

2010



annual report

Cover Rationale

Driving the Development and Progress of Cyberspace in the International Arena

The scope of cyber security is broad due to the nature of today's technology, which is not only borderless but also continuously evolving. Hence, addressing cyber security issues require major efforts, which can be very challenging to CyberSecurity Malaysia.

As the leader in the cyber security arena, CyberSecurity Malaysia's development and progression are in accordance with the flow of technological development at the global level.

Professionalism, expertise, spirit of cooperation and internalisation of positive values in every individual at CyberSecurity Malaysia are the main ingredients that help to position CyberSecurity Malaysia as the reference and specialist centre in the field of cyber security not only in Malaysia but also in the international arena.

The design of the Annual Report 2010 portrays CyberSecurity Malaysia's capability to strengthen its position, for it to be recognized and respected throughout the world.



Contents

ii	Cover Rationale
02	Notice of the Fifth Annual General Meeting
04	Our Direction
05	What We Believe In
06	Client Charter
08	How We Got Here
10	Message by Minister of Science, Technology & Innovation
11	Message by Deputy Minister of Science, Technology & Innovation
12	Message by Secretary General, Ministry of Science, Technology and Innovation
14	Chairman's Statement
16	Board Members
22	Management Committee
30	Forward by the CEO
32	Operation's Review
76	Strategic Partnership
79	Coporate Governance
83	Financial Statement
112	Editorial Committee
113	Proxy Form



Notice of the Fifth Annual General Meeting

Notice of Annual General Meeting

NOTICE IS HEREBY GIVEN THAT the 5th 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 30 June 2011 to transact the following business:

AS ORDINARY BUSINESS

1. To receive the Audited Financial Statements for the financial year ended 31 December 2010 together with the Reports of the Directors and Auditors thereon; Ordinary Resolution 1
2. To re-elect Encik Ir Md Shah Nuri bin Md Zain who is a Director holding office for a term of two (2) years, which term is expiring pursuant to Article 31 of the Company's Articles of Association, and being eligible, offers himself for re-election; Ordinary Resolution 2
3. To re-elect Puan Rubaiah Hj Hashim who is a Director holding office for a term of two (2) years, which term is expiring pursuant to Article 31 of the Company's Articles of Association, and being eligible, offers herself for re-election Ordinary Resolution 3
4. To re-appoint 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 payment of Directors' Fees of RM113,350.00 for the financial year ended 31 December 2010; Ordinary Resolution 5
6. To consider and if thought fit, to pass the following Special Resolution, with or without modifications: Special Resolution 1

PROPOSED AMENDMENTS TO THE MEMORANDUM OF ASSOCIATION OF THE COMPANY

"That the following proposed amendments to the Memorandum of Association of the Company be approved and adopted:

- a) Renumbering of the existing :
 - (i) Clause 3.6 to 3.7; and
 - (ii) Clause 3.7 to 3.8.and
- b) Insertion of a new clause as Clause 3.6 as follows :

"3.6 To provide consultancy services, awareness programmes and/or professional training in connection with, or howsoever related to, information security."

both the above amendments are as per **Appendix 1**, hereto;

AND that the said amendments to the Memorandum of Association shall be effective immediately on the date of the passing of this resolution".

7. 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 : 3 June 2011

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 a 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 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 8, Block A, Mines Waterfront Business Park, No. 3 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.

Our Direction

Vision

- To be a Globally Recognised, National Cyber Security Reference and Specialist Centre by 2020

Mission

- Creating and Sustaining a Safer Cyberspace to Promote National Sustainability, Social Well-Being and Wealth Creation

Key Result Areas (KRA)

- Global Strategic Positioning & Recognition
- National Cyber Security Capability & Capacity Building
- Support Local ICT Security Industry/ Wealth Creation
- Quality of Service
- R&D Capability in Cyber Security
- Creative Innovative & Professional Human Capital

Strategic Goals

- To Achieve Brand Recognition
- To Increase the number of Globally Recognized Cyber Security Professionals
- To Develop National Proactive & Defensive Capabilities
- To Raise National Acculturation in Cyber Security
- To Boost Local Cyber Security Industry Competitiveness
- To Deliver CyberSecurity Malaysia Core Services to Market Segments/ Technology Clusters
- To Secure and Professionally Manage Funds
- To Enhance Internal Research Capacity, Capability & Facility
- To Build Creative & Innovative Work Processes & Environment



What We Believe In



Our Core Values are : Trusted, Impartial, and Proactive.

■ Trusted

Maintaining social, ethical, and organisation norms; firmly adhering to codes of conduct and professional ethical principles

■ Impartial

Provide judgement, advice, and make decisions with high professionalism, unbiased and based on clear facts and rationale; devoid of any personal or conflict of interest

■ Proactive

Taking prompt action to accomplish objectives; anticipate challenges and identify solutions; taking action to achieve goals beyond what is required.

Client Charter



Our Promise To You

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

To make this a reality, we intend to make you, our client, the number one consideration in everything that we do.

We aim to do this through three main areas of focus:

■ Service

In delivering our service to you, we adopt values that reflect our approach and ensure our professionalism in carrying out our work.

■ **We are resourceful**

We understand that one solution never fits all. Your situation will always be specific to your own organisation, as such we are always practical and innovative when solving a problem so that we can deliver solutions that are personalised for you.

■ **We are proactive**

We take the initiative to be forward thinking and progressive when confronting problems in our work, for we know that in our industry, there is just no other way to do things.

■ **We are responsive**

Befitting our calling of keeping our cyberspace safe and secure, we make sure we step up when challenges arise, no matter the complexity, nature of problem or who calls in.

■ Quality

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

■ **We are impartial**

No matter how big or small a problem or case might be, we handle it impartially. We will provide fair and unbiased support, advice and information without discrimination or prejudice.

■ **We specialise**

To ensure you gain maximum benefit from working with us, we do only the best, so that you are assured we won't be sidetracked by issues that might hinder our performance.

■ **We are effective**

In order to maintain the highest level of service to you, we strive to deliver accurate advice and reliable service every single time.

■ Relationship

Beyond the technical world we operate in, a critical factor in our success is relationships – ties between ourselves and our clients, and ties between everyone at CyberSecurity Malaysia. This is what drives us towards excellence.

We support each other

- Each and every single staff here plays a role in helping you solve your problem. We share our expertise and experience so that you enjoy the benefits and skills of every single one of us.

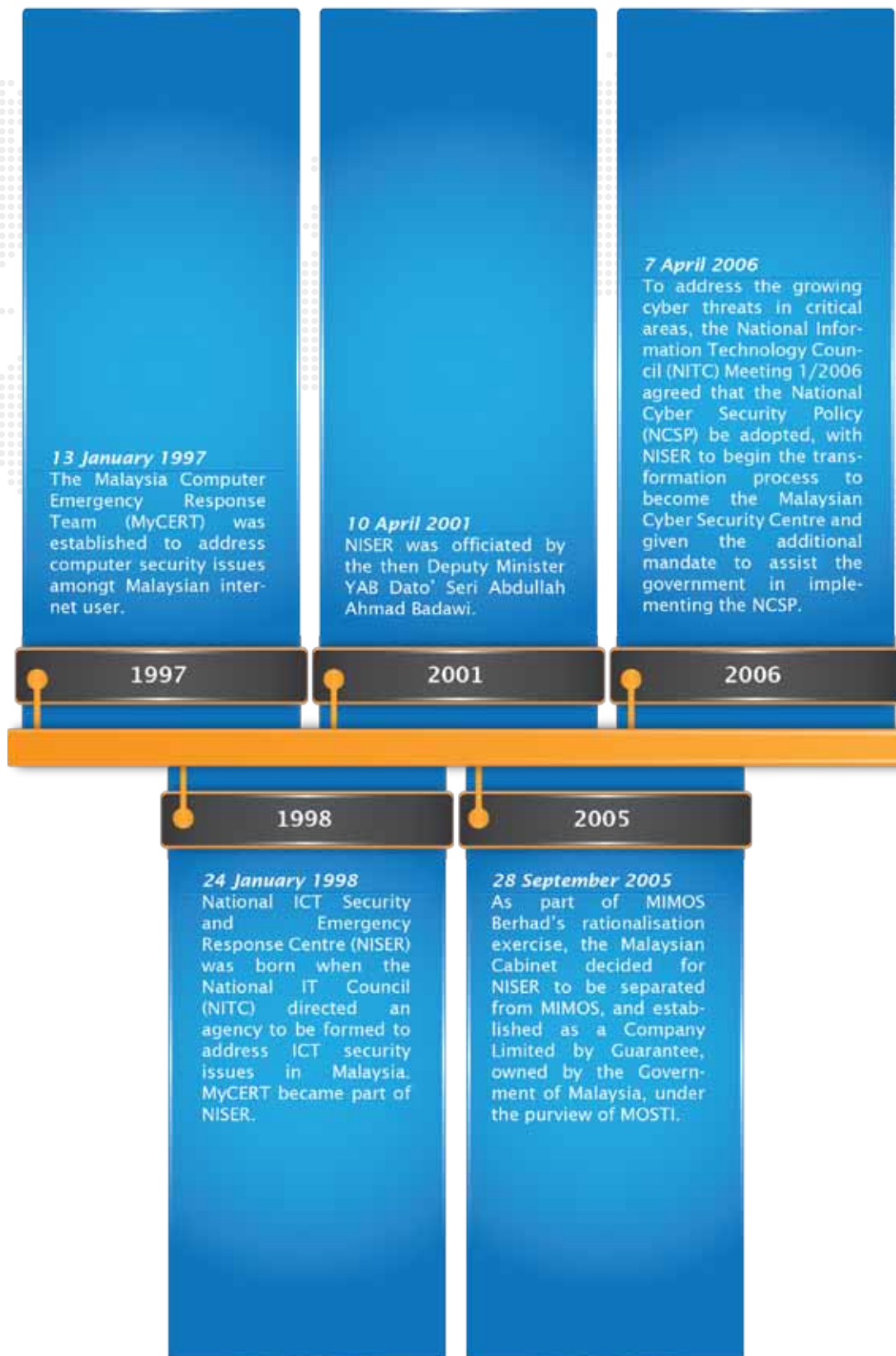
We are passionate

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

We strive to be trustworthy

- Everything we do is focused on one primary goal – you. We are here to safeguard your needs and interests and that of the community. In doing so, we hope to gain your trust and confidence.

