CyberSecurity MALAYSIA

ANNUAL REPORT 2012

Table of Content

Corporate Information

CyberSecurity Malaysia (www.cybersecurity.my) is the national cyber security specialist agency. Previously known as the National ICT Security and Emergency Response Centre (NISER), which was launched in 2001; CyberSecurity Malaysia became an agency under the purview of the Ministry of Science, Technology and Innovation (MOSTI) in 2005 as a national body to monitor aspects of National e-Security. CyberSecurity Malaysia provides the following core services in the field of cyber security:

- Emergency response, incident handling, and digital forensics
- Quality management
- Capability and capacity development
- Outreach and acculturation
- Research and risk assessment
- Evaluation and certification

VISION

Our vision is to be a globally recognised National Cyber Security Reference and Specialist Centre by 2020.

MISSION

Our mission is to create and sustain a safer cyberspace to promote National Sustainability, Social Well-Being and Wealth Creation.

CORE VALUES

Our core values are Trust, Impartiality and Proactive.

Trust:
By maintaining social, ethical and organisational norms; we firmly adhere to codes of acceptable conduct and professional ethical principles.

Impartiality:
By providing consultation, advice and decision making with professionalism based on established facts and rationale, and devoid of any personal or conflict of interest and bias.

Proactive:
By taking prompt action to accomplish objectives; anticipating challenges and identifying early solutions; taking action to achieve goals beyond what is required or expected.

CLIENT'S CHARTER

In order to accomplish our vision, as our client, you are our priority and we aim to do this through three main areas of focus: Service, Quality and Relationship.

Service:
In delivering our services to you, we adopt values that are aligned with our approach and we ensure professionalism in carrying out our work.

We are RESOURCEFUL. We understand that there is no single solution that could fit all or solve every problem. Therefore, we treat each case or problem as special and we search for creative solutions that are practical and appropriate. With CyberSecurity Malaysia, you can be assured of a personalised and careful solution approach.

We are PROACTIVE. We take the initiative to be forward thinking and progressive when confronting problems in our work. We know that in cyber security, this is the right way of doing things.

We are RESPONSIVE. No matter how complex or difficult a problem is, we will rise to the challenge. It is our responsibility to keep Malaysia's cyberspace safe and secure at all times.

Quality:

We always strive to reach for higher levels of quality in service. We truly believe that this is the only way to ensure we remain at the forefront of the industry.

We are IMPARTIAL. No matter how big or small the problem or case might be, we handle it with impartiality and give it the due attention. We provide fair and unbiased support, advice and information.

We SPECIALIZE. In order to ensure that you fully benefit from our services, we do everything to the best of our capabilities. We are focused and will not be distracted by issues that will adversely affect our performance.

We are EFFECTIVE. In order to maintain the highest level of service, we strive to deliver sound professional advice and reliable service every time you need us.

Relationships:

Beyond normal operations, our success also hinges on the relationship that we develop with our clients and amongst each individual at CyberSecurity Malaysia.

This is our main driver towards excellence.

We strive to be TRUSTWORTHY. Everything we do is focused on one primary goal, and that goal is to keep you safe. We are here to safeguard your needs and interests as well as that of the larger community. In doing so, we will gain your trust and confidence.

We are PASSIONATE. We take pride in our work and our rapport with all clients. Working together, we believe we can truly secure our nation's cyber security.

We SUPPORT each other. Each of us plays a role in helping to solve your problem. We collaborate and share our expertise and experience so that you benefit from the collective skills that we can offer.

Chairman's Statement

Chairman's Statement

Our lives have grown increasingly intertwined with the Internet and even more so with the pervasiveness of mobile Internet usage by the public, in the form of netbooks, smartphones and tablets. While it offers benefits, the flip side of this interconnectedness is a security vulnerability that has huge social and economic ramifications, given that the global cyber security market could be worth up to USD 80 billion by 2017, according to a report based on a worldwide cyber security market research by the Global Industry Analysts, Inc.

At CyberSecurity Malaysia, we are mindful of the need to protect our citizens from cyber threats. In 2012, we continued to provide technical expertise and emergency response services. We also intensified our efforts in educating the general public via our CyberSAFE programme, especially in the protection of innocent children.

In pursuing our vision to be a globally recognised, national cyber security reference and specialist agency, I am pleased to report that we have made further inroads into the international scene.

CyberSecurity Malaysia was appointed as the Secretariat of the OIC-CERT (The Organisation of the Islamic Cooperation – Computer Emergency Response Team) for the 2013-2015 terms. This is on top of the Chair position that we are already holding. The dual position displays the confidence and trust that we have gained from the OIC-CERT members.

In addition, our Child Online Protection efforts received international recognition. The CyberSAFE website of CyberSecurity Malaysia received the Saramad Golden Award, the highest award at the 6th International Digital Media Fair and Festival 2012 (IDMF2012) in Tehran, Iran; for being the best Child Online Protection portal out of 148 digital media.

We acknowledge that cyber attacks in a borderless cyber world represent a challenge to cyber security players. Against this backdrop of increased threats, cyber security organisations need to collaborate and cooperate. Thus, in 2012, we expanded our collaborative efforts to Africa by having a working affiliation with the AfricaCERT via the OIC-CERT platform. Coupled with the good relationship with Oman, which is the Cyber Security Regional Center for the Arab nations, this will further boost our professional connection with other players in the international arena.

As the Chair of OIC-CERT and CyberSecurity Malaysia, I have had the opportunity to participate as a speaker at two international events listed below. I believe it shows that the international community and organisations recognise CyberSecurity Malaysia as a frontrunner in the field of online security.

1. Gulf International Cyber Security Symposium, at The Jumeirah Beach Dubai, UAE (9 - 10 December 2012)
2. OIC-CERT Annual Conference & AGM 2012 - CyberSecurity Against Emerging Threats, at Al-Bustan Palace-a-Ritz Carlton Hotel, Muscat Oman (29 - 31 December 2012)

2012 was another successful year of fulfilling our role as a guardian to Malaysia's cyber world. One couldn't emphasise enough the importance of safe and quality practices when it comes to protecting the nation from nefarious cyber criminals. Hence, I would like to thank CyberSecurity Malaysia's Management team and staff for their dedication and commitment. Also, I would like to extend my appreciation to my fellow Board members, and the Ministry of Science, Technology & Innovation (MOSTI) for their continued support and guidance to CyberSecurity Malaysia.

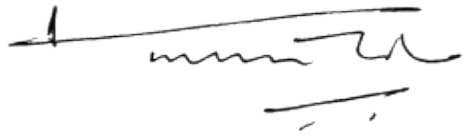
On behalf of the Board, I would like to put on record our gratitude to the former CEO, YBhg Lt Col (Retired) Prof Dato' Husin bin Jazri who was with CyberSecurity Malaysia for 12 years. His contributions to the organisation led it to where it is today. At the same time, a sincere note of appreciation to Encik Zahri bin Hj Yunos for his good work as acting CEO in the interim. Lastly, I wish a warm welcome to Dr Amirudin Bin Abdul Wahab, who has been appointed as CEO from 14 January 2013. Given his extensive experience in Information, Communication & Technology (ICT) matters and the inner workings of the public sector, I am confident that he will be able to lead CyberSecurity Malaysia to greater heights.

Moving forward, CyberSecurity Malaysia will be developing National Centres of Excellence (COE) based on our unique and specialised technical services. Examples of CyberSecurity Malaysia's COE in future are: National Digital Forensic Laboratory, National Malware Centre, and National Cyber

Security Certification Board. The COE will be providing unique and exceptional expertise in specific branch of cyber security.

No doubt, we will see more exciting innovations within the rapidly growing ICT industry that will continue to transform our lives for the better; even though we know that with every new electronic gadget, another window is open to a cyber attack. Yes, cyber threats will not stop, but CyberSecurity Malaysia will continue to be vigilant, protecting Malaysians in the cyber world.

The COEs will ensure that CyberSecurity Malaysia remains relevant to the country, and will drive it to become a Globally Recognized, National Cyber Security Reference & Specialist Centre by 2020.



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

Foreword from Acting CEO

Foreword from Acting CEO

"In 2012, we saw attackers extend their reach to more platforms, from social networks and cloud services to Android mobile devices. We saw them respond to new security research findings more rapidly, and leverage zero-day exploits more effectively. ..... as social engineering attacks such as fake antivirus and ransomware continued unabated." (Sophos Security Threat Report 2013)

A similar trend was seen in Malaysia, where cyber attackers also continued to deface websites and target databases to expose passwords and deliver malware. Out of 9,986 incidents reported to CyberSecurity Malaysia's Cyber999 Help Centre, 4,326 or 43% involved Intrusion, and 4,001 or 40% involved Fraud. Altogether, Intrusion and Fraud made up 83% of total incidents reported to Cyber999 in 2012. The remaining 17% of incidents include malicious codes, spams, cyber harassment, content related, vulnerabilities report, intrusion attempts, and denial of service attacks.

We, at CyberSecurity Malaysia are proud to play the roles of technical agency, whereby our services contribute to strengthening the security of the national cyberspace. During the year under review (2012), we assisted Regulatory Bodies and Law Enforcement Agencies to investigate 660 digital forensic cases and provided expert witnesses when needed. Under our Certifications Services, we certified six new products with Common Criteria ISO/IEC 15408 standard, and carried out security audit to evaluate 10 e-Commerce websites that applied for Malaysia Trustmark certificates. We also conducted Vulnerability Assessment at five Critical National Information Infrastructure (CNII) organisations; and performed Security Compliance Audit under the Chief Government Security Office (CGSO) Tim Naziran Sasaran Penting.

Other key initiatives by CyberSecurity Malaysia in 2012 include initiating four research initiatives (Technical Security Metric Models for SCADA System, Proving The Best Authentication on WIBAN Medical Devices, Transition State Diagram Framework for Android Abnormality Behaviour, and A Cyber Terrorism Framework), creating two new services (MyCyberSecurity Clinic and Malaysia Trustmark for Private Sector), and launching two new products (CyberArmor File Encryption System (CAFES) and DNSChanger Malware Response Detection Service).

In terms of public awareness, our Cyber Security Awareness For Everyone (CyberSAFE) programme reached out to 11,522 students and 2,500 teachers in 250 schools nationwide. In addition, 26,580 adults from the public and private sectors also took part in the programme, which include seminars and exhibitions. Media uptake of cyber attacks on organisations and of individual victims of scams indirectly helped to boost our efforts in raising cyber security awareness among organisations and the public at large.

