTS AND SERVICES

As an agency that looks after the safety of Malaysian's cyberspace, we provide specialized products and services for organizations, cyber security workforce and the general public. The following are the description of products and services recently repackaged and rebranded for selected target markets:

BENEFITS TO CLIENTS:	PRODUCTS / SERVICES PROVIDED BY CYBERSECURITY MALAYSIA
Cyber Security Readiness & Resiliency	**i. CyberRESPONSE** • CyberRESPONSE is a structured and coordinated approach to Security Incident Handling with the help of well-defined policies, procedures and structure. • We assist organizations to develop Cyber Security Incident Response Team (CSIRT) capabilities, which is a combination of theoretical, hands-on learning and coordinated cyber drills. **ii. CyberWARN** • CyberWARN helps organizations develop early warning capabilities for mitigating malware threats using a system called 'LebahNET Mini Service'. • LebahNET is an effective and accessible framework that detects, identifies and collects data on malware threats. It also generates incident analysis reports, which serve as early warning and allow decision makers sufficient time to react accordingly. • As a result, organizations are pre-warned to prevent malware infection and always prepared to handle malware attacks on their computer system and network, hence, avoid financial loss and negative consequences on the organization's reputation. **iii. CyberVAS** • CyberVAS is a Scheduled Vulnerability Assessment Service to address an organization's need for a proactive assessment and mitigation of potential vulnerabilities in the network. • This will improve the security posture through actual assessment or evaluation and defending against cyber threats and exploitation due to information systems and technology vulnerabilities. • Accurate vulnerability assessment data increase business confidence and enhances reputation of the organization.
Attain or Maintain Certification(s) based on International Cyber Security Standards	**iv. Cyber27001** • Cyber27001 is a service to certify organization's Information Security Management System (ISMS) scope based on MS ISO/IEC 27001. • Being certified with ISMS ISO/IEC 27001 provides a degree of assurance that the business processes have been redesigned to reduce security risks and ensure confidentiality, integrity and availability of information assets. • This will increase clients' confidence and trust in the organization.

BENEFITS TO CLIENTS:	PRODUCTS / SERVICES PROVIDED BY CYBERSECURITY MALAYSIA
Attain or Maintain Certification(s) based on International Cyber Security Standards	**v. CRISM** • CRISM is an online training and assessment module for information security management (based on ISO/IEC 27001) for all employees. • We provide this service to organizations that have been certified compliant with the Information Security Management System (ISMS) based on MS ISO/IEC 27001 to help them manage and maintain the ISMS certification. **vi. CyberVALIDATE** • In addition to Cyber27001, we also provide independent security audit of an organization's ISMS certification scope. The audit is based on ISO/IEC 27001 and the accreditation requirements. • This will help an organization to align its business strategy with the security and compliance domains of the international standard ISO/IEC 27001 or ISMS.
Global Competitiveness for Locally Produced ICT Products	**vii. CyberCC** • Evaluation and certification of the security functions of ICT products, based on ISO/IEC 15408 also known as Common Criteria (CC). • Malaysian ICT products that have passed the CC certification are carrying a globally recognized CC certificate, thus, have a better chance to compete in the international markets.
Become a Trusted e-Business Provider	**viii. CyberTRUST** • CyberTRUST will encourage "secure e-Business" to grow and prosper in Malaysia by improving consumers' confidence in e-Businesses. • e-Businesses that are legal, comply to relevant regulations, and follow best practices based on the five domains specified in the World Trustmark Alliance (WTA) code of conduct will receive the Malaysia Trustmark seal from CyberSecurity Malaysia.
Recover Lost or Damaged Data	**ix. CyberRECOVER** • CyberRECOVER is our Data Recovery Service. • Data recovery is a digital forensic process of salvaging data from damaged, failed, corrupted or inaccessible digital storage media and making it readable using computer applications. • CyberSecurity Malaysia is a credible entity and can be trusted to handle confidential data.

BENEFITS TO CLIENTS:	PRODUCTS / SERVICES PROVIDED BY CYBERSECURITY MALAYSIA
Secure Deletion and Sanitization of Data Prior to Disposal of Device(s)	**x. CyberSANITIZE** • CyberSANITIZE is our Data Sanitization Service, to help individuals (or organizations) permanently and securely erase all important data trails from a data storage device and ensure that those data can never be recovered. • Preventing confidential data from being misused after disposal of data storage device such as hard disks of old computers or memory cards of mobile devices.
Trained and Capable Cyber Security Workforce	**xi. CyberTRAIN** • CyberTRAIN is our Cyber Security Professional Training courses offered to organizations and individuals to develop cyber security knowledge and capabilities. • Nurtures with practical capabilities and learning processes that are structured to cultivate innovative mindsets.
Internationally Recognized (Certified) Cyber Security Professionals	**xii. CyberCERTIFY** • In addition to CyberTRAIN, we also offer CyberCERTIFY to assist cyber security workforce to obtain professional certifications that are accredited by international certification bodies such as the SANS Institute, ISACA and (ISC)2 .
Positive Use of the Internet Among Employees / Communities	**xiii. CyberSAFE** • Cyber Security Awareness for Everyone (CyberSAFE) is a structured and knowledge based approach to inculcate information security awareness within an organization or community. • We help organizations conduct Information Security Knowledge Sharing Sessions on a wide range of topics in the Information Security domain, which address the needs of the target audience in terms of both topic and level of difficulty. **xiv. CyberSAFE Ambassadors** • We help train volunteers from within an organization to become CyberSAFE Ambassadors with sufficient knowledge on information security and access to the knowledge bank and resources at CyberSecurity Malaysia. • In return, they will become trainers within their organizations, thus facilitate greater knowledge transfer to nurture cyber security culture and positive use of the Internet.

2013 CALENDER OF ACTIVITIES

7 - 11 January

Information Security Management System (ISMS) MS ISO/IEC 27001:2007 Implementation Course and MS ISO/IEC 27001:2007 Internal Audit.

14 - 18 January

Information Security Management System Implementation Audit Workshop (ISMS).

30 – 31 January

Course on Critical Infrastructure Security.

5 February

Forensic on Internet Application Training.

22 February

Regional ICT Conference at Kinta Riverfront Hotel & Suites Ipoh, Perak.

25 - 28 February

Digital Forensic Training for Inland Revenue Board (IRB).

12 – 15 March

Cyber Intelligence Asia Conference 2013

CyberSecurity Malaysia was involved as a "Supporting Organization" and was appointed as the chairman of the conference this year.

14 March

Mr. Howard Schmidt, Former Special Assistant to President, Cyber Security Coordinator, Executive office of President Obama, United States made his first official visit to CyberSecurity Malaysia.

12 March

Seminar: "Business Online…New Opportunities" at Kinta Riverfront Hotel& Suites, Ipoh, Perak.

24 - 27 March

CyberSecurity Malaysia participated in the Annual Conference of Asia Pacific Computer Emergency Response Team (APCERT): www.apcert.org, a body of 30 Computer Security Incident Response Teams (CSIRTs) members from 20 countries across the Asia Pacific region.

2 April

Seminar on Online Business & Websites: Threats & Opportunities, Kuala Lumpur.

4 April

CyberSecurity Malaysia's visit to Malaysian Communications and Multimedia Commission (MCMC).

8-12 April

Workshop on Information Security Management System (ISMS) Implementation Audit.

10 April

Visit by Royal Malaysian Navy Officers from KD Pelanduk to CyberSecurity Malaysia.

15-19 April

Digital Forensic Training Program for Royal Malaysian Customs Officers (KDRM).

30 April

Visit from Software Engineering Students of Universiti Pendidikan Sultan Idris (UPSI), Perak.

6 May

Visit by Honorable Dr Hamed Salim Al-Rahwi, Information Technology Authority (ITA) Board Member and Delegates from Oman.

20 May

CyberSecurity Malaysia's Visit to the Ministry of Foreign Affairs, Malaysia.

22 May

Seminar Business Online… New Opportunities, Pulau Pinang.

22 May

Visit by Students from UiTM, Shah Alam.

6 June

Hi-Tea with Media and Price Giving Ceremony for Poster and Video Design Competition and CyberSAFE e-Baca Quiz Organized by CyberSecurity Malaysia. The Poster and Video design competitions were carried out over the course of four months beginning December 2012 to March 2013, through CyberSecurity Malaysia's social media platforms on Facebook, Twitter and YouTube. 23 submissions on poster design and 25 submissions for video design were received from local schools and university students.

10 June

Students who have been pursuing a course in Digital Forensics made a follow-up visit to CyberSecurity Malaysia.

11 - 15 June

ISO/IEC 27001:2007 ISMS Lead Auditor Course organized by National Security Council (MKN) in collaboration with CyberSecurity Malaysia.

13 June

CyberSecurity Malaysia's visit to MIMOS Bhd.

8-12 April

Staff Retreat – Teambuilding

This activity was carried out at Institute Budaya Baru Malaysia, Kemensah, Hulu Kelang (IBBM) over two days and one night, participated by all of CyberSecurity Malaysia's personnel. Among the objectives of this teambuilding were to foster closer relationship amongst CyberSecuirty Malaysia staff, to reduce the communication gap as well as to inculcate the spirit of closer teamwork in order to achieve the goal of creating a peaceful and harmonious work environment.

17-20 June

Information Security Management System (ISMS) MS ISO/IEC 27001:2007 Implementation Course organized by National Security Council (MKN) in collaboration with CyberSecurity Malaysia.

18 June

CyberSecurity Malaysia's visit to Bank Negara Malaysia.

24 - 28 June

Certified Ethical Hacker Training (CEH)

This training provided exposure to several staff members of CyberSecurity Malaysia on Network Infrastructure Integrity and Penetration Test.