How We Got Here



25 July 2008

CyberSecurity Malaysia was certified in Information Security Management System (ISMS), ISO/IEC 27001:2005.

8 October 2008

The Government appointed CyberSecurity Malaysia as the sole Certification Body for the evaluation and certification scheme based on MS ISO/IEC 15408:2005 Information Technology - Security Techniques - Evaluation Criteria for IT Security. This certification body is named Malaysian Common Criteria Certification Body (MyCB).

2008

3 March 2010

CyberSecurity Malaysia was appointed as a member in the Key Points Supervisory Team (TIM NSP) by the Office of the Government Chief Security Officer. This appointment aims to implement the Vulnerability Assessment Services which includes ensuring cyber security on National Key Points.

12 March 2010

CyberSecurity Malaysia has been appointed by the Office of the Government Chief Security Officer as a member in the Key Points Centre Committee (JPSP) that aims to provide a completely secure environment for the Critical National Information Infrastructure (CNII) encompassing 15 key sectors. The appointment is expected to complement and strengthen the effectiveness in the process of planning, data summarization and implementation of security procedures on the Critical National Information Infrastructure.

22 Mar 2010

CyberSecurity Malaysia has been appointed as the technical service provider that is entrusted with the honourable duty to protect the Y.A.B Prime Minister's Webpage and Blog from cyber threat.

24 September 2010

Launching of the 'CyberSAFE in School' program at the vicinity of Sekolah Menengah Kebangsaan Tandek, Kota Marudu, Sabah; by the Deputy Prime Minister of Malaysia, who is also the Minister of Education. The program aims to instill awareness on information security to primary and secondary students and their teachers.

26 November 2010

CyberSecurity Malaysia has been appointed by the Ministry of International Trade and Industry as one of the Certifier and Evaluator agency for Malaysia Trustmark that enables the private sector to implement the e-Commerce and e-Payment system.

2010

2007

30 March 2007

NISER was officially renamed CyberSecurity Malaysia and registered with the Companies Commission of Malaysia (CCM).

20 August 2007

CyberSecurity Malaysia was officially launched by the Prime Minister of Malaysia during the NITC Meeting 1/2007 at Cyberjaya.

2009

2 November 2009

CyberSecurity Malaysia services expanded with the launching of its Northern Regional Office in Perak Techno-Trade Center, Ipoh, Perak.

7 July 2009

CyberSecurity Malaysia launched the Cyber999 Help Centre during the Cyber Security Malaysia || SecureAsia@ KL event in Kuala Lumpur Convention Centre. Cyber999 Help Centre is a service offered by CyberSecurity Malaysia to handle security issues or incidents faced by computer and internet users.

1 December 2009

CyberSecurity Malaysia launched the Malware Research Centre during the World Computer Security Day in Royale Chulan Hotel, Kuala Lumpur. This centre is built to conduct research and development in mitigating malware threats, as well as to provide advisories on emerging threats to stakeholders.

Message by the Minister of Science, Technology and Innovation



It is my pleasure to say a few words for the CyberSecurity Malaysia's 2010 annual report.

With 2020 as the targeted year for the realisation of Malaysia's vision of becoming a developed country fortified with an impeccable technological advancement, CyberSecurity Malaysia, as an agency of the Ministry of Science, Technology and Innovation (MOSTI), is poised to engage in the provision of comprehensive Cyber capabilities. This is not only in terms of security but making it affordable, reachable and adaptable to all community segments.

Driven by the fundamental deliverables outlined within the National Key Result Areas (NKRAs) and the National Key Economic Areas (NKEAs), CyberSecurity Malaysia is expected to contribute towards our nation's economic growth by tapping on the global information security market with an estimated value of USD\$180 billion in 2010.

I am confident that CyberSecurity Malaysia is set to take on the challenges ahead and has prepared itself to become the leader in the protection of cyber space.

I would like to congratulate CyberSecurity Malaysia for their unrelenting endeavour to ensure the safety of all Malaysians within the cyber world. The government acknowledges the economic impact this protection provides to individuals, corporations and to our country as a whole.

Let us nurture a "Culture of Cyber Security" within ourselves and thrust forward to greater heights in realising our Vision 2020.

A handwritten signature in black ink, appearing to be 'Maximus Ongkili', written in a cursive style.

Datuk Seri Dr. Maximus Johnity Ongkili
Minister of Science, Technology & Innovation

Message by the Deputy Minister of Science, Technology and Innovation



In 2010, CyberSecurity Malaysia organised a world-class conference appropriately themed "Securing Our Digital City" in tandem with Malaysia's aspiration in becoming a Digital Nation. This is where the "Internet of Things" involving transformation and communication technology (ICT) become pervasively important. Thus, it is necessary to have an agency like CyberSecurity Malaysia to ensure availability, confidentiality and integrity of information as a way to secure the way we live, particularly in the cyberspace.

One of the initiatives by the Ministry of Science, Technology and Innovation (MOSTI) and CyberSecurity Malaysia in 2010 is the study on The Laws of Malaysia to Accommodate the Legal Challenges in the Cyber Environment. The study has since been accepted by the National IT Council (NITC) for further action where the objective is to recommend relevant amendments so as to accommodate our laws with regards to the unique legal challenges in the cyber environment of a digital community. Apart from this, additional technical measures, awareness campaigns and other relevant programmes are continuously conducted by MOSTI and its agencies.

I trust in the years to come, CyberSecurity Malaysia will continue to spearhead and strengthen our nation's cyber security through strategic capabilities and capacities building programmes.

A handwritten signature in black ink, appearing to read 'Fadillah', with a stylized, flowing script.

Datuk Haji Fadillah bin Haji Yusof
Deputy Minister of Science, Technology & Innovation

Message by Secretary General, Ministry of Science, Technology and Innovation



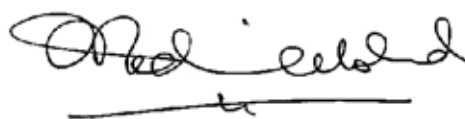
Information and Communications Technology (ICT) strategies are an essential element to developing countries. As such CyberSecurity Malaysia under the purview of the Ministry of Science, Technology and Innovation (MOSTI) plays the role of bridging between ICT and society towards catalysing socio-economic development.

MOSTI acknowledges that the resources available to the private sector alone are inadequate to bridge the digital divide across all market and socio-economic segments. Therefore, the Government via MOSTI is taking the lead in providing ICT platforms that are easily accessible to all parties.

With the pervasive use of ICT, the need for cyber security will also intensify. A strong ICT security in Malaysia that protects privacy and safety of information assets as well as intellectual property, will create confidence for investors to begin their operations here which provide a multitude of economic gains such as new employment opportunities, technology transfer, development of infrastructure, elevation of socio-economic standing and most importantly, wealth creation.

CyberSecurity Malaysia has in 2010 successfully engaged in a series of significant activities for ICT and cyber security development in Malaysia. One example is the provision of the Malaysian Common Criteria Evaluation and Certification (MyCC) Financial Assistance under the Second Economic Stimulus Package Fund to enable innovative companies to access the MyCC Scheme services, which have helped to boost the global market stand of their Made-in-Malaysia ICT products.

I am convinced that CyberSecurity Malaysia will continue to achieve monumental feats in the future in its quest to realise its vision "To be a Globally Recognised, National Cyber Security Reference and Specialist Centre by 2020".



Dato' Madinah Binti Mohamad
Secretary General,
Ministry of Science, Technology and Innovation.



WHAT IS CYBER999

Cyber999 is a service offered by CyberSecurity Malaysia to handle computer security incidents faced by Malaysian internet users.