We also organised a number of events in 2012 as a way to gather the industry players and to increase the awareness on cyber security among organisations and individuals. One of the major events was the CyberSecurity Malaysia – Awards, Conference and Exhibition (CSM-ACE) with the theme: "Cyber Security Risk & Compliance for Economic Transformation". 17 organisations supported the three-pronged event, which was also endorsed by the Ministry of Science, Technology and Innovation (MOSTI) and the Malaysian Communication and Multimedia Commission (MCMC). We are pleased that CSM-ACE 2012 successfully attracted 50 professional speakers and experts in IT security and more than 400 delegates from local and abroad. The conference featured three focused areas: Governance, Standards & Compliance; Technical; and Business Continuity Management. During the event, Malaysia Cyber Security Awards were conferred to highly talented information security professionals, home grown SMEs and global organisations for their outstanding contribution to the ICT security industry in Malaysia. Meanwhile, the exhibition successfully showcased ICT products and solutions that were developed locally and internationally.

Wider broadband penetration, coupled with multi-platform access enhances connectivity among Internet users; however, it presents more challenges for cyber security professionals. For this reason, Malaysia needs to strengthen its human capital in the field of cyber security; hence, in 2012 we trained and certified 1,106 local ICT professionals in various information security disciplines.

Other than developing ICT security professionals for the industry, we realise that we ourselves need to develop and retain our "brains". We cannot compromise on the quality of our employees and we need to stay on top of our field, as CyberSecurity Malaysia aims to be the National Cyber

Security Reference and Specialist Centre. So far, our employees have demonstrated exemplary accomplishments and are sought after as speakers in local and international conferences. In 2012, 33 employees of CyberSecurity Malaysia obtained various professional certifications that are globally recognised. In addition, 16 working papers, journals and articles, by employees of CyberSecurity Malaysia were accepted for international journals, conference proceedings and magazines. To retain our talents, we have a strategy in place and are also introducing new staff retention initiatives that would portray us as an employer of choice among ICT security professionals. We will continue to develop our people in terms of technical skills as well as leadership skills.

Cyber security is viewed as a "global" issue and accordingly, we hope to see more knowledge sharing amongst international agencies and coordinated efforts against cyber crimes. In this regard, we continue to play a pivotal role in the Asia Pacific Computer Emergency Response Team (APCERT - www.apcert.org) and the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT - www.oic-cert.net).

In February 2012, OIC-CERT successfully completed its first cyber drill themed "Targeted Attacks and Cyber Crisis Coordination", where six member countries took part - Bangladesh, Egypt, Malaysia, Oman, Pakistan, and Tunisia. The drill was aimed at measuring the readiness of the participants in facing cyber attacks.

On a bigger scale, APCERT successfully completed its annual drill in March 2012, to test the response capability of the leading Computer Security Incident Response Team (CSIRT) in the region. The theme for 2012 was "Advanced Persistent Threats and Global Coordination". For the first time, this exercise included the cooperation of OIC-CERT. 16 member countries from APCERT and three from OIC-CERT participated in this event. The cyber drills are important and crucial to our efforts in staying vigilant.

CyberSecurity Malaysia also contributes towards standards development in the areas of information security; both locally and internationally. CyberSecurity Malaysia is the co-author of the standard "ISO/IEC 27037 Guidelines of Identification, Collection, Acquisition and Preservation of Digital Evidence". Initially proposed by CyberSecurity Malaysia in 2007, it has been published as an International Standard on 22 October 2012.

For 2013, our focus will be on 'Securing Cyberspace for Economic Growth' as we strongly believe that cyber security is a potent enabler for wealth creation, and it can play a huge part in directly increasing business profits. This requires a change in mindset of how the industry views cyber security. Cyber security must not be viewed as just a protection umbrella for unfortunate incidents. There is a huge opportunity for Malaysian businesses to take advantage of it by leveraging on safe and secure online transaction channels.

More about our achievements and activities in 2012 can be found in the Operation's Review section of this report.

As we have all come to realise, there is no backing out from the cyber world. Once you get in, you will never want to get out. There is no way we can go back living without the Internet or mobile devices. And it is our job as the national cyber security specialist agency to be the enabler of ICT growth in the country -- to enable you to connect and surf the cyber world safely and peacefully.

In doing so, we will continue to be guided by our mission to create and sustain a safer cyberspace to promote National Sustainability, Social Well-Being and Wealth Creation.

Zahri Bin Hj. Yunos
Acting Chief Executive Officer

Board of Directors

1. General Tan Sri Dato' Seri Panglima Mohd Azumi Bin Mohamed (Retired)
   Chairman

2. Dato' Dr. Madinah Binti Mohamad
   Director

3. Datuk Dr. Abdul Raman Bin Saad
   Director

4. Datuk Haji Abang Abdul Wahap Bin Haji Abang Julai
   Director

5. Ir. Md. Shah Nuri Bin Md. Zain
   Director

6. Rubaiah Binti Hashim
   Director

7. Rohani Binti Mohamad
   Director

8. Lt Col Prof. Dato' Husin Bin Jazri (Retired)
   Director

Company Secretary
- Jailany Bin Jaafar

Internal Auditor
- Abd Rouf Bin Mohammed Sayuti

Board's Profile

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

General Tan Sri Dato' Seri Panglima Mohd Azumi Bin Mohamed (retired) was appointed to the Board as Chairman in July 2009. He is also a member of its Audit Committee. Currently he also serves as a trustee of the Perdana Global Peace Foundation (PGPF) and Yayasan Qaseh DCL. He is a member of the Dewan Negara Perak, and Chairman of the Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT). He had a distinguished military career spanning 37 years, retiring in December 2004 as the Chief of the Malaysian Army. He is a recipient of the French Award Ordre Officer National du Merite, the UN Medal for Peacekeeping, and the Pingat Jasa Malaysia.

Dato' Dr. Madinah Binti Mohamad
Director

Dato' Dr. Madinah binti Mohamad was appointed to the Board in July 2009. She is the Secretary General of the Ministry of Science, Technology and Innovation (MOSTI) and is at the forefront of efforts to implement the Government's Biotechnology Policy, IT Policy and the National Science, Technology and Innovation Policy. She has served the public throughout her career, beginning with a posting as an Administrative and Diplomatic Officer with the Ministry of Foreign Affairs in 1981 and subsequent promotions to the Public Service Department, the Ministry of National and Rural Development, the Ministry of Works, and the National Unity and Integration Department.

Datuk Dr. Abdul Raman Bin Saad
Director

Datuk Dr. Abdul Raman was appointed to the Board in June 2009. He is the Managing Partner of ARSA LAWYERS (Abdul Raman Saad & Associates) and Director of Technical University Malaysia Melaka (UTEM). An advocate and solicitor since 1977, he served the Malaysian Judicial and Legal Service in various capacities such as Magistrate, Deputy Public Prosecutor and Assistant Director of Legal Aid before going into private practice. He is acknowledged as one of the most experienced legal advisors in the areas of corporate and commercial law, information and communication technology law and Shariah Finance.

Datuk Haji Abang Abdul Wahap Bin Haji Abang Julai
Director

Datuk Haji Abang Abdul Wahap bin Haji Abang Julai was appointed to the Board in May 2009. He is the sixth mayor of Kuching North City Commission. He had a distinguished career with the Royal Malaysian Police Force for 37 years, retiring in 2007 as Director of Narcotics Crime Investigation Department (NCID). He is a recipient of the 'Panglima Gagah Pasukan Polis (PGPP)', which is the highest award in Malaysian Police Force; and 'Panglima Jasa Negara (PJN)', which carries the title 'Datuk'.

Ir. Md. Shah Nuri Bin Md. Zain
Director

Ir. Md. Shah Nuri bin Md Zain was appointed to the Board in April 2008. He is the Under Secretary to the Cyber and Space Security Policy Division of the National Security Council at the Prime Minister's Department. He has served the Government for more than 20 years, first as a Research Fellow with MIMOS Berhad, then as an engineer with the Public Works Department under the Ministry of Works.

Rohani Binti Mohamad
Director

Rohani was appointed to the Board in January 2010. She is a Deputy Under Secretary in the Information Technology Management Division of the Ministry of Finance, Malaysia. A civil servant for more than 25 years, she was attached to the ICT Security Division of the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), the Information Technology Section and Multimedia Super Corridor Unit of the Procurement Management Division at Treasury Malaysia, the Ministry of Land and Cooperative Development and the Economic Planning Unit (EPU). In 2010, she received 'Anugerah Pingat Kesatria Mangku Negara (KMN)'.

Rubaiah Binti Hashim
Director

Rubaiah was appointed to the Board in April 2008. She is the Under Secretary to the Communications Sector (Infrastructure, Applications & Technology) of the Ministry of Information, Communications and Culture. She has served the Government for more than 25 years in various capacities including as systems analyst to both the Ministry of Public Enterprise and Ministry of Education, then as Principal Assistant Secretary and later Under Secretary to the Communications Sector (Infrastructure & Electronic Applications) of the Ministry of Energy, Water and Communications.

Lt Col Prof. Dato' Husin Bin Jazri (Retired),
Director

Lt Col Prof Dato' Husin bin Jazri (Retired) joined MIMOS Berhad in 2000 to lead the National ICT Security and Emergency Response Centre (NISER). NISER was then separated from MIMOS and incorporated as an agency under MOSTI. In 2007 NISER was renamed CyberSecurity Malaysia, and Dato' Husin became the founding Chief Executive Officer of CyberSecurity Malaysia. He is also the founding President of the Information Security Professional Association (ISPA). Dato' Husin also serves as an Industrial Advisor for the Faculty of Information Science and Technology, Multimedia University; and a Visiting Professor at the Advanced Informatics School (AIS), Universiti Teknologi Malaysia, International Campus. He is a recipient of the (ISC)2 Harold F. Tipton Lifetime Achievement Award.

Corporate Governance Report

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 budgets, 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.

COMPOSITION OF BOARD

The Board consists of members of high calibre with good leadership skills and vastly experienced in their own fields of expertise, which enable them to provide strong support in discharging their duties and responsibilities. They 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) before performing their duties.

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 eight (8) 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.

BOARD MEETINGS AND 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 the 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 2012, nine (9) Board Meetings were held inclusive of circular resolutions passed.

APPOINTMENT AND RE-ELECTION OF THE BOARD MEMBERS

Members of the Board that represent 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 meetings (including where applicable the annual general meeting where the appointment was made), whichever is the longer.