2 July

CyberSAFE in School's workshop for Bestari Coordination Teachers at the Teachers Activity Centre in Sibu, Sarawak.

2 July

Visit by Information Technology Centre TD (PUSTEKMA TD), Army Headquarters, Wisma Pertahanan Jalan Padang Tembak, Kuala Lumpur to CyberSecurity Malaysia.

3 July

Official Launching Ceremony of the Malaysia Trustmark for Private Sector (MTPS), a new service by CyberSecurity Malaysia.

3 - 5 July

'CyberSAFE in Schools' workshop for Bestari Coordination Teacher at the Teachers Activity Centre in Miri, Sarawak.

4 July

Information Security Management System - ISMS MS ISO/IEC 27001:2007 Internal Auditor Course.

4 July

Cyber Security Awareness Talk at Podium B Hall, Menara Ministry of Youth and Sports, Putrajaya.

8 -9 July

CyberSAFE in School's workshop for Bestari Coordination Teachers at the Teachers Activity Centre in Pekan, Pahang.

10 July

ISMS Certification Closing Ceremony for Malaysia Airline System Berhad .

18 July

Meeting and Visit by Social Media Monitoring Technical Committee, Volume 3 – 2013, at CyberSecurity Malaysia.

25 July

ISMS Certification Closing Ceremony for Ministry of Defense Malaysia.

3 - 5 July

MS ISO/IEC 17021 Accreditation by Standards Department, Malaysia

2 - 5 September

Information Technology and Communication Exhibition during Software Testing Conference (SOFTEC) 2013.

4 - 6 September

VMware vCloud Director: Install, Configure & Manage Training.

5 September

Customer Relations Management System Application Usage Workshop for Law Enforcement Agencies.

9 – 10 September

CyberSecurity Malaysia Corporate Social Responsibility Program: Working visit in conjunction with Handing over of 15 Units of Computer to SMK Bengkongan Kota Marudu, Sabah.

10 September

System Stability and Electronic Transaction Forum.

10 - 12 September

ASEAN Regional Forum (ARF) On Measures To Change Cyber Security – Legal and Cultural Aspects, Beijing, China.

10 – 13 September

14th International Common Criteria Conference (ICCC 2013).

19 September

Seminar: "Business Online…New Opportunities", Johor.

20 September

An Integrated Approach for Cyber Security and Critical National Information Infrastructure Protection Talk.

21 September

Creativity and Science4U Program at Sekolah Menengah Kebangsaan Tun Haji Abdul Malek, Cheng, Melaka (Parliament Tangga Batu).

25 September

Visit from Ministry of Information and Communications, Vietnam.

26 September

Technology Update Seminar, INTAN Sarawak(Parliament Tangga Batu).

www.utusan.com.my (25 Nov 2013)

3 remaja ditahan, muat turun filem tanpa kebenaran

7 and 8 November

Operation Spyglass (KL Gangster 2) was held as one of the support services provided by CyberSecurity Malaysia to the Law Enforcement Agencies in the form of digital forensic examination.

12-14 November

Cyber Security Malaysia - Awards, Conference and Exhibition (CSM-ACE) 2013, at the Royale Chulan, Kuala Lumpur.

2-4 December

9th General Conference Of The Council For Security Cooperation In The Asia Pacific (CSCAP), Beijing, China.

4 - 5 September

ICT Product - Security Assessment (IPSA) Workshop, Le Meridien Hotel, Kuala Lumpur.

9 - 20 December

Intensive Course by Indonesian Security Incident Response Team on Internet and Infrastructure/Coordination Center (Id-SIRTII/CC).

10 December

Memorandum of Understanding Signing Ceremony between University Putra Malaysia (UPM) and CyberSecurity Malaysia(Parliament Tangga Batu).

11 - 12 December

2nd National Conference On Information Assurance 2013.

16 - 19 December

Training for Sarawak Energy Sdn Bhd.

CYBERSECURITY MALAYSIA IN THE NEWS

CyberSecurity Malaysia appointed as Secretariat to OIC-CERT

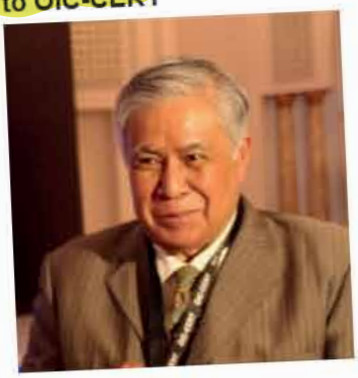


Photo - General Tan Sri Dato' Seri Panglima Mohd Azu of CyberSecurity Malaysia and also the Chair of the O

Malaysia's national cyber security agency CyberSecu appointed as the Secretariat to the Organisation of th Computer Emergency Response Team [OIC-CERT] annual general meeting in Oman recently.

With this appointment, CyberSecurity Malaysia is no Secretariat position of the OIC-CERT, said General Mohd Azumi of the OIC-CE

"CyberSecurit security effort professionalis of the OIC-CE

"The OIC-CE conceived in who grace the activities and OIC-CERT in

In reinforcing unanimously agreed on the idea of having an O Office, which is beneficial for the continuance operation of the collaboration, said Mohd Azu

He added that another outcome of this AGM is OIC-CERT Cyber Drill 2013 in the first half of t exercise is mainly to assess the response cap Security Incident Response Teams (CSIRT) a technology and trends in mitigating cyber thre

The meeting also agreed that under the traini member countries, which are Pakistan, Oma Emirates, have offered their training facilities member countries.

OIC-CERT, which was established in 2009 to countries to develop collaborative cyber secu cyber security related agencies from 18 eco

6 **News**

Cyber Security Agency Has New Head

CyberSecurity Malaysia's CEO comes from Ministry of Science Technology and Innovation.

BY AVANTIKUMAR

National cyber security agency CyberSecurity Malaysia appointed Dr Amirudin bin Abdul Wahab as its new chief executive officer in mid-January.

In a statement, the agency, which is under the purview of the Ministry of Science, Technology and Innovation (MOSTI), said Dr Amirudin served as head of MOSTI's ICT Policy Division since January 2010.

"In his capacity as the Head of MOSTI's ICT Policy Division, Dr Amirudin led and coordinated various development programmes and activities of the ICT Cluster of MOSTI agencies, namely the Multimedia Development Corporation (MDeC), MIMOS Berhad, CyberSecurity Malaysia and .my Domain Registry. He also managed MOSTI ICT-related international affairs, as well as national programmes and promotion of ICT acculturation for the country," continued the statement.

Other Positions

"He headed the Secretariat to the National Information Technology Council (NITC), which is chaired by the Prime Minister of Malaysia and a National Committee Member of e-Sovereignty Working Committee, which is chaired by the Secretary General of the National Security Council."

Dr Amirudin is currently the National Ch...

Jawatankuasa Standard Perindustrian bagi Teknologi Maklumat, Telekomunikasi dan Multimedia, an Adjunct Professor at UNITEN ...

University of Malaysia (UIAM). He is an Industry Advisory Panel (IAP) Member of the Universiti Teknologi Petronas (UTP).

Dr Amirudin holds a doctorate (PhD) in National ICT Policy and Strategic Management, from the School of Information Technology & Electrical Engineering, University of Queensland, Brisbane, Australia. He has a Master's degree in Business Administration (MBA) from the University of Dubuque, Iowa, USA; a Master's degree in Information Technology (MSc. IT), from the National University of Malaysia (UKM), and a Bachelor of Science Engineering in Electrical Engineering (BSEE) d...

CyberSecurity pantau aktiviti alam siber

UTUSAN SARAWAK - MUKA DEPAN
6 APRIL 2013

JUMIET NYIREK

KOTA SAMARAHAN, Jumaat — CyberSecurity Malaysia tidak mempunyai akta yang khas untuk melaksanakan penguatkuasaan berhubung kegiatan jenayah siber.

Ketua Pegawai Eksekutif Dr Amirudin Abdul Wahab berkata CyberSecurity hanya mempunyai pakar bagi membantu kerajaan mengesan atau memantau aktiviti alam siber.

"Tugas kita (CyberSecurity) adalah membantu pihak berkuasa seperti polis dan Suruhanjaya Komunikasi Malaysia berhubung jenayah siber," katanya.

Beliau berkata demikian kepada pemberita selepas menyampaikan ceramah Kesedaran Keselamatan Siber sempena Program Tunas Cemerlang 2.0: Program Cybersafe Mentor di Fakulti Seni Gunaan dan Kreatif, Universiti Malaysia Sarawak (UNIMAS) di sini pagi tadi.

Menurut beliau, CyberSecurity menerima aduan dari pengadu berhubung jenayah siber.

Beliau berkata, laporan itu diterima daripada pihak polis atau SKMM walaupun mencatat tahun Cyber999 milik CyberSecurity.

Dr Amirudin berkata, sehingga Mac tahun ini pihaknya sudah menerima sebanyak 2,499 kes membabitkan jenayah siber dengan 1,160 kes penipuan manakala 862 adalah pencerobohan akaun pengguna siber dan selebihnya lain-lain kes.

Beliau percaya masih ramai lagi menjadi mangsa tetapi enggan tampil untuk membuat laporan.

Dalam mengenai jumlah laporan yang tidak stabil, beliau menjelaskan ia bergantung kepada bilangan laporan diterima daripada pihak berwajib seperti polis, SKMM dan syarikat keselamatan siber itu.

"Mungkin apabila masyarakat telah mempunyai kesedaran mengenai keselamatan siber ini maka ramai akan tampil membuat laporan," katanya.

CyberSecurity Malaysia merupakan pusat pakar keselamatan siber kebangsaan yang bertanggungjawab membantu memantau dan mengendalikan kegiatan jenayah siber di negara ini di bawah kawal selia Kementerian Sains, Teknologi dan Inovasi (MOSTI).