Mode of reporting

Web Reporting

[http://www.mycert.org.my/report_incidents/
online_form.html](http://www.mycert.org.my/report_incidents/online_form.html)

Report via Telephone

Hotline: 1300 - 88 - 2999

Report via Handphone

Handphone No: 019 - 2665850

Report via SMS

Handphone No: 019 - 2813801

Report via Fax

Fax No: +603 - 8945 3442

Report via Email

Email Address: cyber999@cybersecurity.my

CYBER999 FUNCTIONS

- Analyze, detect and contain incidents faced by computer/internet users from further propagating.
- Provide recovery and eradication steps to recover from the incidents.
- Provide preventive measures in order to prevent from future incidents.
- Provide fixes, patches, upgrades information for to secure users computers.
- Provide post-incident follow ups with the complainants.
- Assist in communicating/escalating users reports to third-parties, i.e Law Enforcement Agencies for further investigation, if necessary.

REPORTS/PROBLEMS/INCIDENTS THAT CAN BE REPORTED TO CYBER999

- Intrusion
- Denial of Service
- Hack Threats
- Harassment
- Fraud
- Spam
- Malicious Code

INFORMATION THAT MUST BE INCLUDED IN THE REPORT TO CYBER999

- Brief description of the incident.
- Symptoms of the incident.
- Date and time of the incident occurrence.
- Actions that have been taken to resolve the incident.
- Email full header, if any.
- Log files, if any.
- Your contact details in order for us to call or email you back.

The reporting hours are:

- i. 24x7 for Handphone, SMS, Web and Email Reporting
- ii. Mon - Fri, 8:30 am - 5:30 pm for Telephone and Fax Reporting

Chairman's Statement



“

The cultivation of CyberSecurity Malaysia's innovation culture will become part of our daily life and provides a cyber security code of conduct that we live by. This will be the pinnacle of achievement for CyberSecurity Malaysia. ”

Another year passed by and CyberSecurity Malaysia has shown tremendous growth in all its operational and development aspects, pushing boundaries towards realizing its vision of becoming a Globally Recognised, National CyberSecurity Reference and Specialist Centre by 2020.

Although CyberSecurity Malaysia is entrusted with an enormous task to protect the “virtual world” within our country, the threats posed by the unscrupulous cyber terrorists and criminals is very much real.

CyberSecurity Malaysia has a vital responsibility to ensure the incessant safety of all Malaysian that venture online and as such has further embark and enhance its capabilities on various strategic engagement through the provision of innovative services including its Digital Forensic Lab and Expertise, The Malaysia Common Criteria Scheme (MyCC), Malware Research Centre, CyberSAFE Programme and the inauguration of CyberSecurity Malaysia – Awards, Conference & Exhibition (CSM-ACE).

Our role has transcend beyond mere protection, CyberSecurity Malaysia now functions as an educator that impart, cultivate and nurture vital and innovative knowledge to the target group in order to inculcate an ethical & safe cyber culture.

This is a challenging task indeed, changing ones mindset and organizational practices require exponential infusion of knowledge, understanding and recognition towards the positive impact that these innovation will bring.

With this realization, CyberSecurity Malaysia initiated the CyberSecurity Malaysia – Awards, Conference & Exhibition (CSM-ACE), which has been designed to encourage participation, induce the culture of innovation and promotes cyber security within Malaysian organizations, academicians and practitioners. The program aims to sustain a safe innovative and technological advancement within Malaysia that is able to generate substantial socio-economic value.

CyberSecurity Malaysia strives in their relentless effort to provide a holistic service and education within Malaysia and will continue to pool and acquire new technologies, knowledge & innovative ideas either locally or internationally towards the formation of a healthy connected cyber world.

I am proud to state that CyberSecurity Malaysia will continue to rise beyond its duties and functions as the guardian of the cyber world in Malaysia.

As we advance into the future, the cultivation of CyberSecurity Malaysia's innovation culture will become part of our daily life and provides a cyber security code of conduct that we live by. This will be the pinnacle of achievement for CyberSecurity Malaysia.

I take this opportunity to convey my deepest appreciation to the Board of Directors', Ministry of Science, Technology and Innovation (MOSTI), other government agencies, international liaison and partners that has rendered their valuable support towards the fabrication of a Safer Cyberspace that Promotes National Sustainability, Social Wellbeing and Wealth creation.



**General Tan Sri Dato' Seri Panglima
Mohd Azumi bin Mohamed** (Retired)
Chairman CyberSecurity Malaysia

Board Members



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

General Tan Sri Dato' Seri Panglima Mohd Azumi (Retired) was appointed to the Board as Chairman in July 2009. A soldier with an illustrious military career over 37 years, he had served the Malaysian Armed Forces in various capacities including as Commander of the 10th Parachute Brigade, Commander of the First Infantry Division and Chief of the Army before his retirement in December 2004. During his service, he had the honour of serving with the United Nations Iraq/Kuwait Observation Mission in the aftermath of the First Gulf War. He has been recognised internationally by France and the United Nations, receiving the French Award Officer Ordre National du Merite and the UN Medal for International Peacekeeping respectively. Apart from military credentials from the Officer Cadet School in Portsea, Australia, the Australian Army Infantry Centre and the US Army Infantry Centre at Fort Benning, he also holds a Master of Science in Natural Resource and Strategy from the National Defense University in Washington DC and a Graduate Diploma in Strategy from the Australian Capital Accreditation Agency. Since his retirement, General Tan Sri Dato' Seri Panglima Mohd Azumi (Retired) has been appointed to the National Unity Advisory Panel and the board of several public-listed and private companies.



■ **YBhg. Lt Col Dato' Prof. Husin Bin Jazri (Retired), CISSP CBCP CEH**

ISLA

Director and Chief Executive Officer

YBhg. Lt Col Dato' Prof. Husin Jazri (Retired), has served as Chief Executive Officer and Board Member since the inception of CyberSecurity Malaysia. Among his other posts are Chair of the Organization of Islamic Countries - Computer Emergency Response Team (OIC- CERT), member of the Asian Advisory Board of the International Information Systems Security Certification Consortium, Inc. (ISC)², and Chairman of the Malaysian Vocational Advisory Committee - Information and Communication Technology (ICT), Department of Skills Development, Ministry of Human Resources. He holds a Bachelor's Degree in Engineering from University of Hartford, Connecticut, USA; a Post Graduate Diploma in System Analysis from Universiti Teknologi MARA (UiTM); a Master of Science with Distinction in Information Security from Royal Holloway University of London, UK; and a Master in Business Administration from Universiti Putra Malaysia (UPM). He is a Certified Business Continuity Professional (CBCP) by Disaster Recovery Institute (DRI), USA; a Certified Information Systems Security Professional (CISSP) by the (ISC)2, and a Certified Professional Hacker (CEH) by EC-Council. He received the following Achievement Award in recognition of his life-long contributions and sustained excellence throughout his entire information systems security career.



- Harold F. Tipton Life Achievement Award 2010 by the International Information System Security Certification Consortium (ISC)2, USA.
- One of the most outstanding CSO in ASEAN region in 2010 - by the Chief Security Officer (CSO) Conference & Awards, Vietnam.
- ICT Personality of the Year 2010 - by PIKOM Leadership Awards, Malaysia.
- Senior Information Security Professional 2009 - by the (ISC)2 Asia-Pacific Information Security Leadership Achievement (ISLA) Award, USA.

■ **Dato' Madinah Binti Mohamad**

Director



Dato' Madinah Mohamad was appointed to the Board in July 2009. She is the Secretary General of the Ministry of Science, Technology and Innovation 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.

Dato' Madinah holds a Bachelor's degree in Political Science from Universiti Sains Malaysia (USM) and a Masters in Human Resource Development from Universiti Putra Malaysia (UPM).

Board Members

■ **Datuk Dr. Abdul Raman Bin Saad**

Director

Datuk Dr. Abdul Raman is the Managing Partner of ARSA LAWYERS (Abdul Raman Saad & Associates) and was appointed to the Board in June 2009. An advocate and solicitor since 1977, he had served with 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 today 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 Dr. Abdul Raman holds an Honours Degree in Law from the University of Singapore since 1974 and a Masters Degree in Law (with specialisation in Electronic Law) from the University of Melbourne, Australia. He also holds a Doctorate degree in Business Administration from Midwest Missouri University, USA. He is a Director of Technical University Malaysia Melaka (UTEM)



■ **Datuk Haji Abang Abdul Wahap Bin Haji Abang Julai**

Director



Datuk Haji Abang Abdul Wahap was appointed to the Board in May 2009. He had a distinguished career with the Royal Malaysian Police over 37 years, retiring as the Director of Narcotics Crime Investigation Department in 2007. He had also served as Deputy Director of Management in Training at Bukit Aman Headquarters Kuala Lumpur and Deputy Commissioner of Police for Sarawak. For his service, he was conferred the 'Pingat Panglima Gagah Pasukan Polis', the highest award for police officers. He is presently serving as Independent non executive director to a few companies in Sarawak and is very much involved in Sukan Malaysia (SUKMA) Sarawak Contingent.

Datuk Haji Abang Abdul Wahap holds a Bachelor of Law from the International Islamic University of Malaysia (IIUM) and an Advanced Diploma in Police Science from Universiti Kebangsaan Malaysia (UKM).

■ **Ir. Md. Shah Nuri Bin Md. Zain**

Director

Ir. Md. Shah Nuri 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 Bhd, then as an engineer with the Public Works Department under the Ministry of Works.