Dato' Dr. Madinah binti Mohamad, Director of CyberSecurity Malaysia is not subject to retirement since she is representing MOSTI. Lt Col Dato' Prof. Husin Hj Jazri (Retired), 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. Gen Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired), Datuk Abang Abdul Wahap bin Abg Julai, Datuk Dr Abdul Raman bin Saad and Puan Rohani binti Mohamad who are the Directors holding office for a term of two (2) years, whose terms are expiring pursuant to Articles 31 of the Articles of Association of CyberSecurity Malaysia. They offered themselves for re-election as Directors and will be considered for approval by the Members of CyberSecurity Malaysia at the Sixth Annual General Meeting 2012.

CONTINUING EDUCATION OF DIRECTORS

Directors are encouraged to attend talks, training programmes 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 objectives of CyberSecurity Malaysia. The prescribing and maintenance of a system of internal controls, however, provides a reasonable assurance of effective and efficient operations besides ensuring 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 systems, implementing and entrenching the risk management culture and functions within CyberSecurity Malaysia.

The internal risk control and management programmes 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 the 7th Annual General Meeting

NOTICE IS HEREBY GIVEN THAT the 7th 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 26 June 2012 to transact the following business:

AS ORDINARY BUSINESS

1.	To receive the Audited Financial Statements for the financial year ended 31 December 2012 together with the Reports of the Directors and Auditors thereon;	Ordinary Resolution 1
2.	To re-elect Ir Md Shah Nuri bin Md Zain who is a Director holding office for a term of two (2) years, whose 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
3.	To accept the resignation of Rubaiah binti Hashim who is a Director holding office for a term of two (2) years, whose term is expiring pursuant to Article 31 of the Company's Articles of Association;	Ordinary Resolution 3
4.	To reappoint Messrs Azman, Wong & Salleh as Auditors of the Company and to authorize the Directors to fix their remuneration;	Ordinary Resolution 4

AS SPECIAL BUSINESS

5.	To approve the Directors' accumulated monthly allowance for the financial year ended 31 December 2012; and	Ordinary Resolution 5
6.	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 :

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 or if the appointor is a corporate body, either under seal or under hand of the officer of attorney duly authorized.
3. To be valid, the proxy form duly completed must be deposited at the Registered office of the CyberSecurity Malaysia at Level 5, Sapura@Mines building, 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.

CYBERSECURITY MALAYSIA

(Company No: 726630-U)
(Incorporated in Malaysia)

FORM OF PROXY

*I/We .....

of .....

.....

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

.....

of .....

.....

or failing him .....

.....

of .....

as*my[/our] proxy to vote for *me/us on my/our behalf at the Fourth Annual General Meeting of the Company to be held at the Board Room of the Company, Level 8, Mines Waterfront Business Park, No. 3, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor on the ..... day of ..... 20 ..... time ..... and at any adjournment hereof.

Signed this ..... day of..... 20....

(Signature of Appointor)
**Delete whichever is not desired*

Note:

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 or if the appointor is a body corporate, either under seal or under hand of the officer or attorney duly authorized.

3. To be valid the proxy form duly completed must be deposited at the Registered Office of the CyberSecurity Malaysia at Level 8, Block A, Mines Waterfront Business Park, No. 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan.

Management Committee

1. Zahri Bin Hj, Yunos
   Acting Chief Executive Officer

2. Dr. Solahuddin Bin Shamsuddin
   Vice President, Research

3. Roshdi Bin Ahmad
   Vice President, Corporate Planning and Strategy

4. Mohd Shamir Bin Hashim
   Vice President, Government & Multilateral Engagement

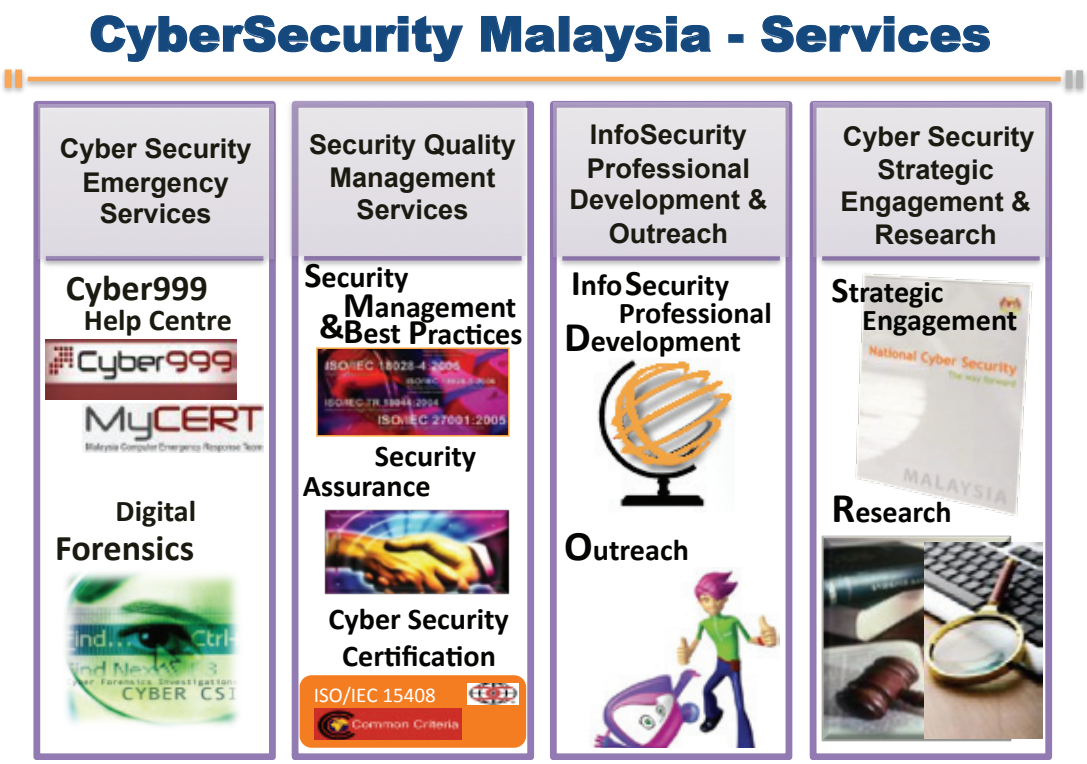
5. Mohd Roslan Bin Ahmad
   Vice President, Management Services

6. Lt Col Mustaffa Ahmad (Retired)
   Vice President, Outreach

7. Jailany Bin Jaafar
   Head, Legal and Secretarial / Company Secretary

Operations Review

1. Review of Core Services



1.1 Cyber999 Help Centre

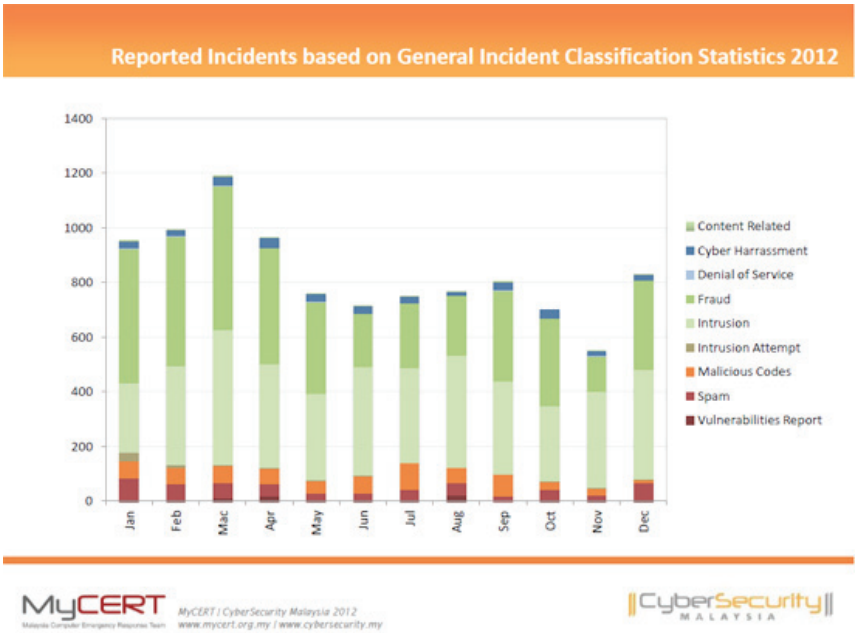
The Cyber999 is a cyber security help centre, provided by the Malaysia Computer Emergency Response Team or MyCERT, which is a department within CyberSecurity Malaysia. The public can rely on Cyber999 to provide technical assistance and incident handling in resolving incidents in cyberspace such as intrusions into computer systems, seditious or defamatory attacks, online frauds and cyber harrassments.

Other services provided by the MyCERT and Cyber999 include issuance of cyber security advisories (cyber early warning), malware research, technical coordination for national cyber emergencies and coordination of cyber drills at national and international level. For more information, go to www.mycert.org.my

Achievement in 2012

Incident Handling

Cyber999 team resolved a total of 9,986 cyber security incidents that were reported by members of the public and organisations. (See charts below).



Cyber Early Warning

Attackers often compromise end users' computers by exploiting vulnerabilities in the users' application. For example, an attacker could trick the user to open a specially crafted file like a PDF document or a web page. Thus, Cyber999 issues advisories to alert users on prevalent scams and phishing threats; as well as vulnerabilities in applications. In 2012, we issued 48 advisories, including alerts on vulnerabilities in applications such as Adobe PDF Reader, Adobe Shockwave Player, Adobe Flash Player, Exim, and multiple Microsoft applications. The advisories are published at www.mycert.org.my and broadcasted through our mailing list and social media.

MyCERT staff also wrote technical papers and delivered technical presentations at various local and international conferences.

Technical Coordination

In 2012, MyCERT was involved in coordinating cyber security exercises or cyber drills among the members of the Asia Pacific Computer Emergency Response Team (APCERT), and the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT).

Malware Research

MyCERT has produced a number of cyber security tools that are available to the public, such as Gallus, DontPhishMe, pKaji: The PHP Analyzer, MyKotakPasir: The Malware Sandbox, DNSWatch, and MyPHPIPS.