Ceramah yang disampaikan itu membentangkan isu serta cabaran di alam siber yang dihadapi warga digital di Malaysia.

Selain itu ia turut membincangkan kepentingan beretika di alam siber dan cara untuk menyumbang ke arah penambahbaikan tentang keselamatan siber.

MAS Receives ISO 27001 Certification

KUALA LUMPUR, July 18 (Bernama) -- Malaysia Airlines (MAS) has joined the league of 74 other companies in Malaysia qualified for the Information Security Management System (ISMS) Certification.

"MAS is the first Malaysia-based carrier company to be certified. The certification for the Data Centre Operations is part of its corporate-wide ISMS implementation programme," said Chief Information Officer Faridah Abdul Rahman in a statement Thursday.

She said the certification acknowledged that MAS was committed to maintaining confidentiality of business and customers' information and ensuring that company information and assets are for authorised use only."

"Receiving the certification is another milestone in our airline's journey to pursue with total determination, a consistent achievement of maintaining a secure operational environment for our customers, staff and other stakeholders," said MAS Group Chief Executive Officer Ahmad Jauhari Yahya after receiving the MS/IEC ISO 27001:2007 certificate from CyberSecurity Malaysia CEO Dr Amirudin Abdul Wahab.

"This accreditation certifies that MAS maintains best practices in information security," he added.

-- BERNAMA

CYBERSECURITY MALAYSIA IN THE NEWS

Cyber-war: Time for our agencies to step up

- *Cyber-warfare is raging between Malaysian and Filipino hackers*
- *It is time for the Malaysian Govt to harden our cyber-defenses*

LAST month, US President Barack Obama issued an executive order to bolster the nation's cyber-defenses, a move unpopular with some hacker movements and civil society advocates, elegantly awarded by many, and considered insufficient by some experts.

Delivered as part of his State of the Union address, Obama said, "We know foreign countries and companies swipe our corporate secrets...Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy," the Los Angeles Times reported.

The daily described it as a "stopgap measure" that would improve "how classified information is shared between the government and the owners and operators of crucial infrastructure, including electric utilities, dams and mass transit."

MIT Technology Review said the Executive Order Improving Critical Infrastructure Cybersecurity wasn't amount to much, adding that it only "requires new information-sharing, standards-setting, and R&D plans to get up and running over the next few months to two years."

"The executive order... won't force companies to introduce measures that would protect infrastructure like the power grid," the Review noted.

But as I read the backlash against Obama, and in the wake of reports of cyber-warfare raging between Malaysian and Filipino hackers, all I could think was that at least the United States is waking up to the reality of the new front in hostilities: The Internet.

According to The Star Online, Filipino blog Pinoy Tech News first reported that some of their government websites were hit by denial-of-service (DoS) attacks, while others were defaced. Filipino hackers then retaliated, attacking and defacing several Malaysian private and government-owned websites.

A statement allegedly made by Anonymous has called for hackers of both countries to stand down, to no avail, the Malaysian daily said in its online edition.

Last July, when I wrote about Stuxnet – courtesy of the US Government – heralding a new era of state-sponsored terrorism, espionage and warfare in cyberspace, I felt that I may have been stretching it a bit. But remember, it's not paranoia if they're really after you.

Since then, malware such as Red October, Gauss, miniFlame and Madi have been identified, all designed for targeted cyber espionage campaigns in varying degrees. More recently, Kaspersky Lab has identified WinDealer, which was used to attack multiple government entities and institutions worldwide recently.

Among the victims were government entities and...

Malaysia Trustmark for private sector launched

- *To audit and validate websites; aims to promote greater trust and confidence in e-business*
- *CSM's Cyber999 Help Centre received 4,001 reports of online fraud incidents last year*

CSM executives and representatives of six companies whose e-businesses have been certified with Malaysia Trustmark

CYBERSECURITY Malaysia (CSM) has launched its Malaysia Trustmark for Private Sector programme, which will assess and certify e-business entities to help consumers identify those that are legitimate.

CSM, an agency under the Ministry of Science, Technology and Innovation (MOSTI), said the programme would audit and validate websites, and aims to promote greater trust and confidence in e-business.

...said the ...in sales by ...websites," ...which ...said in a ...es. ...st. Hence ...

Perkasa keselamatan siber

Malaysia negara keenam paling berisiko diancam *malware*

Oleh MASZUREEN HADZMAN

MALAYSIA berada dalam kedudukan negara keenam di dunia paling berisiko terdedah kepada kadar pendedahan ancaman (TER) ,iaitu peratusan komputer peribadi yang mengalami serangan *malware*, sama ada berjaya atau gagal, dalam tempoh tiga bulan kebelakangan.

Laporan tersebut telah dikeluarkan oleh firma pemaju keselamatan teknologi maklumat (IT), Sophos, berdasarkan pendedahan terhadap ancaman *malware*, bukannya berkenaan ancaman siber.

Mengulas perkara tersebut, Pengerusi CyberSecurity Malaysia, **Tan Sri Mohd. Azumi Mohamed** bagaimanapun berkata, ancaman *malware* juga merupakan sebahagian daripada cabaran keselamatan siber masa kini.

"Serangan serta evolusi *malware* memberi gambaran tentang keadaan landskap ancaman siber pada masa hadapan yang sudah tentu akan sentiasa berubah," katanya.

Jelasnya, cabaran sebegini menggalakkan pihak CyberSecurity Malaysia untuk terus berinovasi dalam pendekatan serta usaha memperkasakan keselamatan siber.

Menyedari kepentingan mempunyai persekitaran siber yang berdaya tahan dan selamat, kerajaan turut merancang beberapa pendekatan keselamatan siber yang sedang dilaksanakan.

Antara pendekatan yang dilaksanakan ialah Dasar Keselamatan Siber Negara (NCSP) bertujuan untuk membangunkan dan mewujudkan program yang komprehensif yang memastikan keberkesanan kawalan keselamatan siber ke atas prasarana maklumat kritikal Negara.

"Di peringkat strategik, kerajaan telah menyediakan NCSP yang memberi tumpuan terhadap peningkatan daya tahan Prasarana Maklumat Kritikal Negara kita (CNII) bagi menangani ancaman siber, dan pada masa yang sama memaksimumkan manfaat ekonomi digital negara dan serantau.

"Kemudian, di peringkat industri atau komersial, kami menggalakkan kerjasama kerajaan-swasta seperti mengadakan kerjasama dengan Microsoft Corp. dan Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan dengan objektif utama untuk mengurangkan peratusan komputer peribadi (PC) di Malaysia yang mengalami serangan *malware* dengan mendidik pengeluar PC dan pengguna,"katanya.

Selain itu, langkah menguatkuasakan undang-undang ke atas peruncit dan peniaga yang menipu pengguna dengan menjual PC dengan perisian cetak rompak yang dijangkiti malware juga penting bagi membendung ancaman malware.

Ini kerana, perisian cetak rompak adalah salah satu punca jangkitan *malware* dan juga digunakan sebagai agen penyebaran jangkitan masalah tersebut .

Jelas Mohd. Azumi, pihaknya turut melaksanakan program mendidik dan membina kesedaran masyarakat melalui

DR. AMIRUDIN Abdul Wahab memberi penerangan d... CyberSecurity Malaysia kepada wakil media, di Seri K...

"Kami tidak mempunyai sebarang akta untuk penguatkuasaan," katanya ketika s... memberi taklimat sempena lawatan wakil media ke agensi tersebut, baru-baru ini .

Menurut beliau, pihaknya bertindak berdasarkan laporan yang diterima daripada pengadu berhubung jenayah

CyberSecurity Malaysia conference, expo and awards in November

- *Public-private driven event with the theme 'Securing Cyberspace for Economic Growth'*
- *Aims to attract 300+ corporate leaders, CISOs, info-security pros, policy makers and others*

NATIONAL cyber-security specialist centre CyberSecurity Malaysia (CSM) has announced it would be holding its flagship event, the Cyber Security Malaysia Awards, Conference & Exhibition 2013 (CSM-ACE 2013), from Nov 13-14 in Kuala Lumpur.

CSM, which is under the purview of the Ministry of Science, Technology & Innovation (MOSTI), said the event, which has the theme 'Securing Cyberspace for Economic Growth,' aims to catalyse innovation and growth in the cyber-security industry.

The event is now open for registration and participation from organisations as well as industry partners, it said in a statement.

"CSM-ACE 2013 is expected to attract over 300 corporate leaders, chief information security officers, information security managers and professionals, policy makers, law enforcement officers and academicians," said CSM chief executive officer Dr Amirudin Abdul Wahab *(pic)*.

The awards component of CSM-ACE consists of eight categories for distinguished individuals and organisations in recognition of their significant contribution to the cyber-security, safety and well-being of Malaysian cyberspace, CSM said.

The conference is aimed at being a knowledge-sharing platform to gather industry experts and the community on the latest trends in cyber-security. There will be two tracks, the first on governance and risk management, while the second is a technical track.

Finally, the exhibition will showcase trade and investment opportunities by assisting and allowing industry players to promote their products and services, CSM said.

"This year, we will also add the CyberSAFE Programme (Cyber Security Awareness For Everyone) as one of the activities to focus on educating Malaysian Internet users on the importance of cyber-security and to inculcate positive use of the Internet," said Dr Amirudin.

"The CyberSAFE programme started in 2009 and has since reached out to more than 114,000 people nationwide," he claimed.

The participation fee for the two-day conference is RM899 per person and is claimable under the HRDF (Human Resource Development Fund). The early birds rate is RM699 per person if registration is made before July 31.

For more details and to register as a delegate, click here.

For more technology news and the latest updates, follow @btnewsasia on Twitter or Like us on Facebook.