Ir. Md. Shah Nuri holds a Bachelor of Science in Electrical Engineering from the Connecticut State University in the United States.



■ **Rubaiah Binti Hashim**

Director



Puan 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.

Puan Rubaiah holds a Bachelor of Science Honours Degree in Mathematics and IT Applications from the University of Wales Institute of Science and Technology (UWIST), in the United Kingdom.

Board Members

■ Rohani Binti Mohamad

Director

Puan 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) at the Prime Minister's Department, 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).

Puan Rohani holds a Bachelor of Science in Statistics and Operations Research from the Institute of Science and Technology, University of Manchester, United Kingdom and a Diploma in System Analysis from Universiti Teknologi MARA (UiTM). In 2010, she received 'Anugerah Pingat Kesatria Mangku Negara (KMN).



■ Jailany Bin Jaafar

Company Secretary,

Head of Legal & Secretarial



■ Abd Rouf Bin Mohammed Sayuti

Head of Internal Audit





CyberSAFE

Cyber Security Awareness For Everyone

www.cyberSAFE.my

Corporate Office:

CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888

Regional Office:

CyberSecurity Malaysia, Level 19, Perak Techno-Trade Center, Bandar Meru Raya, Off Jln. Jelapang, 30020 Ipoh, Perak Darul Ridzuan | Tel: +605 - 528 2088 | Fax: +605 - 528 1905

Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

Management Committee



■ **YBhg. Lt Col Dato' Prof. Husin Bin Jazri (Retired), CISSP CBCP CEH**

ISLA

Director and Chief Executive Officer

(Retired), has served as Chief Executive Officer and Board Member since the inception of CyberSecurity Malaysia. Among his other posts are Chair of the Organization of Islamic Countries - Computer Emergency Response Team (OIC- CERT), member of the Asian Advisory Board of the International Information Systems Security Certification Consortium, Inc. (ISC)², and Chairman of the Malaysian Vocational Advisory Committee - Information and Communication Technology (ICT), Department of Skills Development, Ministry of Human Resources. He holds a Bachelor's Degree in Engineering from University of Hartford, Connecticut, USA; a Post Graduate Diploma in System Analysis from Universiti Teknologi MARA (UiTM); a Master of Science with Distinction in Information Security from Royal Holloway University of London, UK; and a Master in Business Administration from Universiti Putra Malaysia (UPM). He is a Certified Business Continuity Professional (CBCP) by Disaster Recovery Institute (DRI), USA; a Certified Information Systems Security Professional (CISSP) by the (ISC)², and a Certified Professional Hacker (CEH) by EC-Council. He received the following Achievement Award in recognition of his life-long contributions and sustained excellence throughout his entire information systems security career.



- Harold F. Tipton Life Achievement Award 2010 by the International Information System Security Certification Consortium (ISC)², USA.
- One of the most outstanding CSO in ASEAN region in 2010 - by the Chief Security Officer (CSO) Conference & Awards, Vietnam.
- ICT Personality of the Year 2010 - by PIKOM Leadership Awards, Malaysia.
- Senior Information Security Professional 2009 - by the (ISC)² Asia-Pacific Information Security Leadership Achievement (ISLA) Award, USA.

Zahri Bin Yunos

Chief Operating Officer

Zahri has been the Chief Operating Officer since 2007. Zahri was actively involved in the establishment of NISER (National ICT Security and Emergency Response Centre)'s Panel of Experts (POE) and the Organisation of Islamic Conference-Computer Emergency Response Team (OIC-CERT), which boosted Malaysia's international image in cyber security. He is a certified Associate Business Continuity Professional (ABCP) by the Disaster Recovery Institute International (DRII), USA. Zahri has been awarded Senior Information Security Professional Honoree at the Fourth Annual (IS2)2 Asia Pacific Information Security Leadership Achievement Program in July 2010 by the International Information System Security Certification Consortium (IS2)2, USA. Zahri holds a Master of Science in Electrical Engineering from Universiti Teknologi Malaysia (UTM) and a Bachelor of Science in Computer Science from Fairleigh Dickinson University, New Jersey, USA. As a recognition to Zahri's expertise in the area of cyber security, he was appointed as industry panelist by Universiti Teknologi Malaysia's Advanced Informatics School to advice on the development of curriculum for post graduate programmes.



Mohd Roslan Bin Ahmad

Vice President, Management Services



Mohd Roslan has led the Management Services Division since 2007 with a portfolio that includes the departments of Finance, Administration & Physical Security and Procurement & Logistics. He is a certified Safety and Health Officer (SHO) from the National Institute of Occupational Safety and Health (NIOSH) Malaysia and Associate Member of Malaysian Institute of Management (MIM). Mohd Roslan holds a Masters of Management (MMgt) from Open University Malaysia (OUM), a Bachelor of Science in Civil Engineering from University of Hartford, Connecticut, USA and a Post Graduate Diploma in System Analysis from University Technology MARA (UiTM).

Management Committee

■ **Roshdi Bin Ahmad**

Vice President, Corporate Planning & Strategy

Roshdi has been with CyberSecurity Malaysia since 2007 and now leads three departments which include Corporate Branding & Media Relations, Strategy Management, Human Capital Development. He has managed and secured various large ICT projects and has vast experience in different disciplines particularly in corporate strategy, marketing and operations. He holds a Bachelor's Degree (Hons) in Business Studies (Marketing) from Universiti Teknologi MARA (UiTM) and a Diploma in Agribusiness from Universiti Putra Malaysia (UPM).



■ **Adli Bin Abd Wahid**

Vice President, Cyber Security Responsive Services

Head of the Malaysia Computer Emergency Response Team (MyCERT) since 2007, Adli also leads the Cyber999 Help Centre as well as the CyberSecurity Malaysia Malware Research Centre. He is actively involved in numerous global computer security initiatives and has spoken at various computer security forums worldwide. Adli was an honouree of the (ISC)² Information Security Leadership Achievement (ISLA) Award in the IT Security Practitioner category in 2009. He holds a Master of Science in Computer Science specialising in Software Engineering.



■ Mohd Shamir Bin Hashim

Vice President, Government & Multilateral Engagement

Mohd Shamir has been with CyberSecurity Malaysia since 2006 and is now leading the Government and Multilateral Engagement Division. An engineer by training, he has been in the information and communication field for more than 20 years. Presently, he is involved with the ministries and government agencies mainly as a core member of the secretariat team to implement Malaysia's National Cyber Security Policy (NCSP) and a national committee that mitigates cyber security incidences. At the international platform, he is involved in the establishment of the Organisation of Islamic Conference – Computer Emergency Response team (OIC-CERT) and now plays an active role in the administration of the collaboration. Mohd Shamir holds a Bachelor of Science in Civil Engineering from the University of Missouri-Kansas City, USA and is a certified Professional in Critical Infrastructure Protection (PCIP) from the Critical Infrastructure Institute, Canada, Certified Ethical Hacker from the EC-Council and an Associate Business Continuity Professional (ABCP) of the DRI institute. He was also a recipient of the Information Security Leadership Achievements (ISLA)2010 from (ISC)² in recognition of his contribution in information security.



■ Dr. Solahuddin Bin Shamsuddin

Vice President, Research

Dr. Solahuddin leads the Security Quality Management Services Division which includes the departments of Security Assurance, Security Management & Best Practices, Research Coordination, and Cyber Consulting Group. He was one of the pioneers of cyber security efforts in NISER (National Information & Communication Technology Security and Emergency Response Centre). He holds a PhD in Computer Science from University of Bradford, UK, a Degree in Electrical Engineering from Wichita State University, Kansas, USA and a Post Graduate Diploma in System Analysis from Universiti Teknologi MARA (UiTM).

Management Committee

■ **Lt. Col. Mustaffa Ahmad (Retired)**

Vice President, Outreach

Lt. Col. Mustaffa Ahmad (Retired) has been with CyberSecurity Malaysia since 2007 after serving more than 18 years in the Malaysian Armed Forces. Currently, he is the Vice President of Outreach Division, responsible for Outreach and Corporate Event, PR and Protocol Departments. He holds a Bachelor and a Master's Degree in Mass Communications from the University of Wisconsin, Superior, USA; a Post Graduate Diploma in Strategic Studies from University Malaya and he is also a graduate of the Malaysian Armed Forces Staff College in 2000.



■ **Jailany Bin Jaafar**

*Head, Legal and Secretarial Department
/ Company Secretary*



As Head of Legal & Secretarial department since August 2007, Jailany is responsible for all legal and secretarial matters of the company and in advising the management on legal and company secretarial matters. An Advocate and Solicitor (non-practicing) of the High Court of Malaya and a licensed Company Secretary, Jailany holds a Bachelor of Laws (Hons) from Universiti Malaya (UM).