As part of its malware research initiatives, MyCERT has developed 12 security tools in 2012, as follows:

i. DNSChanger Malware Detector
ii. Kelihos.B Malware Detector (detects Kelihos.B infection for Malaysian IP addresses)
iii. Kelihos.B Malware Removal Tool
iv. TrueType Font Fuzzer (Research on security advisories MS11-077, MS11-087)
v. MalShare (Beta): Malware collection and classification
vi. rKaji: Return Oriented Programming (ROP) shellcode Analyzer
vii. G-Decoder (Beta): Universal JavaScript decoder for obfuscated JavaScript
viii. WhoisHammer: Multiple domains whois information gathering
ix. DontPhishME Terbang (v1.7.5): Signature based and fully automated extension compilation
x. Metaware: MOSTI eScienceFund Project
xi. MyLipas: provides web defacement feed scraped from many sources

xii. BrowserInception: Experimental project demonstrating capability of PhantomJS and provides web page screenshot service to MyLipas

1.2 CyberCSI - Digital Forensic Services

CyberSecurity Malaysia's digital forensic laboratory is the first forensic laboratory in Malaysia and in the Asia Pacific region that is accredited by the American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD/LAB) for 'Digital & Multimedia Evidence' discipline, based on ISO/ IEC 17025:2005 and the ASCLD/LAB - International 2011 supplemental requirement specifically for a digital forensics laboratory. The sophisticated digital forensics laboratory is capable of disk mirroring as well as secure collection, preservation, analysis and presentation of digital evidence.

CyberSecurity Malaysia also assists in Crime Scene Investigation (CSI) in relation to digital forensics upon request from law enforcement agencies, regulatory bodies, and government agencies. CyberSecurity Malaysia's digital forensics analysts are recognised as 'expert witness' in digital forensics under the Criminal Procedure Code 399 subsection 3(f).

Achievements in 2012

- The Digital Forensics Department (DFD) handled 660 cases in 2012, including those that involved assisting law enforcement agencies in resolving Cyber Crime Scene Investigation (CyberCSI).
- An in-house web portal was launched in January 2012, to provide the latest data related to cases conducted in forensic laboratories to all DFD employees on daily tasks. All information and inputs will be updated immediately and will summarize all cases submitted by Investigation Officers (IO). The set up has indirectly reduced case processing times and increased operation productivity.
- In early 2012, one of the Regulatory Bodies in Malaysia appointed DFD to develop a Digital Forensics Quality Management System (QMS) in their forensics laboratory in accordance to ASCLD/LAB International and ISO/IEC 17025.

1.3 MyCyberSecurity Clinic

The MyCyberSecurity Clinic is a new service by CyberSecurity Malaysia, launched in 2012. It provides technical assistance for data recovery and sanitization.

Data Recovery is a valuable service, especially for recovering lost confidential data. For example, someone who lost critical files due to a faulty hard disk could make an appointment to see the digital forensic expert at the MyCyberSecurity Clinic.

Data Sanitization is most useful when there is a need to securely cleanse confidential government data, such as before disposing old computers or hard disks in bulk. The digital laboratory of CyberSecurity Malaysia has sufficient capacity for bulk data sanitization service.

For more information, go to http://cybersecurityclinic.my

Achievements in 2012

The MyCyberSecurity Clinic handled more than 100 cases in its first year of operation (2012).

In addition, the MyCyberSecurity Clinic was accepted as one of the projects under the 10th Malaysian Plan (under the Rolling Plan 3).

1.4 Security Management & Best Practices

Under the Security Management & Best Practices (SMBP) department, CyberSecurity Malaysia developed guidelines and contributed towards standardization development at national and international level. CyberSecurity Malaysia is a member of WG7 under TC5 responsible for development of Malaysia Standard: Information Security Management Guidelines for Industrial Automation and Control Systems (IACS). CyberSecurity Malaysia is also a member in standards development activities for WG/G/5-1 ISMS, TC-BCM and TC-Risk.

Achievements in 2012

- The "ISO/IEC 27037 Guidelines of Identification, Collection, Acquisition and Preservation of Digital Evidence", which was initially proposed by CyberSecurity Malaysia in 2007, has been published as an International Standard on the 22 October 2012. CyberSecurity Malaysia is a co-author of this standard.
- Published the Information Security Best Practice: Securing BlackBerry (available online at CyberSecurity Malaysia's websites since 15 August 2012).
- Published four quarterly issues of e-Security Bulletin (online) and one special edition of the Bulletin. (available online at CyberSecurity Malaysia's websites)

1.5 MyVAS - Vulnerability Assessment Service

Under the Security Assurance Department, CyberSecurity Malaysia provides Vulnerability Assessment Service or MyVAS, at the national level with the aim to improve the country's resilience against cyber threats and exploitation due to information systems and technology vulnerabilities.

Achievements in 2012

- Conducted Security Compliance Audits at three critical systems, with Tim Naziran Sasaran Penting under the Chief Government Security Office (CGSO), Prime Minister's Department. (CyberSecurity Malaysia is a member of the Tim Naziran Sasaran Penting)
- Conducted vulnerability assessments at five Critical National Information Infrastructure (CNII) organisations.
- Conducted Control System Security Assessment (CSSA) at two CNII organisations.
- Joint Secretariat for Kumpulan Kerja Pakar Keselamatan Sistem SCADA under Majlis Keselamatan Negara (MKN). This is in relation to the Proposal to establish "Kumpulan Kerja Pakar Keselamatan Sistem SCADA" which was approved by the National Cyber Crisis Management Committee (NCCMC) Bil. 2/2012.

1.6 Cyber Security Certification Services

CyberSecurity Malaysia provides evaluation and certification services under the ISO/IEC 15408, ISO/IEC 27001 and the Malaysia Trustmark.

The following is the review of our Cyber Security Certification Services:

(a) MyCC Scheme
The Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme is a systematic process of security evaluation and certification. It evaluates and certifies the security functionality of ICT products against the international standard ISO/IEC 15408 known as Common Criteria (CC). The methodology used in the evaluation is also a recognised standard known as Common Evaluation Methodology (CEM) or ISO/IEC 18045. For more information, go to www.cybersecurity.my/mycc.

Achievements in 2012

- Seven new products certified with Common Criteria ISO/IEC 15408 standard.
- Four Protection Profile Working Groups (PPGWs) created. PPGWs are responsible to identify the national needs for the development or adoption of minimum-security requirements for specific type of ICT products.

(b) CSM MySEF
CyberSecurity Malaysia operates one of the Malaysia Security Evaluation Facilities (MySEF) known as the 'CyberSecurity Malaysia – Malaysia Security Evaluation Facility' or in short, 'CSM MySEF'.

Achievements in 2012

CSM MySEF is involved in the Malaysian Smart Card Committee and has participated in:

- Development of Protection Profile for Card Acceptance Device
- Development of Malaysia Standard Software Development Kit for Malaysia Multipurpose Smartcard
- Selected as Test Lab for Pilot Project Card Reader Assessment based on MS 2287
- Development of special technical requirements for card reader as part of the technical expert panel for Technical Working Group 9
- Development of STR1.12 Specific Technical Requirements for for Accreditation of Software Testing Laboratories stantards as part of the technical expert panel for Technical Working Group 49

(c) CSM27001

The CyberSecurity Malaysia Information Security Management System Audit and Certification (CSM27001) Scheme was established in May 2011 in support of the National Cyber Security Policy (NCSP). It offers independent security audit based on MS ISO/IEC 27001, which is conducted based on the strict requirements of recognised international standard and accreditation rules. Being MS ISO/IEC 27001 certified provides a degree of assurance that business processes are evaluated to ensure improved performance; while reducing the likelihood of security risks being present. For more information, go to http://csm27001.cybersecurity.my.

Achievements in 2012

- Six organisations certified based on MS ISO/IEC 27001:2007
- Eight Initial Certification audits conducted for organisations from various sectors for example the government, telecommunications, banking, transportation and trading
- Two surveillance audits conducted.
- Selected by the National Security Council (MKN) to certify CNIIs, together with other local certification body.

(d) MTPS

The Ministry of International Trade and Industry (MITI) appointed CyberSecurity Malaysia as the Malaysia Trustmark certifier for the private sector. Hence, we developed the Malaysia Trustmark for Private Sector (MTPS) programme, as one of our new services in 2012. MTPS is a way of validating the legality of an organisation that is involved in e-business. It is a mechanism to encourage e-Commerce between consumers and businesses in Malaysia. For more information go to http://mytrustmark.cybersecurity.my.

Achievements in 2012

- Security audit was carried out to evaluate 10 e-Commerce websites that applied for Malaysia Trustmark certificates
- The World Trustmark Alliance (WTA) maintained CyberSecurity Malaysia's membership in WTA and praised CyberSecurity Malaysia's initiative of developing a Trustmark awareness video, which also promoted the importance of Trustmark certification and membership in WTA.

1.7 InfoSecurity Professional Development

CyberSecurity Malaysia aims to increase the number of Information Security Professionals in the country by providing various information security competency and capability training courses and certifications as well as knowledge-sharing platform for ICT professionals, through our Information Security Professional Development Programme.

CyberSecurity Malaysia's training and examination centres are accredited by international certification bodies such as the SANS Institute and $(ISC)^2$. Majority of the training courses are HRDF claimable. For more information go to www.cyberguru.my.

Achievements in 2012

- In 2012, CyberSecurity Malaysia assisted a total of 1,106 local professionals to obtain certifications in the field of cyber security.
- CyberSecurity Malaysia employs a large number of ICT security professionals and in 2012, 33 employees of CyberSecurity Malaysia obtained various professional certifications that are globally recognised.

1.8 Outreach

CyberSecurity Malaysia aims to inculcate cyber safety and Internet security awareness in order to create a culture of positive Internet usage amongst people from all walks of life in Malaysia. This is carried out through an Outreach Programme known as CyberSAFE (CyberSecurity Awareness For Everyone). This programme includes a CyberSAFE Ambassadors Programme and awareness activities for students called "CyberSAFE in Schools". Organisations and individuals are welcome to join us in spreading safety awareness and nurturing a culture of cyber security among Malaysians.

Achievements in 2012

- The CyberSAFE portal www.cybersafe.my, which is owned and managed by CyberSecurity Malaysia, made it to the top 10 of "the best initiatives" from 148 participating organisations, during the 6th International Digital Media Fair & Festival 2012 (IDMF 2012) in Tehran, Iran; and subsequently won the Saramad Golden Award. The award was given in recognition of CyberSecurity Malaysia's initiative for Child Online Protection.
- In 2012, CyberSecurity Malaysia formed a smart partnership with DiGi Telecommunications, Kementerian Pendidikan, and Childline Malaysia to run the DiGi CyberSAFE programme. The main objective was to inculcate a safe and family-friendly Internet experience.
- As a whole, in 2012 the CyberSAFE programme reached 11,522 students, 2,500 teachers and 250 schools.
- In addition, 26,580 adults from the public and private sectors took part in the programme, which included seminars and exhibitions.