Tahap serius tapi belum mencemaskan

CYBERSECURIY Malaysia menjelaskan bahawa berdasarkan statistik Cyber999, jenayah *scam* di negara ini boleh dikatakan agak serius tetapi belum berada di tahap mencemaskan.

Berdasarkan Statistik Cyber999, analisis kami menunjukkan terdapat peningkatan ke atas Internet scam pada setiap tahun.

Rumusan daripada analisis berdasarkan Statistik Cyber999 menunjukkan bahawa *Internet scam* semakin meningkat di Malaysia dan pengguna perlu berhati-hati serta berwaspada apabila membuat transaksi atau berkomunikasi di Internet terutama dengan orang yang tidak dikenali.

Menurut Ketua Pegawai Eksekutifnya, Dr. Amirudin Abdul Wahab, kebanyakan Internet *scam* berasal dari Negara-negara Afrika dan tidak ada seb mengenai negara yang menerima *scam*.

Mengenai panduan k yang menerima e-mel s beliau menasihati mere mengabaikan atau mem membalas atau memaju tersebut kepada rakan- melaporkan kepada pih seperti kepada CERT, P Perkhidmatan Internet beserta dengan kepala tindakan seterusnya.

Dalam pada itu, beli CyberSecurity Malaysi kepada usaha memaju profesional sebagai Du melalui majikan merek menjalankan program keselamatan siber di o dan keluarga mereka

Children courting danger by sharing info online

by Malati Sirat Posted on October 12, 2013, Thursday

Aaron (right), Ling (second right) and Mustaffa (second left) at the media briefing on the DiGi CyberSAFE Programme yesterday

KOTA KINABALU: Children who share too many details about their house, school and personal information on the Internet will invite certain risks and danger to themselves without knowing it.

CyberSecurity Malaysia content research and development outreach department senior executive Aaron Ikram Mokhtar said the Internet could be used to do research on school reports, communicate with other friends or play interactive games, but every details they share online by that access can also pose hazards.

"The majority of the population in Malaysia are now using mobile phones at a young age due to the rapid acceleration of Internet penetration.

CyberSecurity — pioneer in digital forensic

by KAZI MAHMOOD

LITTLE known to Malaysians is the fact that CyberSecurity, the national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI), is a pioneer in regional digital forensics, a science of the future that will help Malaysia fight cyber crime, said the CEO of the organisation, Dr Amirudin Abdul Wahab last week.

Amirudin said the digital forensic lab under the agency is the only one in existence in Malaysia and in South-East Asia, and has been certified as an international digital forensic lab with regional status that

cation by ASCLD," Amirudin said in an exclusive interview with *The Malaysian Reserve (TMR)* at the agency's headquarters at The Mines recently.

With this credential, it is now possible for Malaysian experts in cybercrime to present evidence and to give their opinion in the country's courts.

This important step has been crossed in the digital forensic science in Malaysia but there are loopholes that will make immense possibilities to solve crimes, whether cyber or otherwise, more difficult. McAfee Inc, the US based anti-virus and Internet security provider estimates that the global cost of

the videos from these cameras are either of very poor digital quality or a number of these cameras there are just used as a deterrent," Amrirudin said.

When a crime happens, we have difficulties to process the images and to identify the culprits. The government has recommended that closed-circuit television's (CCTV) should be placed across the streets and buildings, but the other problem is we have people rushing for the cheapest and lowest quality," Amirudin explained.

Amirudin said the CyberSecurity's forensic division is in the process of proposing to the Malaysian

tion of the culprit in the event of a criminal activity. But nowadays, this is a tough call," Amirudin said.

Based on the organisation's experience with digital videos sent to the agency for identification of criminals, Amirudin said there is the need to upgrade the CCTVs.

He said the current lot of CCTV's installed in some places and buildings were of such poor quality that it defeated the purpose of having such a system around.

CyberSecurity is yet to propose to the government the new standards which the CEO of the

Kerjasama tangani jenayah siber

Cybersecurity Malaysia sedia membantu pihak berkuasa kumpul bukti

Oleh Rosnan Mustaffa

KOTA SAMARAHAN: Cybersecurity Malaysia bersedia membantu pihak berkuasa dalam bersama-sama menangani jenayah siber di negara ini.

Ketua Pegawai Eksekutifnya Dr Amirudin Abdul Wahab berkata, Cybersecurity Malaysia merupakan pusat pakar keselamatan siber nasional di bawah Kementerian Sains, Teknologi dan Inovasi yang bertindak mengenal pasti individu terlibat dalam jenayah siber di negara ini.

"Kita merupakan badan profesional yang bertindak mencari dan mengenal pasti bukti untuk diguna pakai oleh pihak berkuasa menangani masalah jenayah siber di negara ini," katanya.

> "Kita merupakan badan profesional yang bertindak mencari dan mengenal pasti bukti untuk diguna pakai oleh pihak berkuasa menangani masalah jenayah siber di negara ini."

Beliau berkata demikian ketika diminta selepas menggalakkan cerunah kesedaran keselamatan siber anjuran bersama Institut Kuka Bestrak dan Inovasi dan Fakulti Seni Gunaan dan Kreatif Universiti Malaysia Sarawak (UNIMAS) di sini semalam.

Pada masa sama, Amirudin menjelaskan dari Januari hingga Mac tahun ini sebanyak 2,499 kes melibatkan jenayah siber dilaporkan kepada pihaknya.

"Dua kategori jenayah siber yang paling tinggi rundahnya dari tempoh tersebut adalah penipuan melibatkan 1,316 kes dan pencerobohan, 862 kes.

"Justeru, kita sebagai badan profesional tentang perkara ini sentiasa membuka pintu untuk membantu pihak berkuasa mengenal pasti atau mengumpul bukti bagi menangani jenayah siber ini," jelasnya.

Menyentuh mengenai khabar angin atau fitnah yang disebarkan menerusi siber terutamanya pada Pilihan Raya Umum Ke-13 (PRU13) ini, Amirudin memberitahu pihaknya hanya dapat membantu mengumpul bukti dan mengenal pasti individu tidak bertanggungjawab jika diminta atau menerima laporan mengenai perkara itu.

"Untuk mengambil tindakan undang-undang, kita tidak ada mempunyai akta khusus dan tindakan itu akan kita serahkan kepada pihak berkuasa untuk menyelesaikannya kerana kita hanya badan profesional yang mencari bukti dan mengenal pasti pelaku jenayah siber ini," jelasnya lagi.

Terdahulu, dalam ceramahnya yang bertajuk 'Kesedaran Keselamatan Siber,' beliau memberitahu tujuan program itu adalah membentangkan isu serta cabaran di alam siber yang dihadapi masyarakat Malaysia.

Selain itu, katanya, ia sebagai platform berkongsi pengalaman berkaitan kes atau kisah benar serta kajian berkaitan pelbagai insiden di alam siber dan memberikan cadangan etika di dunia siber untuk pemahaman tentang keselamatan siber.

TINGKATKAN KESEDARAN: Amirudin memperjelaskan isu berkaitan keselamatan siber di UNIMAS semalam.

MegaFokus

Manipulasi Internet

Menipu pengguna di alam siber dengan tawaran luar biasa

'Cyber security in Malaysia under control'

KUALA LUMPUR: CyberSecurity Malaysia has given assurance that the cyber security in Malaysia is still under control despite concerns over the increasing number of cyber attacks during the 13th general election process.

Its chief executive officer, Dr Aminuddin Abdul Wahab, said CyberSecurity, Royal Malaysian Police and the Malaysian Communications and Multimedia Commission were always monitoring the situation to ensure peace in the cyber world.

"Internet users need not to worry. All of them, especially the adults, can help maintain peace in the cyber world by adhering to the law while surfing the internet," he said in a statement here.

He said the most important thing that should be done by an internet user to maintain cyber-peace was to be an ethical social citizen when using emails and social websites like Facebook, Twitter and blogs.

"Think rationally. Don't get too emotional and don't simply believe the information spread by unknown sources. Don't simply like, share or forward the information as it tantamounts to spreading lies," he explained.

Meanwhile, Universiti Teknologi Mara communication and media studies faculty lecturer Shahnon Mohamed Saleh said although it cannot be confirmed that cyber attacks would occur during the polling day of the 13th polls tomorrow, it was almost definite that the attacks, should they occur, would not only involve Facebook and Twitter, but also emails.

"The objective for the cyber attacks is to cripple certain software to prevent dissemination of information so that the public won't be able to get the truth," he told Bernama when contacted.

He said the attacks would also be done to steal information from emails, especially those belonged to targeted politicians.

In case of any cyber security incident, Internet users are advised to lodge a report by sending an email to cyber999@cybersecurity.my or by filling the form at http://

Be vigilant against cyber-attacks

...ri Mohd Azumi Mohamed *(right)*

...ssions," he said.

Amirudin also said the exhibition showcases the latest gadgets and solutions in cyber-security. It also provides a one-stop and conducive platform for business matching as well as trade and investment opportunities.

Some of the companies featured include Fortinet, BAE Systems, BDO, Deloitte, ISC8, Kaspersky, Sai Global and Microsoft.

The highlight of CSM-ACE 2013 will be the Malaysia Cyber Security Awards 2013 in recognition of information security professionals, home-grown SMEs and organisations with outstanding contributions to the Malaysian cybersecurity industry.

This year's event also includes CyberSAFE programme as an initiative to educate young Internet users on the importance of cybersecurity and inculcate proper and positive use of the Internet.

It's time to conquer the cyberspace

INVALUABLE BENEFITS: Fourth CSM-ACE to help SMEs tap e-commerce opportunities in secured environment

FREDERICK the Great, King of Prussia, once said the greatest and the noblest pleasure which we have in this world is to discover new truths, and the next is to shake off old prejudices.