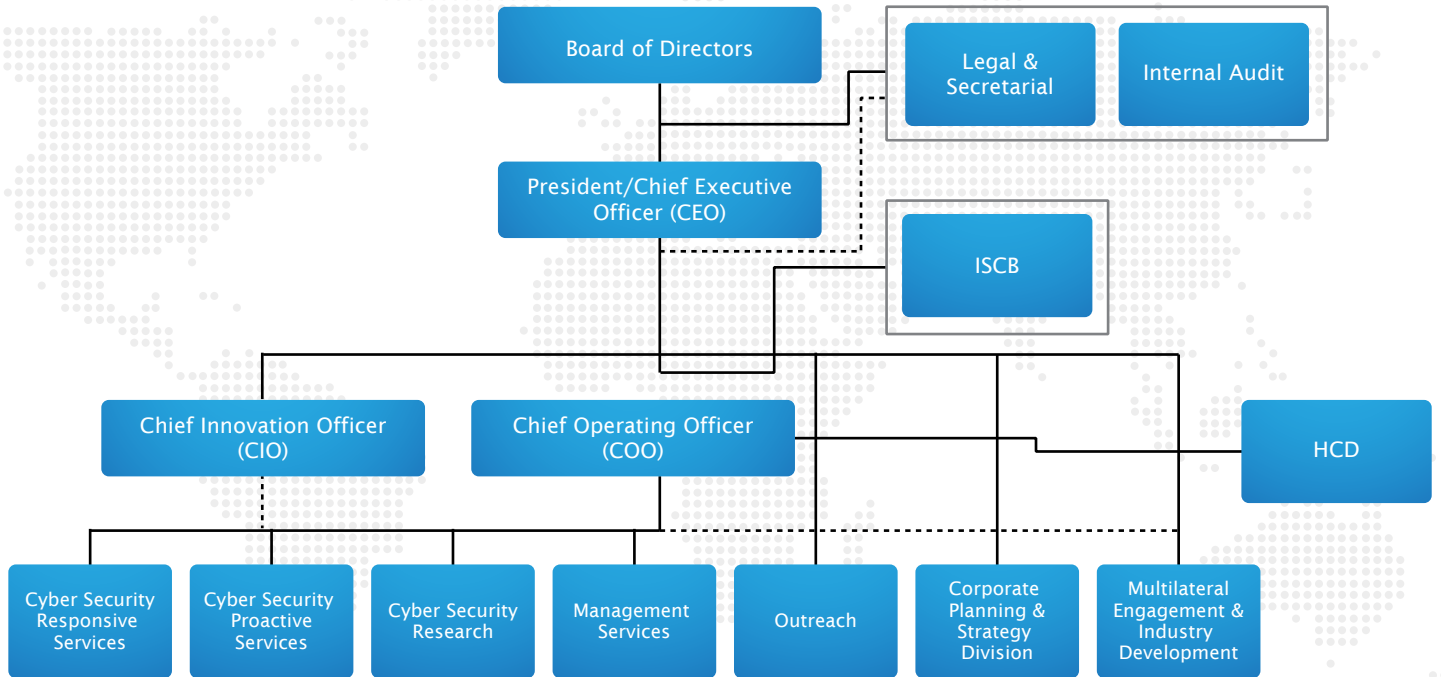
■ Razman Azrai Bin Zainudin

Head, Strategy Management

Head of Strategy Management, Razman has more than 16 years of experience in the ICT industry, leading ICT consultation services to key companies in the Asia Pacific region. He was a member of the National Strategic ICT Roadmap Technical Committee. Razman is also CyberSecurity Malaysia's secretariat to the Management Committee. He holds a Bachelor of Science in Management Science & Information Systems from University of Rhode Island, USA, MBA (IT) from Staffordshire University, UK and he is a Kaplan Norton Balanced Scorecard certified.



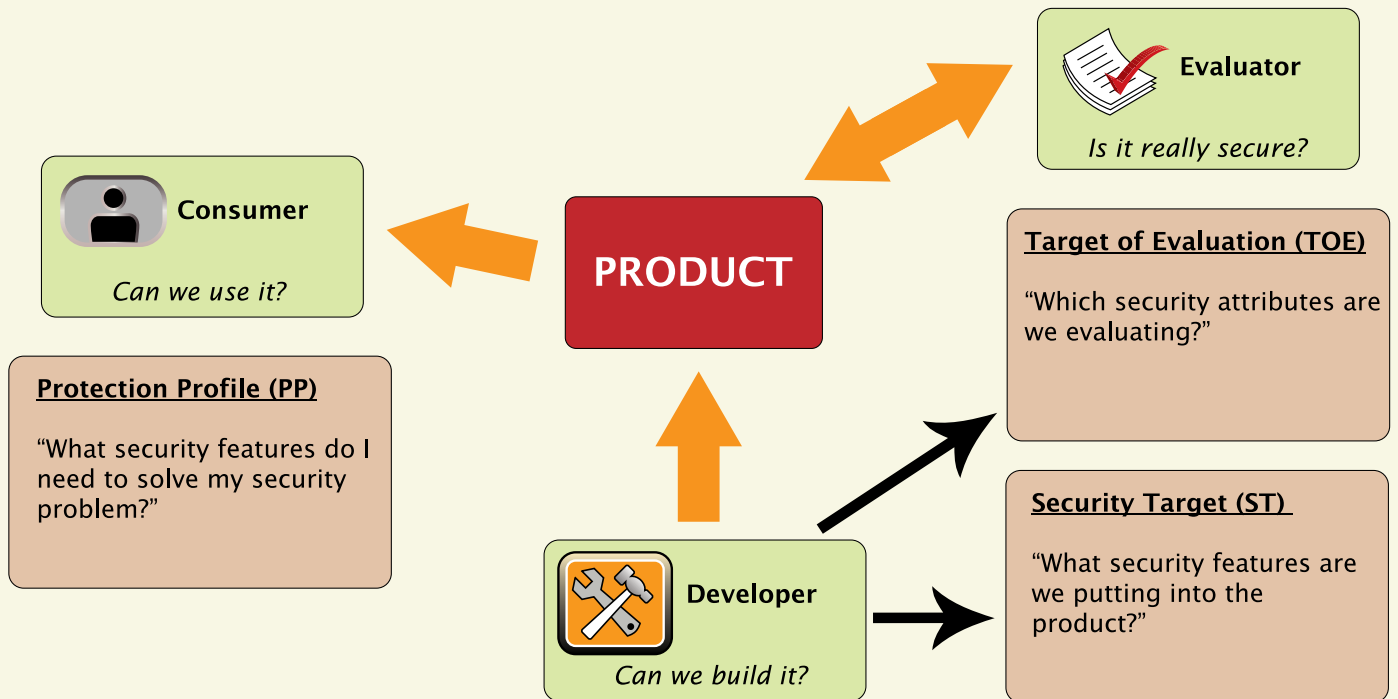
Organisation Chart



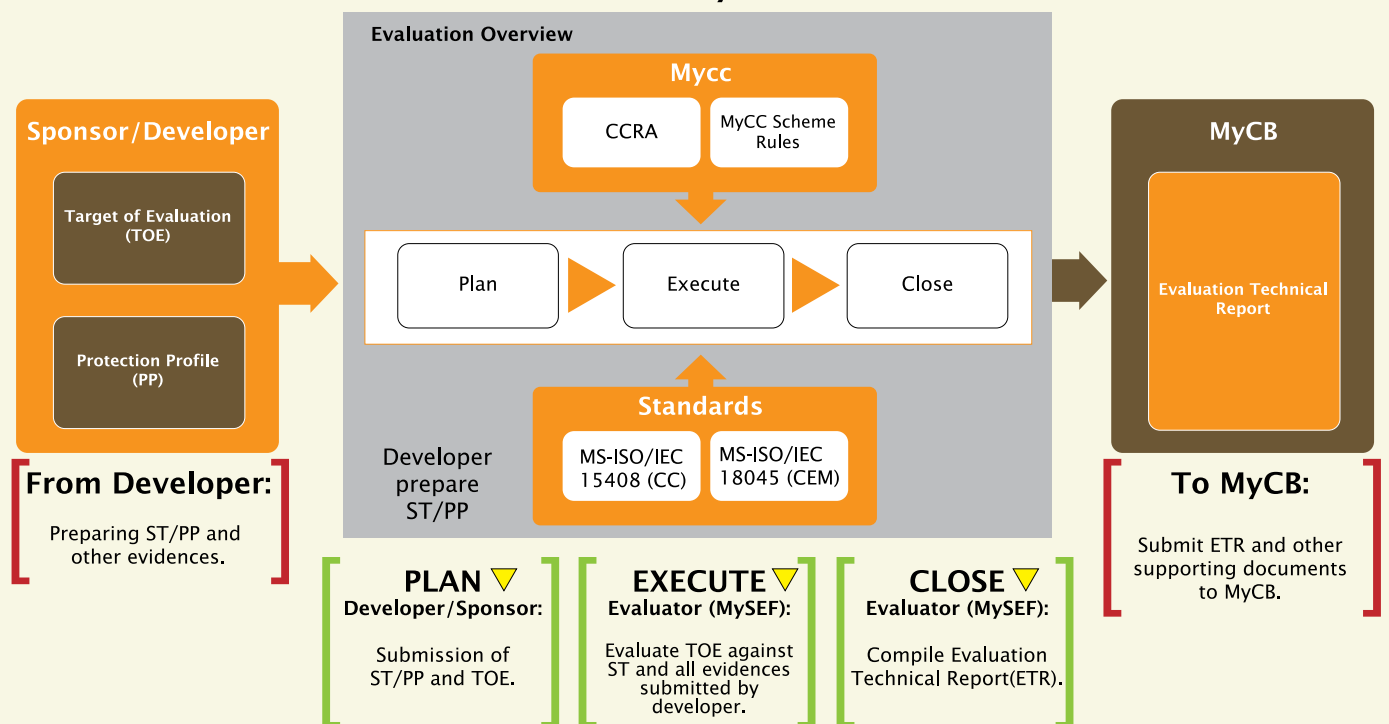
ISCB - Information Security Certification Body
HCD - Human Capital Development Dept

Process of Product Evaluation for Certification

Part 1: Understanding the Core Element of Common Criteria (CC) (for Developers and Consumers)



Part 2: Product Evaluation Process under MySEF



Corporate Office:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888

Regional Office:
CyberSecurity Malaysia, Level 19, Perak Techno-Trade Center, Bandar Meru Raya, Off Jln. Jelapang, 30020 Ipoh,
Perak Darul Ridzuan | Tel: +605 - 528 2088 | Fax: +605 - 528 1905

Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

Foreword by the CEO



“

2010 has been declared by MOSTI as the “Innovation Year for Malaysia”. We at CyberSecurity Malaysia fully supports the Malaysia Innovative 2010 program and has embarked on various activities that is poised to strengthen our presence and service engagement to the general public.