1.9 Strategic Engagement

(a) Government Engagement
Strategic Engagement with the Malaysian Government - to identify and drive various government collaborations, working relations and activities to advocate the cyber security agenda.

Achievements in 2012

- The National Security Council (NSC), with technical support from CyberSecurity Malaysia facilitated the implementation of Capability and Capacity Building Programmes for CNIIs. NSC together with MAMPU and CyberSecurity Malaysia has embarked on a Fast Track ISMS Implementation program in 2012, which comprises a series of ISMS trainings, workshops and certification programme for more than 60 CNIIs. In 2012, programmes that have been conducted include:
  - ISMS Implementation and Internal Auditor Training
  - ISMS ISO27001 Lead Auditor Training and Certification Exam
  - ISMS Implementation workshop
  - Business Continuity Management (BCM) Preparatory Plan Lab.

- Under Standards Adoption Programme, CyberSecurity Malaysia provides technical support to NSC on the following:
  - Development of ISMS Implementation Guidelines
  - Workshop on the Development of MS Information Security Management Guideline (ISMG) on Industrial Automation And Control System (IACS)
  - Development of guidelines for CNIIs to determine the requirement for Information Professionals
  - Seminars on Standard Compliance
  - Common Criteria Protection Profile Development workshop and working group meeting
  - Workshop on the Introduction to International Society of Automation (ISA99) Security Standards
  - Industry Standards Adoption Awards

- CNII Portal
  - CyberSecurity Malaysia is the administrator for the Critical National Information Infrastructure (CNII) portal at http://cnii.cybersecurity.my
  - A monthly email newsletter on the latest articles on critical information infrastructure protection uploaded into the portal is sent regularly to registered members of the CNII Portal.
  - Some 50,398 users have visited the CyberSecurity Malaysia CNII portal in 2012

- Organised and co-organised various seminars and conferences at national level

(b) Multilateral Engagement

Other than engaging the Malaysian Government, we also need to have a Multilateral Strategic Engagement programme because of the nature of cyber security, which often require cross-border cooperation. CyberSecurity Malaysia is the co-founder of the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) and actively involved in the Asia Pacific Computer Emergency Response Team (APCERT).

Achievements in 2012

- CyberSecurity Malaysia is the Chair of the OIC-CERT and a member of the Steering Committe of APCERT. In 2012, CyberSecurity Malaysia was elected as Secretariat of the OIC-CERT, in addition to being the OIC-CERT Chair.
- Co-organised various events and cyber drills at International level.
- Manages the OIC-CERT website http://www.oic-cert.net. The total no of hits for 2012 is 37,552 visitors, with an average of 3,126 visitors per month. According to Google analytics in December 2012, 10,613 visitors viewed the page with 1,721 visits are from new visitors and 1,236 visits are returning visitors.

1.10 Research

One of CyberSecurity Malaysia's Strategic Goals is "To Enhance Internal Research Capacity, Capability & Facility". This goal is attained through the Research Division, where research initiatives pertaining to cyber laws, emerging technologies, content and new policies on cyber security climate in Malaysia are done. The Research Division also produces research documents for reference by stakeholders and for input to policy decision makers; develops cryptographic algorithm, key management, cryptanalysis and applied cryptography; and develop security tools.

Achievements in 2012

- Developed four research initiatives:
  - Technical Security Metric Models for SCADA System
  - Proving The Best Authentication on WIBAN Medical Devices
  - Transition State Diagram Framework for Android Abnormality Behaviour
  - A Cyber Terrorism Framework

- Launched two new products:
  - CyberArmor File Encryption System (CAFES). CAFES is an easy to use encryption system. It protects the privacy of sensitive data or files during transmission or within storage, using a combination of symmetric and asymmetric encryption algorithms. Only the valid data owner or receiver can decrypt the encrypted data or files.
  - DNSChanger Malware Response Detection Service (http://dnschanger.detect.my/). In 2012, CyberSecurity Malaysia developed the DNSChanger Malware Response Detection Service Portal Phttp://dnschanger.detect.my/) to assist about four million Internet users worldwide who were affected by DNSChanger malware, which attacks a user's Domain Name System (DNS) and diverts the user to illegal sites. The portal helps Internet users check their computer for DNSChanger malware infections, and clean up computers that are infected.

- Presented papers in various local and international conferences.

2. Key Events Organised/Co-organised at National Level

One of CyberSecurity Malaysia's Strategic Goals is "To Enhance Internal Research Capacity, Capability & Facility". This goal is attained through the Research Division, where research initiatives pertaining to cyber laws, emerging technologies, content and new policies on cyber security climate in Malaysia are done. The Research Division also produces research documents for reference by stakeholders and for input to policy decision makers; develop cryptographic algorithm, key management, cryptana

April 2012

Seminar, **DDoS Attacks: Defeat or Be Defeated,** co-organized with Arbor Networks.

30 May 2012

Awareness seminar for the Malaysia Trustmark for Private Sector (MTPS)

4-6 June 2012

The 3rd International Conference on Cryptology & Computer Security 2012 was co-organised with Universiti Sains Malaysia (USM) and Institute for Mathematical Research (INSPEM) of Universiti Putra Malaysia (UPM).

27 September 2012

Seminar, **Cyber Trends and Its Impact to Businesses**, co-organised with SME Corporation Malaysia and the Ministry of International Trade and Industry (MITI)

1-5 October 2012

Training Course, **Digital Forensic Investigation & Analysis,** co-organised with KPerak Implementation & Coordination Corporation

23 October & 29 November 2012

Seminar for the Critical National Information Infrastructure (CNII), **Cyber Security Standards Awareness Programme: What You Need to Know**

6-7 November 2012

The annual **Cyber Security Malaysia – Awards, Conference & Exhibition (CSM-ACE)** was held at the Double Tree by Hilton hotel in Kuala Lumpur, as one of the satellite programmes of the World Innovation Forum Kuala Lumpur 2012.

28-29 November 2012

Training Course, ***Kursus Standard Keselamatan ISA99 Bagi Sistem Kritikal Negara.*** Representatives from 14 CNII organisations and government agencies attended the course.

September - December 2012

Training Courses co-organised with the Majlis Keselamatan Negara (National Security Council) :

1. **Information Security Management System (ISMS) – MS ISO/IEC 27001:2007 Implementation**
2. **MS ISO/IEC 27001:2007 for Internal Auditor**

CSM ACE 2012 at DoubleTree by Hilton, Kuala Lumpur

3. Supported Seminars/Conferences

In 2012, CyberSecurity Malaysia supported five industry events (see table below). Supporting industry events helps to promote MOSTI and CyberSecurity Malaysia.

26 April 2012 Cloud Malaysia 2012 Conference
26 May 2012 Smart Parenting Seminar
30 May 2012 Seminar on Cybercrime Trends, Impact and Safeguards for Businesses
17 July 2012 Wireless Security Seminar
17-18 October 2012 CloudSec 2012 Conference

4. Key Events Co-organised at International Level

In 2012, five international level events were co-organised by CyberSecurity Malaysia with various international partners.

14 February 2012

APCERT Cyber Drill

The annual drill by Asia Pacific Computer Emergency Response Team (AP-CERT) was conducted to test the response capabilities of computer security incident response teams in the region. The exercise saw the participation of the Organisation of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) countries for the first time.

The theme of the APCERT Drill 2012 was 'Advance Persistent Threats and Global Coordination'. The objective was for participating teams to exercise incident response handling arrangements locally and internationally in response to incidents, which are capable of impairing critical infrastructure and economic activities. The exercise reflected the strong collaboration within the group, and it also enhanced the communication protocols, technical capabilities and quality of incident responses for assuring Internet security and safety.

19 CSIRTs (Computer Security Incident Response Teams) from APCERT- Australia, Bangladesh, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Macao, Malaysia, Myanmar, Singapore, Sri Lanka, Thailand and Vietnam and 3 CSIRT teams from OIC-CERT - Tunisia, Egypt and Pakistan participated in the drill.

22 February 2012

OIC- CERT Cyber Drill

Established in January 2009, the OIC-CERT is a collaboration of Computer Emergency Response Teams (CERT) among the Organisation of Islamic Cooperation (OIC) countries.

The OIC-CERT held the first cyber drill among its members on 22 February 2012. The drill was themed "Targeted Attacks and Cyber Crisis Coordination", and aimed to assess the response capability of Computer Security Incident Response Teams (CSIRT) from respective OIC-CERT teams to mitigate targeted cyber attacks.

The objective of the drill was for the participating teams to exercise their incident response handling arrangements locally and internationally to measure the readiness of the participants in facing cyber attacks. The drill scenario was about cyber attacks targeted at high profile parties, where unknown vulnerabilities were exploited with malwares, which then led to information leakage that tarnished the reputation of the high profile parties.

Six teams took part in the drill namely Bangladesh, Egypt, Malaysia, Oman, Pakistan, and Tunisia.

25 – 28 March 2012

AP-CERT (www.apcert.org) - Annual Conference & Annual General Meeting 2012

CyberSecurity Malaysia plays a key role in the Asia Pacific Computer Emergency Response Team (APCERT), as a member of the Steering Committee.

CyberSecurity Malaysia participated in the APCERT Conference and AGM was held in Bali, Indonesia and hosted by Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC).

As the countries in Asia Pacific region were focusing on the development and adoption of "Web 2.0", the next generation of the cyber world including web-based communities, web applications, social networking sites, video-sharing sites, wikis, and blogs, the theme of the AGM 2012 was "Cleaning the Cyber Environment". The conference was conducted in three different sessions:

- Workshops, working group meetings and closed members discussion
- The Annual General Meeting (AGM) of all APCERT members; and
- Open conference sessions for all invited parties and members.

11-12 September 2012

ASEAN Regional Forum (ARF) Seminar On Confidence-Building Measures In Cyberspace

The Government of Malaysia and South Korea co-organised the ASEAN Regional Forum (ARF) Seminar On Confidence-Building Measures In Cyberspace, in Seoul, Korea. The Ministry of Foreign Affairs and CyberSecurity Malaysia were appointed as Co-Chair of the seminar, to represent Malaysia.

ASEAN Regional Forum (ARF) Seminar On Confidence-Building Measures In Cyberspace

29-31 December 2012

The OIC-CERT Annual Conference & General Meeting (AGM) in Muscat, Oman were a three-day events consisting of the following:

Day 1: OIC-CERT Incident Handling Workshop - "Do you know Infosec if Broken?"
(29 December)

It was a closed event attended by 40 participants from OIC-CERT team members. The speaker was Mr Jorge Sebastiao from First Information Security, Middle East Regional Office.