This was the most difficult and probably also the easiest thing I may have done since the advent of the Internet. The easiest was to discover the potential and the myriad of opportunities in cyberspace, which is the new truth of the emerging virtual world of the 21st century.

The difficult part was, and continues to be, the challenge to shake off old as well as new prejudices about how we define information confidentiality and privacy, and how we can optimise as well as benefit from the cyberspace.

The Internet permeates every aspect of modern trade, businesses and lifestyles. The potential is beyond one's imagination but what comes with it are the grave cyber-security concerns that inhibit its acceptance as an effective tool for innovation and growth.

As beneficiaries, users or businesses must show confidence and believe that with our National Cyber Security Policy in place, information can be safely relayed and commerce will not be compromised.

With an objective to instil such confidence and create a culture of security, Cyber Security Malaysia will be organising the fourth Cyber Security Malaysia Awards, Conference and Exhibition 2013 (CSM-ACE 2013).

To be held on November 13-14 in Kuala Lumpur, the event is aptly themed "Securing Cyberspace for Economic Growth".

More than 300 delegates and experts are expected to participate in this unique event to share latest cyber security trends, recognise contributions of individuals and organisations in the field of cyber security, and showcase trade investment opportunities by industry players.

The CSM-ACE also aims to inculcate and nurture cyber security awareness among users by educating and offering support for the Malaysian industry, including small and medium enterprises (SMEs), to be self-reliant in terms of technology and human resources. As a strong advocate of innovation and technology, for me this is undoubtedly an event not to be missed by our SMEs.

Hafsah Hashim Speaks

The SMEs should be in the forefront of adopting new technology, especially ICT platforms, and optimising cyberspace opportunities available.

According to Nielson and Paypal Analysis 2011 Report, the online commerce market size is gauged at RM3.63 billion in 2013, and is estimated to increase to RM5.76 billion by 2015.

Similarly, there will be more than 21 million Internet users in Malaysia by 2016. These projections reflect the potential that can be tapped by 49 per cent of the SMEs that are in wholesale and trading as well as manufacturing.

The ACCCIM 2012 SME Survey indicates that 72 per cent of these SMEs are not doing any form of e-commerce.

The SME Census 2011 conducted by the Department of Statistics Malaysia had reported that only 27 per cent of our SMEs used ICT in their business operations, out of which 67 per cent were using the Internet. This further reinforces the fact that there is a dire need for SMEs to increase their business efficiencies and productivity through ICT.

The good news is that Malaysia has developed a positive reputation in the cyber security industry in providing the global solutions. Around 10 per cent of local IT revenue and 30 per cent of export IT revenues are derived from cyber security products and services.

Furthermore, Malaysia has good international cyber security credibility, but is yet to fully capitalise on the lucrative business opportunities through innovative initiatives, such as developing capability for cyber security enforcement through compliance with international standards in areas like e-commerce. SMEs can be the source as well as the beneficiary to such initiatives.

In keeping with the vision and objectives of the government's Digital Transformation Programme, better known as Digital Malaysia, the role of cyber security is paramount to support the nation's move towards a knowledge-based economy (k-economy).

So, to all SMEs out there, grab this opportunity to participate in the CSM-ACE 2013. It offers a wealth of invaluable benefits. Tap on the cyber security's important role as a new source of growth towards transforming your competitiveness on the global platform; gain insights through presentation from various industry experts and panel discussion; network with similar set-ups and expand knowledge of interests; and take in new information on latest trends, topics and ideas for much renewed views on cyber security to further develop your business models.

For more information on CSM-ACE 2013, log on to www.csm-ace.my. Registration closes on Friday.

Datuk Hafsah Hashim is the chief executive officer of Small and Medium Enterprise Corporation Malaysia (SME Corp Malaysia).

A. KEY EVENTS ORGANISED/CO-ORGANISED AT NATIONAL LEVEL

FIRST QUARTER:

1. 7 - 11 January 2013: Information Security Management System (ISMS) MS ISO/IEC 27001:2007 Implementation Course and MS ISO/IEC 27001:2007 Internal Audit course which was organised by National Security Council (MKN) in collaboration with CyberSecurity Malaysia

2. 14 – 18 January 2013: ISMS Implementation Audit Workshop was organized by CyberSecurity Malaysia, National Security Council (MKN) and MAMPU to audit selected agencies on preparation of detailed documentation on ISMS implementation

3. 30 – 31 January 2013: Critical Infrastructure Security Course was organised by CyberSercurity Malaysia and conducted by EC-Council Academy

4. 5 February 2013: Forensic on Internet Application Training organised by CyberSecurity Malaysia aimed to expose forensic officers from Malaysian Communications and Multimedia Commission (MCMC), College University Islam Sultan Azlan Shah and KPerak INC Corporation to forensic inspection and analysis based on unique cases.

5. 25 -28 February 2013: Training for Inland Revenue Board (IRB) organised by CyberSecurity Malaysia aimed as a knowledge sharing session in the areas of digital forensic and current technology

SECOND QUARTER:

6. 8 - 12 April 2013: Workshop on Information Security Management System (ISMS) Implementation Audit was jointly organised with National Security Council (MKN) in an effort to develop and implement a series of programs under National Cyber Security Policy (NCSP) initiative for agencies under Critical National Information Infrastructure (CNII).

7. 15 – 19 April 2013: Digital Forensic Training Program for Royal Malaysian Customs Officers (KDRM)

8. 20 May 2013 : CyberSecurity Malaysia made an honorary visit to the Ministry of Foreign Affairs, Malaysia as part of a series of visits planned for Ministries and Government Agencies to establish closer collaboration in the field of cyber security

9. 11 - 15 June 2013: MS ISO/IEC 27001:2007 Lead Auditor Course &17 – 20 Jun 2013: ISO/IEC 27001:2005 ISMS Implementation Course organised by National Security Council (MKN) in collaboration with CyberSecurity Malaysia

10. 17 - 29 June 2013: Information Security Management System (ISMS) MS ISO/IEC 27001:2007 Implementation Course organised by National Security Council (MKN) in collaboration with CyberSecurity Malaysia

THIRD QUARTER:

11. 2 -4 July 2013: Information Security Management System - ISMS MS ISO/IEC 27001:2007 Internal Auditor Course. CyberSecurity Malaysia in cooperation with National Security Council designed and implemented a program under Development of Capability and Capacity for Enforcement initiative for Critical National Information Infrastructure – CNII agencies.

12. 1-2- July 2013: CyberSAFE in Schools workshop for Bestari Coordination Teachers (CyberSAFE in Schools Powered by DiGi Telecommunication), Teachers Activity Centre Sibu, Sarawak

13. 3-5 July 2013: CyberSAFE workshop in Schools for Bestari Coordination Teacher (CyberSAFE in Schools Powered by DiGi Telecommunication), Teachers Activity Centre Miri, Sarawak

14. 4 July 2013: Cyber Security Awareness Talk at Podium B Hall, Menara Ministry of Youth and Sports, Putrajaya

15. 8-9 July 2013: CyberSAFE in Schools workshop for Bestari Coordination Teachers (CyberSAFE in Schools Powered by Digi Telecommunication), Teachers Activity Centre Pekan, Pahang

16. 10 July 2013: ISMS Certification Closing Ceremony – Malaysian Airline System Berhad. Malaysian Airline System Berhad is now listed as an organization that had successfully obtained MS ISO/IEC 27001:2007 certification

17. 25 July 2013: ISMS Certification Closing

Ceremony – Ministry of Defense Malaysia

18. 3 August 2013 : Tunas Cemerlang 2013 "Raya Shopping" with underprivileveged children of Bait Al-Amin from Parit, Perak and Contribution of Hari Raya donations to Teachers of Bait Al-Amin and students of University Petronas

19. 19-21 August 2013 : Incident Handling and Network Security Training for X-Maya Drill

20. 2- 5 September 2013: Information Technology and Communication Exhibition during Software Testing Conference (SOFTEC) 2013

21. 5 September 2013: Customer Relations Management System Application Usage Workshop for Law Enforcement Agencies.

22. 20 September 2013 : An Integrated Approach for Cyber Security and Critical National Information Infrastructure Protection Talk

23. 21 September 2013 : Creativity and Science4U Program at Sekolah Menengah Kebangsaan Tun Haji Abdul Malek, Cheng, Melaka (Parliament Tangga Batu)

FOURTH QUARTER:

24. 21 – 22 October 2013: CyberSecurity Malaysia has organised Advanced Information Reconnaissance: Open Source Intelligence and Information Gathering Techniques Course for Inland Revenue Board, State of Perak branch at Perak Techno Trade Centre (PTTC), Ipoh Perak

25. 7 – 8 November 2013: Operation Spyglass (KL Gangster 2). It is one of the support services provided by CyberSecurity Malaysia to the Law Enforcement Agencies in the form of digital forensic examination

26. 13 - 14 November 2013: Cyber Security Malaysia - Award, Conference and Exhibition (CSM-ACE) 2013 at Royale Chulan, Kuala Lumpur

27. 18 – 22 November 2013: First Responder Training Program for Bank Negara Malaysia

28. 19 -21 November 2013: Training to Introduce New Edition of ISMS, ISO/IEC 27001:2013

29. 25 – 27 November 2013: National Cyber Crisis Exercise (X-MAYA 5). It is one of the training programs conducted under the National Cyber Security Policy, specifically under Thrust 7 - Cyber Security Emergency Readiness; which has National Security Council (MKN) as the Thrust Leader

30. 4 - 5 December 2013: ICT Product Security Assessment (IPSA) Workshop

31. 9 – 20 December 2013: Intensive Course to Indonesian Security Incident Response Team on Internet and Infrastructure/Coordination Center (Id-SIRTII/CC)