”

2010 has been a very challenging yet productive year for CyberSecurity Malaysia. And 2010 was declared by MOSTI as the “Malaysia Innovative Year”. We at CyberSecurity Malaysia fully supports the Malaysia Innovative 2010 programme and has embarked on various activities that is poised to strengthen our presence and service engagement to the general public.

Individuals, organizations and governments’ dependency on the global interconnection within the cyber world has become something of an imminent value that pushes the global economic reach even further. Efforts are being made to bring together organizational structures at the national and international level to facilitate communication, information exchange and recognition of digital credentials across regions and jurisdictions.

This being the factual truth has been the triggering point for the creation of an Innovation Culture in Malaysia that is expected to contribute towards the economic impact of sustainable proportion for Malaysia to advance further as a safe country for internet trading, commerce and eventually wealth creation.

One of the main focuses initiated by CyberSecurity Malaysia towards the realization of the above mentioned objective is the introduction of The Malaysia Common Criteria Scheme (MyCC).

Through MyCC, the two fundamental building blocks of an innovative culture namely "Research" and "Entrepreneurship" will be promoted. Research promotes the production of new inventions and the innovation of existing products and technology that will be developed for commercialisation into profitable end products.

Entrepreneurship complement the function of "Research" via the engagement of industry players to create and manufacture technologically advanced cyber security products that generate economic benefit for Malaysia and encourages the setting up of a Common Criteria evaluation services to cyber security product developers locally and abroad.

The spin-off from this program will be the production of value-added products, increase in GDP growth, employment and investment opportunity. In August 2010, CyberSecurity Malaysia forged a collaborative agreement with stractec.net, a leading provider of independent information security consulting and testing services in Australia and South East Asia under the MyCC Scheme. This collaboration sets up a standard in which products containing cyber security components will be evaluated and certified under the Common Criteria MS ISO/IEC 15408 standard, elevating the products value towards global acceptance and competitiveness.

Year 2010 also sees the incremental incidence of cyber threat, in which since the commencement of its operation, our Cyber999 Help Centre has attended more than 188,686 cyber security related incidents including 8,090 incidences that are reported directly to Cyber999 Help Centre, 155,809 spam cases, 24,187 Honeynet related incidences and 600 digital forensic cases.

The collective goal is to prevent, prepare for, respond to and recover from any incidents rapidly while minimizing damage. This can only

be achieved via the collaborative effort not only from CyberSecurity Malaysia as the protector, but from a knowledgeable user that engages in a safe practice within the cyber world, hence the introduction of CyberSAFE (Cyber Security Awareness for Everyone) programme that is of national interest to propagate and inculcate cyber security awareness to all Malaysians reaching out to diverse demographic and geographical profile.

The CyberSAFE programme receives tremendous public response in which for year 2010 alone, a total of 30,257 Malaysian participated in the program coming from various public and private sector background.

As society strides forward into the revolutionary future, CyberSecurity Malaysia continues to explore, innovate, acquire and disseminate new capabilities within the cyber world, in our task to provide the pinnacle of security excellence for all Malaysia.

We are proud to become one of the catalysts and the forefront provider of cyber security infrastructure within Malaysia and we aspire to turn Malaysian into a "Digitally Savvy and Safe Cyber Society" able to contribute towards our country's wealth creation.



**YBhg. Lt Col Dato' Prof. Husin Bin Jazri
(Retired),**
CISSP CBCP CEH ISLA
Director and Chief Executive Officer
CyberSecurity Malaysia

Operation's Review

2010 has been a very productive yet exciting year for CyberSecurity Malaysia. Apart from running our core technical services, we have embarked on several hallmark activities such as organizing the CSM-ACE 2010, participating in Malaysia Innovative 2010, and celebration of a Safer Internet Day as well as World Computer Security Day. Our Corporate Social Responsibility (CSR) programme also took off in 2010, and our contribution has been globally recognized through the conferment of various awards from local and international organizations. Another major milestone is the establishment of our first branch for the Northern Region in Ipoh, Perak in late November 2009 in which within its short period of inception has managed to conduct several productive activities in 2010. The operations review is divided into a review of our core cyber security services and the key events in 2010 as per the list below:

1. Our Services

- 1.1 MyCERT and Cyber999 Help Centre
- 1.2 Digital Forensics and Cyber CSI
- 1.3 Security Management and Best Practices (SMBP)
- 1.4 Security Assurance
 - 1.4.1 Malaysian Security Evaluation Facility (MySEF)
 - 1.4.2 Malaysian Vulnerability Assessment Centre (MyVAC)
- 1.5 Malaysian Common Criteria Certification Body (MyCB)
- 1.6 Cyber Security Research and Policy
 - 1.6.1 Strategic Policy Research
 - 1.6.2 Cyber Media Research
 - 1.6.3 Policy Implementation Coordination
- 1.7 Outreach
- 1.8 Information Security Professional Development
- 1.9 Northern Region branch

2. Key Events in 2010

- 2.1 Awards & Recognition
- 2.2 CyberSecurity RSA Seminar 2010
- 2.3 The 3rd National Cyber Drill-X-Maya 3
- 2.4 Strategic Collaboration Agreement with stratsec.net Australia for MyCC
- 2.5 CSM-ACE2010
- 2.6 Safer Internet Day (SID)
- 2.7 World Computer Security Day (WCSD)
- 2.8 Corporate Social Responsibility Projects
- 2.9 MI2010 Zon Selatan and Malam Kreativiti MI2010 Zon Selatan

1. Our Services



1.1 MyCERT and Cyber999 Help Centre

Malaysia Computer Emergency Response Team (MyCERT) established in 1997 has seen an increase of reports relating to computer incident since the commencement of its operation. Apart from its primary role to maintain computer and cyber security, MyCERT also provides advisory services through its Cyber999© Help Centre to local Internet users and actively assists other international computer security incident response teams (CSIRTs) around the world to handle cyber threat through cooperation, knowledge sharing, and capability development.

The Cyber999© Help Centre handled a total of 8,090 security incident cases formally reported in 2010. In addition, MyCERT had also processed about 40,076 incidents related to malware intrusion attempts, infection attempts and remote file inclusion (RFI) attacks transpired in its research network project operated by the Malware Research Centre.

To further strengthen cooperation with other security organizations, MyCERT through CyberSecurity Malaysia signed Memorandum of Understanding (MoU) with the United Arab Emirates Computer Emergency Response Team (aeCERT) and Taiwan Information Security Center National Cheng-Kung University (TWISC) to manage Incident Handling cooperation and HoneyNet information capacity exchange activities. In addition, Non-Disclosure Agreement (NDA) also signed with Khazanah Nasional Berhad, My-Partners and F-Secure forging collaboration towards data and information sharing for the HoneyNet Malware research project.

New partnership with the Conficker Working Group and SpamCOP, as well as existing international cooperation with the Asia Pacific Computer Emergency Response Teams (APCERT), Organization of the Islamic Conference – Computer Emergency Response Teams (OIC-CERT) and the Forum of Incident Response Security Team (FIRST), enabled MyCERT to further strengthen its capability.