Day 2: OIC-CERT Annual Conference 2012, "Cyber Security Against Emerging Threats"
(30 December)

Oman National CERT (OCERT) hosted the OIC-CERT Annual Conference 2012, with the theme "Cyber Security Against Emerging Threats". It was an initiative under Information Technology Authority (ITA) and co-organized by CyberSecurity Malaysia.

The event was held to discuss new threats in cyber security and regional cooperation in combating emerging threats. 150 people from 30 countries attended the event, which was officiated by the Minister of Legal Affairs of the Sultanate of Oman, HE Dr. Abdullah bin Mohammed bin Said Al Saeedi.

Day 3: OIC-CERT 4th Annual General Meeting (AGM).
(31 December)

During the AGM, the members elected Malaysia (through CyberSecurity Malaysia) as the OIC-CERT Secretariat for 2013 – 2015 terms

With this appointment, CyberSecurity Malaysia is now holding dual positions as Chair and Secretariat of the OIC-CERT and continues to be the leader and the driving force of the OIC-CERT.

With six membership categories, currently the OIC-CERT has 26 members from 18 OIC member countries. Countries that are not a member of the OIC may apply for OIC-CERT membership under the "Affiliate" category.

OIC-CERT Annual Conference & General Meeting (AGM) in Muscat, Oman

Source: *http://www.flickr.com/photos/oiccert2012*

5. Local and International Visits Received

CyberSecurity Malaysia also receives dignitaries, international visitors, students/researches and representatives from various organisations at our premises as part of our customer service and branding activities, as well as to form an understanding between the visiting parties and Cyber-Security Malaysia. Guests are briefed about our roles and services. Below is the list of guests received in 2012:

No	Date	Description of guests
1	11 January 2012	Students from International College of Yayasan Melaka (ICYM)
2	13 February 2012	Authority for Info-communications Technology Industry of Brunei Darussalam
3	1 March 2012	Students from Sapura Smart School
4	2 March 2012	Minister of MOSTI and delegation
5	7 March 2012	Students from MARA Professional College Indera Mahkota
6	8 March 2012	Students from Institut Komunikasi dan Elektronik Tentera Darat
7	21 March 2012	Commercial Crime Bureau (CCB) of Hong Kong Police (HKP)
8	4 April 2012	Students from Cybernetics International College of Technology
9	5 April 2012	Students from Kolej Komuniti Pasir Salak
10	17 April 2012	Students from Kolej Komuniti Hulu Selangor
11	19 April 2012	Pahang CERT
12	25 April 2012	Participants of Cyber-Terrorism Workshop organised by South-east Asia Regional Centre for Counter-Terrorism (SEARCCT) Ministry of Foreign Affairs, Malaysia
13	27 April 2012	National Union of Teaching Profession (NUTP)
14	7 June 2012	Students from UNITEN
15	12 June 2012	Participants of Cyber Law Workshop at Institut Latihan Kehakiman dan Perundangan (ILKAP)
16	21 June 2012	Students from UiTM Shah Alam
17	18 July 2012	Institut Pengurusan Ruang Angkasa (INSPRA)
18	19 July 2012	Students from Kolej Teknologi Antarabangsa Cosmopoint Cawangan Ipoh
19	4 September 2012	Students from Pusat Teknologi dan Pusat Lanjutan (PTPL) Seremban
20	11 September 2012	TM Berhad representative during meeting/discussion
21	12 September 2012	Students from Universiti Malaya (The MM-ATM Programme)
22	19 September 2012	Students from Management and Science University (MSU)
23	25 September 2012	Students from Malaysian Academic & Skills Advancement (MASA College)
24	2 October 2012	Students from IKIP International College
25	26-29 November 2012	Visit from the Nigerian Government, comprising 13 delegates from various agencies led by Senator Adeniyi Anthony Ademuyiwa, Member of the Senate Committee on Communication

Certified Professionals in CyberSecurity Malaysia

Below is the list of CyberSecurity Malaysia's employees who obtained professional certifications in 2012. The list is arranged in chronological order (by month).

No	Name	Department	Certification	Month
1	Ahmad Dahari Jarno	SA	GIAC Web Application Penetration Tester (GWAPT)	Feb-12
2	Norahana Salimin	SA	GIAC Network Penetration Tester and Ethical Hacking (GPEN)	Feb-12
3	Norhazimah Abdul Malek	ISCB	Certified Information Security Audit (CISA)	Feb-12
4	Wan Nasra Wan Firus	ISCB	Certified Information Security Audit (CISA)	Feb-12
5	Mohammad Noorhisyam Muda	SA	E-Business Security	Feb-12
6	Asmuni Yusof	SMBP	Lead Auditor ISMS/ISO 27001	Feb-12
7	Nazri Mohamed	DF	Lead Auditor ISMS/ISO 27001	Feb-12
8	Noraini Abdul Rahman	IC	Lead Auditor ISMS/ISO 27001	Feb-12
9	Zarina Musa	SA	Lead Auditor ISMS/ISO 27001	Feb-12
10	Mohd Syamsyul Shuib	APS	Lead Auditor ISMS/ISO 27001	Feb-12
11	Zaharah Zulkifli	ISCB	Lead Auditor ISMS/ISO 27001	Feb-12
12	Farhana Aqilah Mohd Suffian	ISCB	Lead Auditor ISMS/ISO 27001	Feb-12
13	Azrul Ehsan Ahmad	ISCB	Lead Auditor ISMS/ISO 27001	Feb-12
14	Imran Hasnan	MyCERT	Lead Auditor ISMS/ISO 27001	Feb-12
15	Sarah Abdul Rauf	MyCERT	Lead Auditor ISMS/ISO 27001	Feb-12
16	Mohd Azlan bin Mohd Nor	STS	EC-Council Certified Security Analyst (ECSA)	Mar-12
17	Mohd Nor'akashah Mohd Kamal	STS	COMPTIA SECURITY +	Mar-12
18	Azira Abd Rahim	Outreach	ISMS Lead Auditor	Mar-12
19	Zarith Fariha Ramdzan	ISPD	ISMS Lead Auditor	Mar-12
20	Nur Edlina Haida binti Ramli	DF	Cellebrite UFED Certified	Mar-12
21	Muhammand Firdaus bin Ismail	DF	Access Data Certified Examiner (ACE)	Apr-12
22	Tajul Josalmin Tajul Ariffin	DF	Access Data Certified Examiner (ACE)	Apr-12
23	Rafizah Abd Manaf	DF	Access Data Certified Examiner (ACE)	Apr-12
24	Nur Aishah Mohamad	DF	Access Data Certified Examiner (ACE)	Apr-12
25	Muhammad Reza Shariff	SA	GIAC Windows Security Administrator (GCWN)	May-12
26	Najibah Mat Ali	ME	BCLE2000	May-12
27	Norlinda Jaafar	MyCERT	COMPTIA SECURITY+	Jun-12
28	Nor Liyana Azman	SA	COMPTIA SECURITY+	Jun-12
29	Norazlila Mat Nor	SA	COMPTIA SECURITY+	Jun-12
30	Sharifah Roziah Mohd Kassim	MyCERT	GIAC SYSTEMS AND NETWORK AUDITOR (GSNA)	Jul-12
31	Nurul Husna bt Mohd Nor Hazalin	STS	Certified Information Security Audit (CISA)	Aug-12
32	Engku Azlan Engku Habib	CAIT	EC-Council Certified Security Analyst (ECSA)	Dec-12
33	Mohd Rizal Abu Bakar	CAIT	EC-Council Certified Security Analyst (ECSA)	Dec-12

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	Authors	Publication
1	How Do Malaysian Men And Women Use Adverbs in Blogs?	Syahrir Mat Ali	Elsevier Procedia Social and Behavioral Sciences
2	Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standards	Nor Azuwa Muhamad Pahri and Dr Solahuddin Shamsuddin	International Journal of Cyber Security and Digital Forensics
3	Code and platform level SQL Injections Defenses	Ahmad Zaidi bin Said	Hakin9 Magazine
4	Super resolution hybrid methods for CCTV forensic interpretation	Nazri Ahmad Zamani	Proceedings of the Soft Computing and Pattern Recognition International Conference 2012
5	Sparse representation super-resolution method for enhancement analysis in video forensics	Nazri Ahmad Zamani	Proceedings of the Soft Computing and Pattern Recognition International Conference 2012
6	Object hallucination methodology in video forensics enhancement analysis	Nazri Ahmad Zamani	Extended abstract for the Proceedings of the 11th Asian Conference on Computer Vision 2012
7	A study on Android-based IDS: A Propose for Cost-Sensitive based Intrusion Response System	Naqliyah Zainuddin	Proceedings of the 11th WSEAS International Conference on Information Security & Privacy
8	Towards Secure Model for SCADA Systems	Dr Solahuddin bin Shamsuddin	Proceedings of the International Conference on Cyber Security; Cyber Warfare and Digital Forensics
9	Enhancement of Asset Value Classification for Mobile Devices	Ahmad Ismadi Yazid Sukaimi	Proceedings of the International Conference on Cyber Security; Cyber Warfare and Digital Forensics
10	A Propose Technical Security Metrics Model for SCADA System	Nor Azuwa Muhamad Pahri	Proceedings of the International Conference on Cyber Security; Cyber Warfare and Digital Forensics
11	Understanding Cyber Terrorism: The Grounded Theory Method Applied	Zahri Yunos	Proceedings of the International Conference on Cyber Security; Cyber Warfare and Digital Forensics
12	Economic benefits through information security standards	Sabariah Ahmad	Microsoft FUTURES e-magazine
13	The Application of Mixed Method in Developing a Cyber Terrorism Framework	Zahri Yunos	Journal of Information Security
14	Illicit Activities and Terrorism in Cyberspace: An Exploratory Study in the Southeast Asian Region	Zahri Yunos; Syahrir Mat Ali and Dr Solahuddin Shamsuddin	Springer Lecture Notes in Computer Science
15	A Dynamic Cyber Terrorism Framework	Zahri Yunos	International Journal of Computer Science and Information Security
16	Perception on Cyber Terrorism: A Focus Group Discussion Approach	Zahri Yunos	Journal of Information Security