B. SUPPORTED SEMINARS/CONFERENCES AT NATIONAL LEVEL

1. **22 February 2013** - Regional ICT Conference
2. **12 March 2013** - Business Online New Opportunities
3. **13 – 15 March 2013** - Cyber Intelligence Asia 2013
4. **18 – 19 June 2013** - IT Governance 2013 & Conference
5. **27 – 29 August 2013** - ZebraCON 2013
6. **11 – 13 September 2013** - CyberSec Asia

C. KEY EVENTS CO-ORGANISED AT INTERNATIONAL LEVEL

1. Annual Conference of Asia Pacific Computer Emergency Response Team (APCERT)

- CyberSecurity Malaysia had participated in the Annual General Meeting (AGM) and Conference of the Asia Pacific Computer Emergency Response Team (APCERT): www.apcert.org, a body of 30 Computer Security Incident Response Teams (CSIRTs) members from 20 countries across the Asia Pacific region.
- At the APCERT AGM and Conference which was held in Brisbane, Australia; CyberSecurity Malaysia was once again elected as the Steering Committee for two terms from 2013 to 2015.
- CyberSecurity Malaysia's selection to the APCERT Steering Committee is an achievement. It is also an acknowledgement of CyberSecurity Malaysia's leadership, professionalism and technical expertise.
- CyberSecurity Malaysia's involvement in international arena creates opportunities for continuous implementation of various cyber security programs and initiatives based on the mandate given by the Malaysian government. CyberSecurity Malaysia also takes this opportunity to forge closer relationship and cooperation with other global organizations to collectively protect global cyber security.

2. 10 September 2013 – System Stability and Electronic Transaction Forum

- The forum that was held in Harris Convention Centre, Bandung Indonesia was officiated by Ashwin Sasongko, Director General, Informatics Application, Republic Indonesia.
- It was attended by 700 participants consisting of ICT practitioners and experts, private companies, public sector, academicians as well as university students.
- This forum created bilateral cooperations between CyberSecurity Malaysia and Indonesia. It also allowed information sharing on cyber security in Malaysia and at the same time promoted services offered by CyberSecurity Malaysia.

3. 10 -12 September 2013 : ASEAN Regional Forum (ARF) On Measures To Change Cyber Security – Legal and Cultural Aspects, Beijing, China.

- This forum was co-chaired by China and Malaysia (represented by National Security Council).
- 60 delegates attended this two-day forum from 18 ARF member countries, European Union and ASEAN Secretariat. Malaysian delegation presented 4 papers including two papers by CyberSecurity Malaysia namely: 'The Roles of States in Cyber Space' by Zahri Hj. Yunos, Chief Operating Officer, and 'Capacity Building in Enhancing Cyber Security' by Lt. Col. Sazali Sukardi (Retired), Vice President Strategic Research.
- Two more presentation was by National Security Council titled Recent Development of National and Regional Practice On Cyber Security and by Malaysia Communication and Multimedia Commission titled Cultural Dimensions in Cyber Space.
- CyberSecurity Malaysia's representative also shared their knowledge and experience based on their respective expertise in cyber security related issues. Those views presented are capable of providing impact on regional cyber security outlook.
- CyberSecurity Malaysia's involvement in this forum showcased its leadership as a leading cyber security agency in Malaysia. It also highlighted the Nation's commitment of supporting international community in handling cyber security related issues and threats.

4. 10 – 13 September 2013 : 14th International Common Criteria Conference (ICCC 2013)

- 14th International Common Criteria conference organized by National Information Assurance Partnership (NIAP) was held in Orlando, Florida, United States on 10-12 September 2013.
- The conference was coordinated by Certification bodies that represent Arrangement on the Recognition of Common Criteria Certificates in the areas of IT security.
- During this conference, CyberSecurity Malaysia promoted Malaysian Common Criteria Evaluation and Certification (MyCC) scheme.
- This conference was an opportunity for

CyberSecurity Malaysia to rub shoulders with other international Certification Bodies and Evaluation Facilities.

- This opportunity was taken to ensure Malaysia is continued to be recognized and also to make it easier for Malaysia to participate in other international conferences.
- Additionally, this was also a platform to introduce CSM-MySEF lab to other countries. Success of MySEF in evaluating smart card operating system in establishing smart card as National Identity was also shared during this conference.

5. 11 - 12 November 2013: Regional Asia Information Security Exchange - RAISE Forum Meeting

- RAISE Meeting is an annual event since 2004. Members of RAISE including countries such as Singapore, Taiwan, Korea, Japan, China, Hong Kong and Malaysia.
- The purpose of RAISE is to provide a platform to share information, exchange ideas and hold dialogues on information security; discuss standards development activities and ensure the unique needs of Asian region are taken into account during international standards development.

6. 18 – 20 November 2013: Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) 2013 Annual Conference and 5th Annual General Meeting (AGM)

- OIC-CERT is cooperation amongst the OIC countries in the field of cyber security. To date, members of OIC-CERT consist of 24 computer emergency response teams (CERT) or cyber security relevant agencies from 19 OIC countries, 3 commercial companies, one professional and one honorary member from the field of cyber security.
- Since OIC-CERT's official inception in 2009, the cooperation has successfully organised 4 annual conferences and AGMs. In 2013, the 5th OIC-CERT AGM was held in Bandung, Indonesia on 18 - 20 November 2013.
- Below are the outcomes of OIC-CERT Annual Conference and the 5th AGM 2013:
  i. Appointment of Oman as the Chairman of OIC-CERT and Driving Committee Members of OIC-CERT for the period of 2013 – 2015
  ii. Appointment of Malaysia as OIC-CERT Permanent Secretariat
  iii. Appointment of General Tan Sri Dato' Seri Panglima Mohd Azumi Mohamed (Retired), Chairman, Board of Directors, CyberSecurity Malaysia as the advisor to OIC-CERT Chairman.

D. LOCAL AND INTERNATIONAL VISITS RECEIVED

CyberSecurity Malaysia also receives dignitaries, international visitors, students/researches and representatives from various organizations at our premises as part of our customer service and branding activities, as well as to form an understanding between the visiting parties and CyberSecurity Malaysia. Guests are briefed about our roles and services. Below is the list of guests received in 2013:

No.	Date (2013)	Description of guests
1	14 March	In conjunction with Cyber Intelligence Asia 2013 Conference, Mr. Howard Schmidt, Former Special Assistant to President, Cyber Security Coordinator, Executive office of President Obama, United States made his first official visit to CyberSecurity Malaysia
2	10 Apr	Visit by Royal Malaysian Navy Officers from KD Pelanduk to CyberSecurity Malaysia
3	30 Apr	Visit from Software Engineering Students of University Pendidikan Sultan Idris (UPSI), Perak
4	06 May	Visit by Honorable Dr Hamed Salim Al-Rahwi Information Technology Authority (ITA) Board Member and Delegates from Oman
5	22 May	Visit by Students from UiTM, Shah Alam
6	10 Jun	Follow Up Visit by Digital Forensic Course Students
7	02 Jul	Visit by Information Technology Centre TD (PUSTEKMA TD), Army Headquarters, Wisma Pertahanan Jalan Padang Tembak, Kuala Lumpur
8	18 Jul	Meeting and Visit by Social Media Monitoring Technical Committee Volume 3 2013 at CyberSecurity Malaysia
9	5 Aug	Maiden visit to CyberSecurity Malaysia by YB Datuk Dr. Abu Bakar bin Mohamad Diah, Deputy Minister Science Technology and Innovation
10	28 Aug	Study visit in conjunction with ICT Data Storage and Security Officers and Staff of Hulu Langat District Education Department (Group 1) Course
11	29 Aug	Learning visit by Students and Lecturers of Multimedia University to CyberSecurity under Centre of Diploma Program
12	25 Sep	Visit from Ministry of Information and Communications, Vietnam
13	03 Oct	Visit from National Information Technology Agency, Senegal
14	23 Oct	Visit from the Ministry of Science and Technology, Republic of Uganda

E. PROFESSIONAL CERTIFICATIONS

Below is the list of CyberSecurity Malaysia's employees who obtained professional certifications in 2013. The list is arranged in chronological order (by month).

No	Name	Department	Certification	Date/ Month
1	Nuur Ezaini Akmar Ismail	SA	Certified Ethical Hacker	Jan-2013
2	Nur Sharifah Idayu Mat Roh	SA	Certified Ethical Hacker	Jan-2013
3	Syafiq' Aizat Abdul Wahab	SA	Certified Ethical Hacker	Jan-2013
4	Maslina Daud	CSPS	Certified Information Security Manager (CISM)	Jan-2013
5	Teoh Chooi Chi	NORTHERN	Certified Business Continuity Professional (CBCP)	Jan-2013
6	Muhammad Muttaqin Abd Aziz	STS	Certified Ethical Hacker	Feb-2013
7	Noor Azwa Azreen Abd Aziz	SPR	Associate Business Continuity Professional (ABCP)	Mar-2013
8	Lim Jun Yi	MyCERT	GIAC Reverse Engineering Malware (GREM)	Mar-2013
9	Wan Zariman Omar	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Apr-2013
10	Hazlin Abdul Rani	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Apr-2013
11	Kamarul Baharin Khalid	SA	EC-Coucil Certified Encryption Specialist (ECES)	Apr-2013
12	Ahmad Dahari Jarno	SA	EC-Coucil Certified Encryption Specialist (ECES)	Apr-2013
13	Norahana Salimin	SA	EC-Coucil Certified Encryption Specialist (ECES)	Apr-2013
14	Zarina Muda	SA	EC-Coucil Certified Encryption Specialist (ECES)	Apr-2013
15	Mohammad Noorhisyam Muda	SA	GIAC Secure Software Programmer -Java (GSSP-Java)	Apr-2013
16	Saiful Syazwan Yaakob	SA	Certified Ethical Hacker	Apr-2013
17	Mukhriz Hamzah	SA	Certified Ethical Hacker	Apr-2013
18	Nor Liyana Azman	SA	Certified Ethical Hacker	Apr-2013
19	Yati Mohamad Yasin	GE	ISO 22301 Lead Auditor BCM	Apr-2013
20	Fazlan Abdullah	GE	ISO 22301 Lead Auditor BCM	Apr-2013
21	Sharifah Sajidah Syed Noor Mohammad	HCD	ISO 22301 Lead Auditor BCM	Apr-2013
22	Ida Rajemee Ramlee	SMBP	ISO 22301 Lead Auditor BCM	Apr-2013
23	Nazhalina Nazri	SMBP	ISO 22301 Lead Auditor BCM	Apr-2013
24	Salman Abdul Wahab	ISPD	ISO 22301 Lead Auditor BCM	Apr-2013
25	Mohd Syamsyul Shuib	APS	ISO 22301 Lead Auditor BCM	Apr-2013
26	Nuzeita Hashim	SMBP	ISO 22301 Lead Auditor BCM	Apr-2013
27	Syafiqa Anneisa Leng Abdullah	SMBP	ISO 22301 Lead Auditor BCM	Apr-2013
28	Siti Hajar Mohamad Ali	SMBP	ISO 22301 Lead Auditor BCM	Apr-2013
29	Sabariah Ahmad	SMBP	ISO 22301 Lead Auditor BCM	Apr-2013