Contribution in terms of security feeds exchange have also been extended to the Critical National

Operation's Review

Information Infrastructure (CNII), consisting of:

- Malaysia Airlines
- New Straits Time Press (NSTP)
- Jaring
- Tenaga Nasional Berhad (TNB)
- MSN
- Ministry of Health (MOH)
- Technical University of Malaysia Malacca (UTEM)
- International Islamic University Malaysia (IIUM)
- Universiti Malaysia Pahang (UMP)
- TM
- SIRIM
- Department of Public Works, Malacca (JKR MELAKA)
- MELAKA NET
- F-Secure
- McAfee

MyCERT is active in knowledge sharing and participated in various conferences, training and seminars both in the local and international arena. MyCERT personnel conducted over 40 talks locally including at the following events:

- CyberSecurity RSA Conference, Kuala Lumpur
- Program in Collaboration with CGSO
- Program in Collaboration with Syariah Judicial Department, Bangi
- MSC Malaysia Open Source Conference 2010 (MSCMOSC2010), Kuala Lumpur
- KL Green Hat 2010, Kuala Lumpur
- MYGOSSCON 2010, Kuala Lumpur

And at the following international events:

- A-ISAC and Botnet Prevention Conference, Taipei, Taiwan
- APCERT Annual Conference and Annual General Meeting, Phuket, Thailand
- The Honeynet Project 9th Annual workshop, Mexico
- APWG - The fourth annual Counter-eCrime Operations Summit (CeCOS IV), Brazil
- 5th ENISA Workshop, Heraklion, Crete Greece Via Skype
- SIGINT 2010, Chaos Computer Club (CCC), Cologne, Germany
- 22nd Annual FIRST Conference, Miami, USA
- 6th International Conference on Information Security, Islamabad, Pakistan
- CSM-ACE 2010
- OICCERT Regional Workshop (Asia), Kuala Lumpur

MyCERT also conducted hands-on training at the following events:

- Log Analysis & Web Security, OIC-CERT Regional Workshop (Middle East), Cairo, Egypt
- Incident Handling Analysis, OIC-CERT Regional Workshop (Africa Region), Rabat, Morocco
- Analyzing Malicious PDF with Open Source Tools, MSCMOSC2010, Kuala Lumpur, Malaysia
- Interception and Analysis of Malicious Traffic Based on NDIS Intermediate Driver, SYSCAN2010, Hangzhou, China
- Log analysis hands-on training & Analyzing Malicious PDF File, CSM-ACE 2010 / OICCERT Regional Workshop (Asia), Kuala Lumpur

MyCERT was involved in three cyber security exercises in 2010 - the Asia Pacific CERT (APCERT) Drill, the ASEAN CERT Incident Drill (ACID) and the National Cyber Drill (X-Maya 3) designed to assess and improve National Cyber Crisis Management Plan together with CNII to prepare them against cyber attacks.

In 2010, four (4) of MyCERT's personnel achieved their certification from the prestigious SysAdmin, Audit, Network, Security (SANS) Institute, for the SANS GPEN (Penetration Testing), and SANS GREM (Reverse Engineering). Meanwhile, eight (8) team members received the Certified Ethical Hacker (CEH) certification from the EC Council.

MyCERT registered three significant outcomes in 2010 through the launching of its in-house security tools development. The launching of MyKotakPasir and Gallus during the X-Maya3 National Drill on 4th August 2010 proved that security professionals in CyberSecurity Malaysia are able to develop critical security tools that contributes towards our unrelentless effort to safeguard our nation's cyber security.

- DontPhishMe add-on for Mozilla Firefox; developed and launched on 3rd July 2010 was invented by a member of the team. This invention provides a security mechanism that prevents online banking phishing threats and is specifically designed to protect local banks in Malaysia.
- CyberSecurity Malaysia's Customer Contact Centre (CCC) was established in 2010 with the toll free number: 1300 88 2999. The main objective of the establishment of the CCC is to create a centralized unit to better manage MyCERT's customer activities and streamline the objective of providing and achieving excellent customer service satisfaction. A total of 555 calls were received in its first six months of inception. CCC is an effective and efficient way to track and manage customer's demand that has become increasingly critical and urgent.



2011 is perceived as a challenging year for MyCERT with an expected increase of incidents report to be encountered from the Malaysian public as well as to fulfil our imperative task to produce newly improved security tools under the Malware Research Centre. Strengthened by other support services offered by CyberSecurity Malaysia, MyCERT will continue to position itself at the forefront in its role to safeguard the nation from cyber security threats. MyCERT looks forward to all the challenges and interesting engagements in 2011.

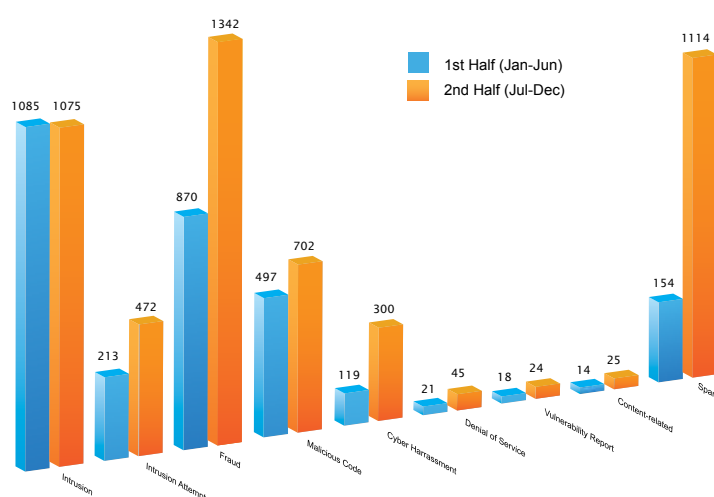


Figure 1: Cyber Security Incidents Reported to the Cyber999 Help Centre in 2010. Total reports received was 8,090 incidents.

Operation's Review

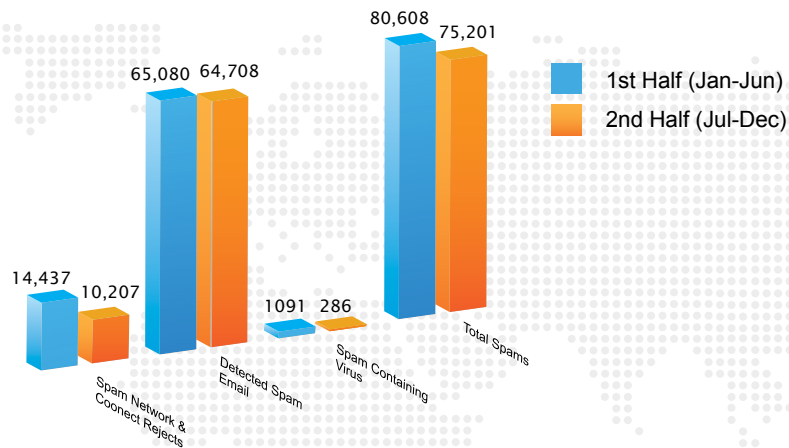


Figure 2: Early Warning System & Honeynet Data. Total spams detected in 2010: 155, 809.

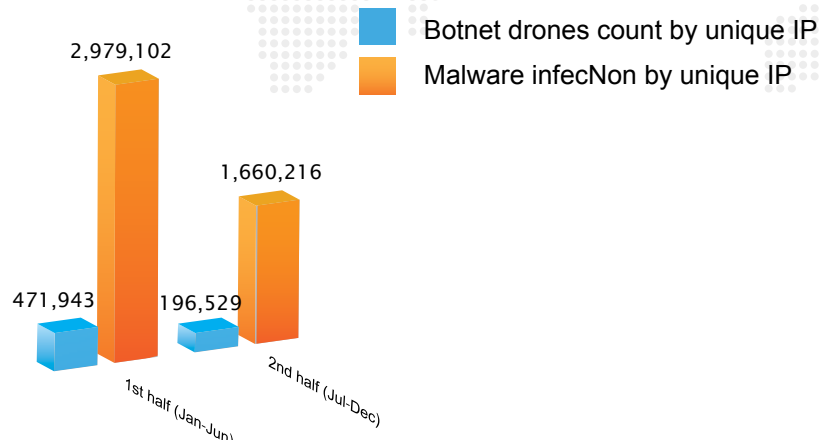


Figure 3: Cyber Early Warning System & Honeynet Data. Total Botnet drones & malware infection for 2010: 5,307,790

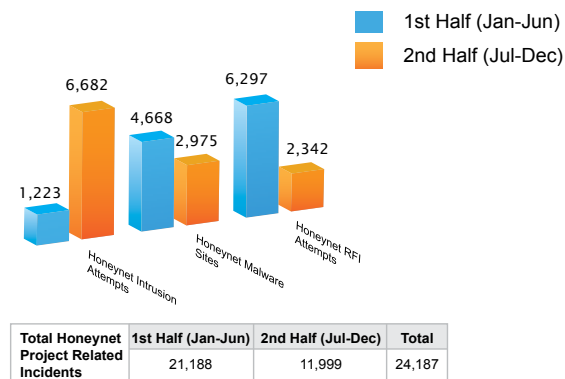


Figure 4: Cyber Early Warning System & Honeynet Data. Total Honeynet Project-related Incidents: 24, 187



1.2 Digital Forensics and Cyber CSI

The Digital Forensics Department (DFD) of CyberSecurity Malaysia has been providing digital forensics services to Law Enforcement Agency (LEA) and Regulatory Bodies (RBs) since 2005. As the vision of DFD in the Tenth Malaysia Plan is to continually become the National Centre of Reference and Excellence in Digital Forensics, DFD strived to offer a service of high quality that continually meets the international standard which is the American Society of Crime Lab Directors/LAB (ASCLD/LAB) Standard to the stakeholders. The team, nonetheless, is dedicated to promote excellence in forensics science through continuous research and innovation.