Financial Report

Statement of Financial Position as at 31 December 2012

	31.12.2012	31.12.2011	1.1.2011
	RM	RM	RM
ASSETS			
Non Current Assets			
Property, plant and equipment	23,763,222	26,918,169	29,907,889
Intangible assets	2,398,208	2,472,145	3,207,060
	26,161,430	29,390,314	33,114,949
Current Assets			
Trade receivables	295,022	117,739	1,160,847
Other receivables	889,102	830,221	961,728
Short term deposit with licensed banks	72,100,750	1,300,000	5,000,000
Cash and bank balances	1,620,922	1,080,484	1,724,233
	74,905,796	3,328,444	8,846,808
Total Assets	**101,067,226**	**32,718,758**	**41,961,757**
RESERVES AND LIABILITIES			
Reserves			
Accumulated reserves	1,447,253	1,435,369	1,509,686
Non Current Liabilities			
Government grants	99,177,851	29,923,772	40,237,037
Current Liabilities			
Other payables and accruals	442,122	1,345,773	164,120
Tax payable	-	13,844	50,914
	442,122	1,359,617	215,034
Total Reserves and Liabilities	**101,067,226**	**32,718,758**	**41,961,757**

Financial Report

Statement of Comprehensive Income for The Year Ended 31 December 2012

	2012 RM	2011 RM
INCOME FROM GRANTS	36,381,776	40,236,427
OPERATING REVENUE	1,949,594	2,384,849
OTHER INCOME	445,272	57,776
	38,776,642	**42,679,052**
STAFF COST	(21,799,220)	(17,812,954)
DIRECTORS' EMOLUMENTS	(616,606)	(696,283)
DEPRECIATION AND AMORTISATION	(5,009,693)	(4,853,069)
RENTAL	(4,057,221)	(4,195,601)
OTHER OPERATING EXPENSES	(7,295,862)	(15,165,272)
DEFICIT OF INCOME BEFORE TAXATION	**(1,960)**	**(44,127)**
TAXATION	13,844	(30,190)
TOTAL COMPREHENSIVE INCOME / (DEFICIT) FOR THE YEAR	**11,884**	**(74,317)**

Statement of Changes in Reserves for The Year Ended 31 December 2012

	Accumulated Reserves RM
As at 1 January 2011	1,509,686
Total Comprehensive deficit for the year	(74,317)
Balance at 31 December 2011	1,435,369
Total comprehensive income for the year	11,884
Balance at 31 December 2012	**1,447,253**

Financial Report

Statement of Cash Flows for The Year Ended 31 December 2012

	2012	2011
	RM	RM
CASH FLOWS FROM OPERATING ACTIVITIES		
Deficit of income before tax	(1,960)	(44,127)
Adjustments for:		
Depreciation of property, plant and equipment	3,921,591	3,897,598
Amortisation of intangible assets	1,088,102	956,138
Property, plant and equipment write off	21,979	-
Interest income	(266,730)	(55,376)
Grant income recognised	(36,381,776)	(40,236,427)
Operating loss before working capital changes	(31,616,834)	(35,438,067)
Changes in working capital:		
(Increase) / decrease in trade receivables	(177,283)	1,043,108
(Increase) / decrease in other receivables	(58,881)	141,859
(Decrease) / increase in other payables	(903,651)	1,181,653
Increase in government grants	(70,000,000)	-
	(102,756,649)	(33,071,447)
Operating government grants received	20,400,000	18,000,000
Interest received	266,730	55,376
Tax paid	-	(67,261)
Net cash used in operating activities	(82,091,879)	(15,127,459)
CASH FLOWS FROM INVESTING ACTIVITIES		
Purchase of property, plant and equipment	(788,623)	(918,229)
Purchase of Intangible assets	(1,014,165)	(221,223)
Net cash used in investing activities	(1,802,788)	(1,139,452)
CASH FLOWS FROM FINANCING ACTIVITY		
Development government grant received	155,235,855	11,923,162
NET INCREASE / (DECREASE) IN CASH AND CASH EQUIVALENTS DURING THE YEAR	71,341,188	(4,343,749)
CASH AND CASH EQUIVALENTS AT BEGINNING OF OF THE YEAR	2,380,484	6,724,233
CASH AND CASH EQUIVALNETS AT END OF YEAR	**73,721,672**	**2,380,484**
CASH AND CASH EQUIVALNTS COMPRISE:-		
Fixed deposit	72,100,750	1,300,000
Cash and bank balances	1,620,922	1,080,484
	73,721,672	**2,380,484**

Activities

21 Mac 2012
InfoSecurity World Exhibition & Conference (ISWec) 2012, PWTC

29 Mac 2012
Innovation & Creativity Festival, Padang Kawat UTM

19-20 May 2012
Karnival Sains dan Inovasi, program utama Tahun Sains dan Gerakan Inovasi Nasional (SGI2012) Zon Sabah, Hongkod Koisaan, KDCA, Penampang Sabah

Activities

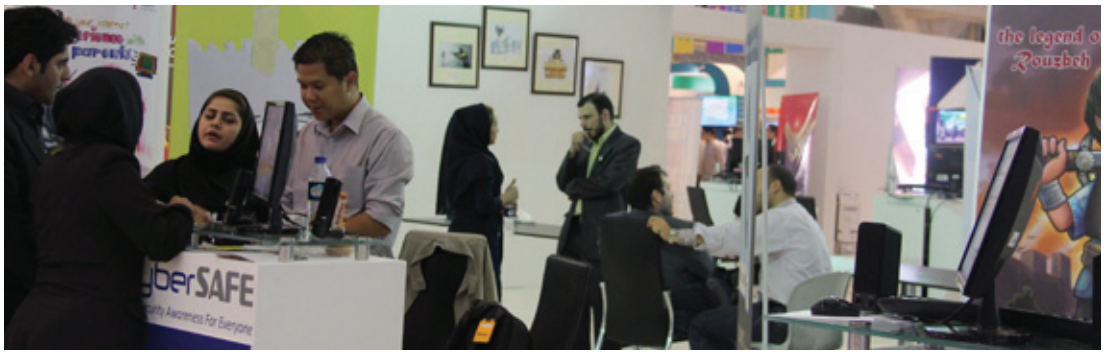
23-27 May 2012
Himpunan Jutaan Belia 2012 Anjuran Kementerian Belia & Sukan, Putrajaya

19-25 Jun 2012
Pameran & Ceramah Interaktif CyberSAFE sempena Minggu Sains, Teknologi dan ICT Negeri Johor

8 August 2012
Majlis Berbuka Puasa CyberSecurity Malaysia Bersama Anak-anak Yatim Bait Al-Amin dan juga pelajar UTP, Hotel Seri Malaysia, Ipoh

9 August 2012
Perhimpunan Staf & Majlis Berbuka Puasa CyberSecurity Malaysia, Palace Of Golden Horses

Activities



7-13 September 2012
The 6th International Digital Media Fair and Festival, Tehran, Imam Khomeini Great Mosalla

15-16 September 2012
Karnival Sains dan Inovasi Zon Sarawak sempena Majlis Perasmian Regatta Sarawak 2012

6-7 November 2012
CSM ACE 2012 at DoubleTree by Hilton, Kuala Lumpur

6 December 2012
Ceramah Maal Hijrah 'Pengertian Hijrah dan Bagaimana Menghayatinya dalam Kehidupan Seharian' oleh Ustaz Don Daniyal

News & Highlights

Keselamatan sib

Isu yang perlu diberi perhatian oleh pengguna pada masa ini

Early Intervention On Cyber Security To Safeguard Young - Fadillah

KUCHING, July 6 (Bernama) -- Cyber security incidence in Malaysia could rise if proactive measures are not taken to instill cyber security awareness and to provide early intervention among int young, said Science, Technology and Innova Fadillah Yusof.

According to him, the Cyber999 Cyberse recorded 11 incidents involving youngsters ag complaints as at June this year.

He said the incidents comprised hacking malware (virus) and vulnerability threats, wh was lodged involving a 13-year-old girl who relationship with a married man through Face

"There were 7,404 complaints in the sam reporters after launching the state-level C Petra Jaya, here Friday.

He said the number of internet users incre million in the first month of this year. The reported that throughout that month, more visited by internet users.

-- BERNAMA

ISO15408 bantu ICT pergi jauh

SYARIKAT teknologi maklumat dan komunikasi (ICT) tempatan disaran mendapatkan sijil Kriteria Biasa (ISO15408) bagi produk yang mahu dipasarkan di peringkat antarabangsa.

ua Pegawai berSecurity Yunos berit mampu keyakinan angsa de- piawaian gi produk. arikat luar h sijil ter-." katanya rkan pra urity Ma- onference SM-ACE)

ICT Developers Urged To Get Certification For Their Products

KUALA LUMPUR, Oct 17 (Bernama) -- Local information and communication technology (ICT) developers can access international markets by certifying their products under the Common Criteria (ISO15408) via the Malaysia Common Criteria Evaluation and Certification Scheme (MyCC), CyberSecurity Malaysia said.

Acting chief executive officer, Zahri Yunos, said this was because the accreditation would ensure that a product comply with globally-accepted standards and assurance requirements, whereby CyberSecurity Malaysia was the authorised certification body for the scheme.

"So far we have certified 26 products and we hope by setting up a special pavilion in the coming Cyber Security Malaysia Awards, Conference and Exhibition (CSM-ACE) 2012, we can attract their prod

CyberSecurity warns against phishers on Twitter

PETALING JAYA: If you receive a tweet from someone you know, sa that some people are talking bad about you on a particular website, out. It's likely to be an attempt to glean your Twitter account login, password and personal details.

Whatever you do, do not go to the site that's listed in the tweet.

CyberSecurity Malaysia has confirmed that this is a phishing attack.

Phishers are unscrupulous people, who try to trick Internet users into revealing the details of their online accounts.

In this case, clicking on the link in the tweet will take you to what looks l a Twitter log-in screen.

A message will then pop up telling you that your Twitter session has time

Don't become an 'accidental' outlaw

WITH one update status on Facebook, a university student instantly became a Wanted man.

To the Universiti Sains Malaysia student, it was a mere joke; but to the authorities, his posting on Prime Minister Datuk Seri Najib Tun Razak that read "najib is coming to our campus... let's bomb his helicopter..." was a real security threat.

The Police immediately hauled him in for questioning on criminal intimidation suspicion under Section 506 of the Penal Code.

Adli Abdul Wahid, Cyber Security Malaysia's responsive services vice-president, says there are many who think they can do and say whatever they want on the Internet.

News & Highlights

Selesaikan masalah virus DNSChanger

SEJAK kebelakangan ini, CyberSecurity Malaysia banyak menerima laporan mengenai penyebaran virus komputer dikenali sebagai *DNSChanger*.

Rentetan itu, organisasi tersebut telah mengenal pasti sebanyak 1,000 hingga 1,500 Penyedia Perkhidmatan Internet (ISP) dan pemilik rangkaian di Malaysia berhadapan dengan masalah virus berkenaan.