No	Name	Department	Certification	Date/ Month
30	Wan Nasra Wan Firus	ISCB	ISO 22301 Lead Auditor BCM	Apr-2013
31	Noor Aida Idris	SMBP	ISO 22301 Lead Auditor BCM	Apr-2013
32	Nor Safwan Amirul Salleh	SA	Certified Ethical Hacker	Apr-2013
33	Nurul Izratul Zolkafle	SA	Certified Ethical Hacker	Apr-2013
34	Abdul Qaiyum Hamzah	SA	Certified Ethical Hacker	Apr-2013
35	Noraziah Anini Mohd Rashid	SA	Certified Ethical Hacker	Apr-2013
36	Hafizah Che Hasan	SA	SANS Gweb	May-2013
37	Shazil Imri Mohd Hizam	SA	SANS Gwapt	May-2013
38	Sarah Abd Rauf	MyCERT	Comptia Security +	May-2013
39	Juanita Abdullah Sani	MyCERT	Comptia Security +	Jun-2013
40	Abdul Alif Zakaria	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Sept-2013
41	Liyana Chew Nizam Chew	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Sept-2013
42	Nor Azeala Mohd Yusof	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Sept-2013
43	Isma Norshahila Mohammad Shah	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Sept-2013
44	Suhairi Mohd Jawi	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Sept-2013
45	Norul Hidayah Omar	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Sept-2013
46	Nik Azura Nik Abdullah	CTR	EC-Coucil Certified Encryption Specialist (ECES)	Sept-2013
47	Nur Aishah Mohamad	DF	Computer Hacking Forensic (CHFI)	Sept-2013
48	Mohd Nor Akashah Mohd Kamal	STS	EC-Coucil Certified Security Analyst (ECSA)	Sept-2013
49	Nurul Husna Binti Mohd Nor Hazalin	STS	EC-Coucil Certified Security Analyst (ECSA)	Sept-2013
50	Wan Nasra Wan Firus	ISCB	Comptia Security +	Oct-2013
51	I.D Safairis Amat Noor	ISCB	Comptia Security +	Oct-2013
52	Nur Shazwani Zakaria	ISCB	Comptia Security +	Oct-2013
53	Yusrun Fitri Yaziz	CAIT	Certified Ethical Hacker	Nov-2013
54	Yati Mohamad Yasin	GE	Associate Business Continuity Professional (ABCP)	Dec-2013

F. PUBLISHED TECHNICAL PAPERS AND ARTICLES

Below is the list of technical papers and articles authored or co-authored by employees of CyberSecurity Malaysia. In this list, only the names of CyberSecurity Malaysia's employees are mentioned as authors. Please refer to the actual publication for complete list of authors.

No	Title	Author/s	Publication	Date
1.	A Survey About Impacts of Cloud Computing on Digital Forensics	Dr. Solahuddin bin Shamsuddin	International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 77-94	January
2.	Integrated framework of software engineering and common criteria practices.	Khairunnisa Osman	International Journal of Computer Science Engineering and Technology (IJCSET) - March 2013 | Vol 3, Issue 3, 64-70	March
3.	Definition and framework of cyber terrorism	Zahri Yunos & Noor Azwa Azreen Abd Aziz	SEARCCT Selection of Articles Volume 1	26 -March
4	Multiple Frames Combination Versus Single Frame Super Resolution Methods for CCTV Forensic Interpretation	Nazri A. Zamani	Journal of Information Assurance and Security 06/2013	27 -June
5	Digital Camcorder Forensics	Dr. Aswami Fadillah bin Ariffin	Eleventh Australasian Information Security Conference (AISC 2013), Adelaide, Australia (CRPIT Volume 138 - Information Security 2013)	16 -July
6	A Proxy-based Adaptive Security Implementation for SSL Ecosystem	Suhairi Mohd Jawi	Kolokium Siswazah Sains Komputer dan Matematik Peringkat Kebangsaan 2013	4 -September
7	Randomness analysis of grain-128 stream cipher	Norul Hidayah Lot	International Conference on Mathematical Sciences and Statistics 2013 (ICMSS2013)	27-September
8	Cyber Security As A Central Strategy to National Sovereignty And Economy	Dr Amirudin Abdul Wahab and Lt. Col. Sazali Sukardi [R]	ICT Strategic Review 2013/14 The Digital Opportunity	October
9	Data Recovery from Proprietary Formatted Cctv Hard Disks	Dr. Aswami Fadillah bin Ariffin	IFIP Advances in Information and Communication Technology Volume 410, 2013, pp 213-223	10-October
10	Object Signature Search for Capturing Processes Memory Image of Windows System	Khairul Akram Zainol Ariffin [Research]	International Journal of Computer and Communication Engineering	6 -November
11	iOS Forensics: How can we recover deleted image files with timestamp in a forensically sound manner?	Dr. Aswami Fadillah bin Ariffin	FARES 2013 : The Eight International Workshop on Frontiers in Availability, Reliability and Security	8-November
12	Automated Enhancement Tool For Malware Incident Handling	Nur Mohammad Kamil & Sharifah Roziah Mohd Kassim	International Conference on Artificial Intelligence and Computer Science 2013	26 -November
13	Holistic Approach for Memory Analysis in Windows System	Khairul Akram Zainol Ariffin and Dr Solahuddin Shamsuddin	Open Access Journal of Information Systems (OAJIS)	4 -December

G. LIST OF PRESENTATIONS AT INTERNATIONAL LEVEL

No	Name	Presentatation title	Name of Conference, Seminar	Location	Date (2013)
1	Jazannul Azriq Aripin & Mohamad Nizam Kassim	CyberSAFE Approach and 5 Effective Strategic Cyber Parenting	Social Harm Prevention: Emerging Social Harms, Theories and Strategies Conference	Iran	3-March
2	Zahri Yunos	Cyber Terrorism: Threat to Critical National Information Infrastructure.	Cyber Defence Summit	Muscat, Oman	4-March
3.	Zahri Yunos	Mobile & Cloud Security	APCERT Public Conference Panel Discussion	Brisbane, Australia	24-March
4.	Sharifah Roziah Mohd Kassim	In-house Developed Tools to Enhance Incident Response - Sharing MyCERT's Experience	FIRST Technical Colloquium (TC)	Cisco Campus, Amsterdam	3-April
5.	Zahri Yunos	Malaysia's National Cyber Security Policy - An Integrated Approach For Cyber Security And Critical National Information Infrastructure Protection	Cyber Secure Pakistan 2013	Islamabad. Pakistan	18-April
6.	Mohd Zabri Adil Talib / Fauzi Mohd Darus	NTFS Forensic Analysis Workshop	CyberSecure Pakistan 2013	Islamabad, Pakistan	18-April
7.	Mohd Zabri Adil Talib	Cyber CSI: Admissibility of electronic evidence	CyberSecure Pakistan 2013	Islamabad, Pakistan	20-April
8.	Syahrir Mat Ali	The Role Of Enterprise In Ensuring Cyber Security The Malaysian Experience	Cards And Payments Asia 2013 Conference	The Marina Bay Sands, Singapore	24-April
9.	Zahri Yunos	Child Online Protection - CyberSecurity Malaysia Initiatives.	Child Online Protection in MENA & South East Asia, World Summit in Information Society 2013	Geneva (via web cast)	16-May
10.	Lt. Col. Sazali Sukardi (Retired)	Cyber Dimension	The 12th Iiss Asia Security Summit The Shangri-La Dialogue 2013	Shangri-La Hotel, Singapore	1-June
11.	Maslina Daud	A focus on mitigation and namagement of cyber threats	Business Continuity Planning & Crisis Management for Financial Institutions	Singapore	13-June