Sebagai menyokong inisiatif global yang diterajui *DNSChanger Malware Working Group* (DCWG), CyberSecurity Malaysia telah membina sebuah laman web khas untuk pengguna Internet di negara ini memeriksa sama ada komputer mereka terkena jangkitan itu.

Mereka boleh berbuat demikian dengan melayari pautan *http://dnschanger.detect.my*.

Jika virus itu dikesan,

www.mycert.org.my.

Hackers may cause Internet users to become victims of Evidence Act

Reports by P. ARUNA and TASHNY SUK

PETALING JAYA: Rampant hack
at risk of being prosecuted for of
they did not publish with the new
onus of proof on them.

According to Cybersecurity Mala
accounts, blogs and websites a

"It doesn't take an expert to hac
Facebook, Twitter and e-mail,"
executive officer Lt-Col (Rtd) P

"Any computer literate person

He added that Internet users w
were the easiest targets.

PC users urged to check for malware

By JO TIMBUONG
bytz@thestar.com.my

PETALING JAYA: Come July 10, thousands of computers infected with the DNSChanger malware (malicious software) will be disconnected from the Internet if their users don't take some necessary steps.

The problem is that many PC users may not even know that their computers have been infected.

F-Secure Labs Malaysia security adviser Goh Su Gim explained that the United State Federal Bureau of Investigation (FBI)
hacker
infecte
chaos

More than 300 expected at this year's CyberSecurity Malaysia conference

AvantiKumar | Oct. 23, 2012

*Photo - (from left) Fong Chiok Hin, director of Disaster Recovery & Infrastru
Management for HeiTech Padu; Zahri Hj. Yunos, acting chief executive offi
CyberSecurity Malaysia; and Razman Azrai Zainudin, CyberSecurity, Malay
vice president of Corporate Planning & Strategy.*

More than 300 industry delegates are expected to attend the third annual CyberSecurity Malaysia Awards & Exhibition (CSM-ACE) 2012, organised by national IT security agency CyberSecurity Malaysia.

Boleh akses jika produk tepati kriteria MyCC

2012/10/18 - 05:15:08 AM

Emel Kawan Cetak

Like 0 Tweet 1 +1 0

Pembangun teknologi maklumat dan komunikasi (ICT) boleh mengakses pasaran antarabangsa jika produk mereka disahkan dalam Kriteria Seragam (ISO15408) menerusi Skim Pensijilan dan Penilaian Kriteria Seragam (MyCC).

Pemangku Ketua Eksekutif CyberSecurity Malaysia, Zahri Yunos, berkata ia susulan akreditasi akan memastikan produk mematuhi standard dan syarat jaminan yang diterima global.

Jelasnya, CyberSecurity Malaysia adalah badan pensijilan sah untuk skim itu.

> *"Kami mengesahkan 26 produk dan berharap menerusi acara khas pada CSM-ACE 2012 Cyber Security Malaysia, kita boleh mendapatkan lebih banyak produk pemaju ICT tempatan disahkan," - Zahri Yunos, Pemangku Ketua Eksekutif CyberSecurity Malaysia*

"Setakat ini kami mengesahkan 26 produk dan berharap menerusi acara khas pada Anugerah, Persidangan dan Pameran (CSM-ACE) 2012 Cyber Security Malaysia, kita boleh mendapatkan lebih banyak produk pemaju ICT tempatan disahkan," katanya pada taklimat media mengenai persidangan itu di Kuala Lumpur, semalam.

News & Highlights

Cyber security's role in the nation's economic transformation: CyberSecurity Malaysia event

AvantiKumar | Nov. 8, 2012

Photo - (from left): Nizar Najib, Executive Director, Deloitte Mala... Yunos, Acting CEO CyberSecurity Malaysia; General Tan Sri D... Mohd Azumi Mohamed, Chairman CyberS... Australasian Regional Director of BAE Sy... Mohammad, Executive Director, HeiTech...

The national cyber security agency Cybe... year... Awards, 2012... Tra... Fo...

Are you guilty of cyber crime?

Stories By HARIATI AZIZAN
sunday@thestar.com.my

There are laws that you may be breaking online without your knowledge.

TECHNICAL glitches and Internet security issues are the top tasks for national cyber security specialist centre Cyber Security Malaysia.

Lately, however, the reported incidents they have received are falling more in the difficult-to-define "human behaviour" category, says the centre's responsive services vice-president Adli Abdul Wahid.

"Technical complaints are still high, but we are also getting an increased number of reported incidents connected to behavioural issues," he tells *Sunday Star*, "with some of the more frequently asked questions including Is this sue-able? You read this...

Internet use, online safety must go together — Fadillah

Posted on July 7, 2012, Saturday

KUCHING: Online safety awareness must be inclusive of the rapid growth of information technology.

Making the call was Deputy Minister of Science, Technology and Innovation Datuk Fadillah Yusof who said Internet ...ers must be aware of their vulnerabilities when they go online.

...ted to CyberSecurity Malaysia through their Cyber999 hotline," ...gramme at SMK Petra Jaya yesterday.

...6 per cent within the same period in 2011, Fadillah believes that ...pecially children.

...hose below 18 years old.

...go unreported," said Fadillah, who broke down the categories into ...intrusion attempt, intrusion, fraud, denial of service (DoS attack),

...Gi CyberSAFE programme was timely and relevant as it reaches out ...

...users in Malaysia, out of the 28 million population.

...out in Lundu and Sematan, saw the participation of more than 400 ...

...educated more than 3,700 students, educators and parents from 170 ...lan, Johor, Melaka, Terengganu, Sarawak and Sabah.

...ion with the Ministry of Education, CyberSecurity Malaysia, Childline ...Multimedia Commission and DiGi.

All netizens should learn more about cyber security

WHILE in the midst of a rendezvous with a programmer, I was intrigued at the sight of his broadband stick. We were in a Wi-Fi zone of a restaurant.

I asked why. He cited one core reason. He wants to show me something where a user password is required. He further elaborated that a Wi-Fi zone was a non-secure area.

Flashback. CyberSecurity Malaysia had warned against Internet banking in a Wi-Fi zone such as in a restaurant "Free Wi-Fi users warned" (*Sunday Star*, April 8).

The hacker may just be sitting at the next table. The hacker is hungry and waiting to steal another's user password given the opportunity. Our personal information is always on the favourite menu of hackers.

Better safe than sorry. Restaurants, saloons or any commercial outlets offering free Wi-Fi services should put up warning signs. I hope the Information Ministry will make it mandatory.

I surfed CyberSecurity Malaysia's website and found it to be a crucial

News & Highlights

Pemaju ICT Digesa Dapatkan Pensijilan Untuk Produk Masing-Masing

KUALA LUMPUR, 17 Okt (Bernama) -- Pemaju teknologi maklumat dan komunikasi (ICT) boleh mengakses pasaran antarabangsa jika produk mereka disahkan dalam Kriteria Seragam (ISO15408) menerusi Skim Pensijilan dan Penilaian Kriteria Seragam Malaysia.

Pemangku Ketua Pegawai Eksekutifnya Zahr akreditasi akan memastikan produk me jaminan yang diterima global, dengan Cybe badan pensijilan sah untuk skim itu.

"Setakat ini kami mengesahkan 26 produk k khas pada Anugerah, Persidangan dan Pan Security Malaysia, kita boleh mendapatkan ICT tempatan disahkan," katanya pada persidangan itu di sini pada Rabu.

CSM-ACE 2012, dengan tema Risiko Keselam ekonomi, menyasarkan untuk meningk pematuhan wajib standard keselamatan m platform strategik untuk agensi kerajaan me standard keselamatan maklumat.

Acara dua hari mulai 6 Nov, merupakan Transformasi Negara menerusi Inisiatif menjalankan acara dan peluang membuat pa

Banks put lid on online scams

By P. ARUNA
aruna@thestar.com.my

PETALING JAYA: Banks will introduce a new layer of security as they work closely with cyber security authorities and the police to combat the proliferation of online fraud.

Cybersecurity Malaysia said fraud cases reported to the agency had doubled from 606 in 2009 to 1,328 in 2010 and 3,142 last year.

"As of April this year, we received nearly 2,000 cases of online banking

Protection against cyber crime

By ZORA CHAN
zora@thestar.com.my

For improved safety: (From third right) Fadillah, Education Department assistant director Abdul Wahed Rosli, Wee and other VIP guests launching the Digi Cyber Safe at SMK Petra Jaya in Kuching.

KUCHING: More strategic alliances between the public and private sector are needed to address online child safety because cyber crimes nowadays are also targeted at children.

Deputy Science, Technology and Innovation Minister Datuk Fadillah Yusof said as more people have internet access and using it to better their lives, the greater exposure they had to various forms of cyber crimes.

"Many of these crimes are targeted at our children. As of June this year, CyberSecurity Malaysia Cyber999) received a total of 5,581 complaints nationwide, out of which 11 involved those below 18 years old.

Hackers have their ways to tap into accounts

PETALING JAYA: A graphic designer was not aware that pornographic pictures appeared on his Facebook page until a friend alerted him.

The 25-year-old man, who wanted to be known only as Shan, said he had been asleep at home when he received the call from his friend.

"I found that I could no longer log in to my account as the password had been changed.

"Someone was using my account to post the content under my name," he said, adding that he then contacted his friends and asked them to delete the compromised account from their list.

Cybersecurity Malaysia CEO Lt-Col (Rtd) Prof Datuk Husin Jazri said there were special devices in the market that enabled anyone to "sniff" WiFi networks.

Editorial Committee

Advisor:

Zahri Bin Yunos
Chief Operating Officer

Editor:

Mohd. Shamil Mohd Yusoff
Head, Corporate Branding & Media Relations

Sandra Isnaji
Manager, Corporate Branding & Media Relations

Layout artists & graphic designers:

Zaihasrul Ariffin
Graphic Designer, Secure Technology Services

Nurul 'Ain Zakariah
Graphic Designer, Secure Technology Services

Contributors:

Abd. Rouf Mohammed Sayuti
Head, Internal Audit

Azman bin Ismail
Head, Finance

Azlin Samsudin
Executive, Legal and Secretarial

Ernieza Ismail
Executive, Strategy Management

Photographer:

Zul Akmal Manan
Executive, Corporate Branding & Media Relations

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	:	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

This page is intentionally left blank

CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

Corporate Office:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan | Tel : +603 8992 6888 | Fax : +603 8992 6841
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my