H. LIST OF PRESENTATIONS AT NATIONAL LEVEL

No	Name	Presentatation title	Name of Conference, Seminar	Location	Date (2013)
1	Dr. Solahuddin Shamsuddin	Integrating Inter Agency Efforts Effectively to Enhance Cyber Security	Cyber Security for Government Asia	Novotel Hotel, Kuala Lumpur	29-January
2	Norul Hidayah Ahmad Zawawi	Randomness Analysis on Grain-128 Stream Cipher	International Conference on Mathematical Science and Statistics 2013 (ICMSS2013)	Sunway Putra Hotel, Kuala Lumpur	6-February
3.	Nik Azura Nik Abdullah	Statistical Analysis on LBlock Block Cipher	International Conference on Mathematical Science and Statistics 2013 (ICMSS2013)	Sunway Putra Ho-tel, Kuala Lumpur	6-February
4.	Norhazimah Abdul Malek	Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme	MyCC Awareness Workshop	One World Hotel	7-February
5.	Hasnida Zainuddin	Enhance Trust and Confidence in e-Business	Regional ICT Conference & Chinese New Year "Lou Sang" Dinner	Kinta Riverfront Hotel & Suites, Ipoh	22-February
6.	Hasnida Zainuddin	Malaysia Trustmark Application Process Briefing	Business Online…New Opportunities	Kinta Riverfront Hotel & Suites, Ipoh, Perak	12-March
7.	Zahri Yunos	Cyber Terrorism	Cyber Intelligence Asia	Kuala Lumpur, Malaysia	12-March
8.	Sabariah Ahmad	Bringing together All Stakeholders in the Fight against Cyber Threats	InfoSec Asia 2013 Conference;	PWTC KL;	21-March
9.	Lt. Col. Sazali Sukardi (Retired)	Utilization Of Data Mining Techniques To Prevent And Employee From Committing A Fraud	Internal Fraud Investigation & Control By The Asian Strategic And Leadership Institute	Chorus Hotel, Kuala Lumpur	9-April
10.	Lt. Col. Sazali Sukardi (Retired)	Cyber Terrorism	Seminar Siasatan Jenayah Siber Siri 1/2013 Bahagian Penguatkuasa Kementerian Perdagangan Koperasi Dan Kepengunaan	Rainbow Paradise Beach Resort, Pulau Pinang.	16-April
11.	Lt. Col. Sazali Sukardi (Retired)	Cyber Security And E-Crime	E-Crime Conference By The Asian Strategic And Leadership Institute	Sunway Putra Hotel, Kuala Lumpur	16-May

No	Name	Presentatation title	Name of Conference, Seminar	Location	Date (2013)
12.	Lt. Col. Sazali Sukardi (Retired)	The Cyber Media And Information Management - The Armed Forces Situation	The Seminar By The Malaysia Armed Forces Staff College	The Malaysia Armed Forces Staff College, Mindef	20-May
13.	Lt. Col. Sazali Sukardi (Retired)	The Cyber Security Challenges To The Malaysian Armed Forces	The Malaysian Navy Senior Officers' Seminar	The Naval Base, Lumut, Perak	21-May
14	Hasnida Zainuddin	Enhance Trust And Confidence In E-Business	Business Online…New Opportunities	Sunway Carnival Convention Centre, Seberang Jaya, Pulau Pinang	22-May
15.	Lt. Col. Sazali Sukardi (Retired)	Malaysia's Cyber Security Landscape	Southeast Asia Regional Centre For Counter-Terrorism (Searcct)	The Royale Bintang, Kuala Lumpur	28-May
16.	Lt. Col. Sazali Sukardi (Retired)	Malaysia's Cyber Security Landscape	Ministry Of Foreign Affairs, Malaysia In Collaboration With The International Cooperation Department Of The Ministry Of Interior, France	The Royale Bintang, Kuala Lumpur	28-May
17.	Carrine Teoh	Online Business With Malaysia Trustmark	World Mobile Payment, Remittances & Financial Inclusion Conferece 2013	Ritz Carlton, Kuala Lumpur	13-June
18.	Norhazimah Abdul Malek	Malaysian Common Criteria Evaluation & Certification (Mycc) Scheme	Mycc Awareness Workshop	One World Hotel, Kuala Lumpur	18-June
19.	Ismamuradi Dato' Hj Abdul Kadir	Mosti Pre-Commercialisation Grant Application	Mycc Awareness Workshop	One World Hotel, Kuala Lumpur	18-June
20.	Lt. Col. Sazali Sukardi (Retired)	Cyber War And Cyber Attack	The Seminar By The Malaysian Armed Forces Defense College	The Malaysia Armed Forces Staff College, Mindef	19-June
21.	Noor Aida Idris	Information Security Awareness	Bank Negara Malaysia Risk Management Day	BNM, KL	22-August
22.	Suhairi Mohd Jawi	A Proxy-Based Adaptive Security Model for SSL Ecosystem	Siswazah Kolokium Perinkat Kebangsaan 2013 (SISKOM2013)	UiTM Shah Alam, Selangor	28-August

No	Name	Presentatation title	Name of Conference, Seminar	Location	Date (2013)
23.	Lt. Col. Sazali Sukardi (Retired)	Staying Ahead of the Game - The Future of Cyber Security in Malaysian Financial Services	KL Security Conference, Technology & Innovation – the Future of Security in Financial Services	Prince Hotel and Residence on	29-August
24.	Fazlan Abdullah	Cyber security Issues and challenges	Hari Keselamatan Perlindungan Negeri Kedah Tahun 2013	Wisma Perseku-tuan, Alor Setar , Kedah	3-September
25.	Lee Hwee Hsiung	Chairperson for the Summit, • Opening keynote address • Roundtable discussion/ presentation on CIO roles and responsibilities • Roundtable discussion/ presentation on Big Data initiatives	3rd. Annual Information Security Summit	Royale Chulan KL	3-September
26.	Muhamad Izwadee Bin Hamzah	CSM-ACE 2013	Seminar: "Business Online…New Opportunities"	Grand BlueWave Hotel Johor Bahru	17-September
27.	Hasnida bt Zainuddin	Online Business with Malaysia Trustmark	Seminar: "Business Online…New Opportunities"	Grand BlueWave Hotel Johor Bahru	18-September
28.	Muhammad Reza Bin Mohd Shariff	Cyber Trends and Its Impact	Seminar: "Business Online…New Opportunities"	Grand BlueWave Hotel Johor Bahru	19-September
29.	Zahri Bin Yunos	An Integrated Approach for Cyber Security and Critical National Information Infrastructure Protection	An Integrated Approach for Cyber Security and Critical National Information Infrastructure Protection	Universiti Curtin, Miri, Sarawak	20-September
30.	Syahrir Mat Ali	Facebook: Keeping It Safe and Social	Technology Update Seminar	INTAN Sarawak, Kota Samarahan	26-September
31.	Dr. Solahuddin Shamsuddin	"White Color Crime: Staying One Step Ahead of the Perpetrators".	4th International Cyber & Economic Crimes Conference / White Color Crime: Staying One Step Ahead of the Perpetrators	Park Royal KL	22-October

EDITORIAL COMMITTEE

Advisor:
Zahri Bin Hj. Yunos
Chief Operating Officer

Reviewer:
Lt. Col. Mustaffa bin Ahmad (Retired)
VP, Outreach and Capability Building Division

Mohd. Shamil Mohd Yusoff
Head, Outreach and Corporate Communications

Editor:
Sandra Isnaji
Manager, Outreach and Corporate Communications

Layout artists & graphic designers:
Zaihasrul Ariffin
Senior Analyst, Secure Technology Services Department

Nurul 'Ain Zakariah
Executive, Secure Technology Services Department

Content Contributors:
Abd. Rouf Mohammed Sayuti
Head, Internal Audit Department

Azlin Samsudin
Senior Executive, Legal and Secretarial Department

Ernieza Ismail
Senior Executive, Strategy Management Department

Azrina Md. Saad
Senior Executive, Finance Department

Nur Nadira Mohamad Jafar
Executive, Procurement and Logistics Department

Photographer:
Zul Akmal Manan
Executive, Outreach and Corporate Communications

FORM OF PROXY

CyberSecurity MALAYSIA

(Company No. 726030-U)

*I/We .....

of.....

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

.....

of .....

or failing him / her .....

of .....

as *my / our proxy to vote for *me / us on my / our behalf at the 8th Annual General Meeting of the Company to be held at the Board Room of the Company, Level 7, Sapura@Mines, No. 7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor on the ..... day of ..... 2014 time ..... and at any adjournment hereof.

Signed this .....day of 2014

(Signature of Appointor)
*Delete whichever is not desired

Notes :

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

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

3. To be valid the proxy duly completed must be deposited at the Registered Office of the CyberSecurity Malaysia at Level 5, Sapura@Mines, No. 7 Jalan Tasik, The Mines Resort City, Seri Kembangan, 43300 Selangor Darul Ehsan, Malaysia not less than forty-eight (48) hours before the time for holding the meeting.

This page is intentionally left blank

CONTACT INFORMATION

Emails:

To report cyber security incidents	:	cyber999@cybersecurity.my
General enquiry	:	info@cybersecurity.my
Training enquiry	:	training@cybersecurity.my
Media Inquiry	:	media@cybersecurity.my

Address:

Corporate Office	:	CyberSecurity Malaysia, Level 5, Sapura@Mines, No. 7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia. **GPS Coordinate:** 3.03648, 101.709386 Phone: +603 - 8992 6888 **Fax:** +603 - 8992 6841
CyberSecurity Malaysia - Northern Regional Office Product Development and Marketing Department	:	Level 19, Perak Techno-Trade Centre Bandar Meru Jaya, Off Jalan Jelapang 30020 Ipoh, Perak Darul Ridzuan Malaysia **GPS Coordinate:** 4.665146, 101.074746 **Phone:** +605 - 528 2088 **Fax:** +605 - 528 1905

Corporate Office:
CyberSecurity Malaysia
Level 5, Sapura@Mines
No. 7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

Tel: +603 8992 6888
Fax: +603 8992 6841
Email: info@cybersecurity.my
Customer Service Hotline: 1300 88 2999
www.cybersecurity.my

©CyberSecurity Malaysia 2014 - All Rights Reserved

People First, Performance Now

Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

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

Status Company

Best Child Online Protection Website