Year 2010 has shown a tremendous increase in the number of digital-related crimes handled by DFD. It is indeed another challenging year for DFD, with the explosion of digital technologies available on the market nowadays, DFD needs to continuously enhance its know-how and capabilities to match the forthcoming challenges such as cloud computing, iPad, disk-less computer, and others, which will keep DFD on its toes in the future.

As the vision of CyberSecurity Malaysia is to increase the number of cyber security professionals and to build national capacity in information security, DFD is actively and continuously involved in the provision of training to locals, contributing knowledge to LEAs and RBs, and sharing of experience in local and international events.

Some of the talks and seminars participated by DFD in 2010 include programme conducted at National Institute of Public Administration, Maritime Institute of Malaysia, Royal Malaysian Police Johore, Malaysia Cooperative Commission, Judicial and Legal Training Institute, Attorney General's Chamber of Malaysia and Japan Police Department.

DFD is also committed to Research & Development (R&D). The focus of our R&D activities last year was on biometric forensics. 2010 has shown an increase on CCTV cases related to biometric comparison, thus more R&D need to be conducted in this area providing valuable knowledge for DFD to solve crimes effectively and efficiently.

Operation's Review

The objective of our R&D program is to create awareness and improvement in digital forensics investigation and as such several MoUs were initiated with local Institutes of Higher Learning (IPTA and IPTS) to increase the dissemination of this valuable knowledge to the target group. One example was the collaboration with Universiti Teknologi Malaysia. We also assisted other varsities and colleges such as UiTM, UUM, UTM, UKM, UIA, and UTP with the development of their course module, part-time lecturing, student internship programmes and supervising research programmes at postgraduate level. This genuine endeavor is done in our effort to nurture more graduates in digital forensics expertise. To-date we were informed by the IPTA & IPTS that our program has shown positive result and is fruitful in which more students have enrolled in digital forensics related courses.

2010 is also a triumphal year for DFD, through the successful organisation of two major seminars during the CSM-ACE 2010 (<http://www.csm-ace.my/>) held at Kuala Lumpur Convention Centre (KLCC) on 25-29 October 2010. The first seminar conducted was on 'Digital Forensics Closed Session Seminar for Law Enforcement Agencies and Regulatory Bodies' and the second seminar conducted was on 'Digital Forensics Satellite Event for Researchers & Academicians'.

DFD actively conducts professional trainings to LEAs and RBs in order to develop digital forensics capabilities within our country. Among the training programs conducted was the Certified Fraud Examiner (CFE) training under the Central Bank of Malaysia (Bank Negara Malaysia) and for the Royal Malaysian Customs Academy.

In addition, under the initiative of knowledge sharing, DFD continuously participates in talks and lectures invitation to all interested parties from the government, non-profit organizations and private sectors.

2010 has been a great starting year for the Tenth Malaysia Plan for DFD. The same vision from the Ninth Malaysia Plan will be carried onto the Tenth Malaysia Plan in order to sustain its noble intention. This coming year, 2011, DFD will put more focus on building the nation's capacity and capability in digital forensics. Last but not least, DFD will continue to serve and strive to deliver the best digital forensics services.

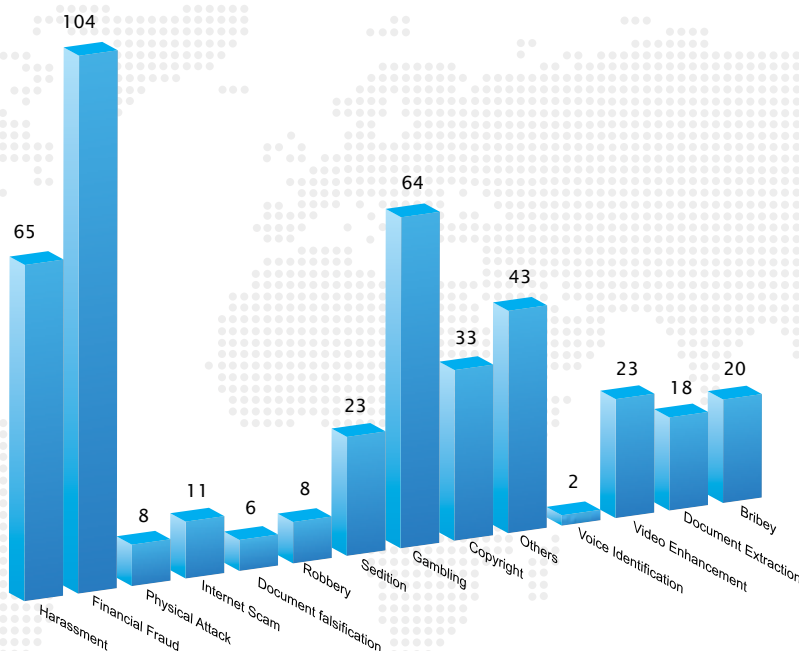


Figure 5: Digital Forensics Statistic for 2010

As shown in the Chart above, criminal activities involving financial fraud topped the list for year 2010 with 104 cases reported to DFD. Case studies indicates that the highest number of financial fraud cases was contributed by fraud relating to multi level marketing and unlicensed direct selling.

The second and third highest categories were harassment and gambling which recorded 65 and 64 cases respectively. Harassment cases include sedition and sexual stalking. Gambling cases that were mostly committed within the premise of cyber cafés, drastically increased from only 2 cases in 2009 to 64 cases in 2010.

Other cases; such as castigation and murder, takes fourth place with 43 cases being reported to DFD. The fifth place in the chart is Copyright, with cases reported as many as 33.

Bribery is a new category introduced in 2010, and recorded a total of 20 cases referred to DFD. For Physical Attack, Robbery, Document Falsification and Voice Identification, the cases recorded were the lowest compared to other cases. Cases involving document falsification, such as forgery of passport, has shown a decreasing number compared to last year. In 2009, a total number of 24 cases were recorded.

Operation's Review



1.3 Security Management & Best

CyberSecurity Malaysia is at the forefront in its efforts to promote, encourage and support the implementation of Security Management and Best Practices (SMBP) in information security among the public and private organisations in the country. In particular, CyberSecurity Malaysia is working to extend security management and best practices to CNII agencies in line with the cabinet directive for critical organisations to be certified within three years.

CyberSecurity Malaysia has taken a step forward to become an ISMS Certification Body by 2011. SMBP has taken a lead towards this initiative by establishing ISMS Certification Pilot programme for selected CNII agencies.

To ensure the readiness of the organisation to provide critical services to stakeholders, the SMBP Department consistently enhances its Business Continuity programmes. It also played a significant role in the third annual National Cyber Drill - codenamed X-MAYA3 - a simulated and coordinated exercise to assess the cyber security emergency readiness of Malaysia's CNII against cyber attacks.

As part of its responsibilities, the department consistently develops guidelines and best practices for use by external organisations and internet users. These guidelines serve to offer guidance on dealing with the increasingly challenging security issues faced by the cyber community. In addition, quarterly information security bulletin, known as eSecurity bulletin, has reached out to significant audiences in promoting information security awareness.

Publication of the guidelines, best practices and eSecurity bulletin has achieved its intended objective to promote information security awareness to the target group.

As eSecurity bulletin is also available online at CyberSecurity Malaysia's websites, many have benefited from the knowledge and experience shared by our experts. Often, positive remarks have passed to CyberSecurity Malaysia from local industries and even overseas associations.

CyberSecurity Malaysia also contributes to the development of standards in information security and business continuity management for both local and international bodies. The organisation co-produced an ISO project i.e. ISO/IEC 27037: Guideline for Identification, Collection/Acquisition and Preservation of Digital Evidence presented at the SC27 Working Group meeting in Berlin, Germany in October 2010. Its subsequent approval represented a significant achievement and recognition of CyberSecurity Malaysia in ISO standards development. CyberSecurity Malaysia is currently working on the committee draft 1 document which is expected to be published as an ISO standard in June 2012.

As part of its ongoing activities for continuous improvement in the implementation of ISMS as well as in maintaining the ISO/IEC 27001:2005 ISMS certification, several activities (i.e. risk assessment exercises, management reviews, quarterly ISMS awareness workshops & ISMS online assessments, internal ISMS audit and ISMS Treasure Hunt) were organized by SMBP in 2010.

As an active participant, SMBP has been appointed as the secretariat of the National Cyber Drill (X-Maya 3) jointly organized by the National Security Council (NSC) and CyberSecurity Malaysia. A total of 34 agencies from 9 CNII sectors took part in X-Maya3. The exercise involved incident handling activities such as malware analysis, information leakage and targeted attack.

SMBP also actively participated in international forum:

- A member of SMBP staff was selected to present her paper on "Cyber attacks: A threat to business and national resilience" at the BCM World Conference and Exhibition on November 2010. From there, the article bearing the same title was published in Continuity Magazine UK.
- A member of SMBP staff is the secretary for Regional Asia Information Security Exchange (RAISE) forum, a platform for Asian standardization community to exchange ideas and dialogues on information security standards and challenges. In the same forum, the SMBP staff member presented a paper on "Raising Critical National Information Infrastructure Organizational Resiliency through ISMS Certification".

In 2010, three SMBP personnel achieved certification of ISMS Lead Auditor from BSI. One personnel achieved Associate Business Continuity Professional from DRI Malaysia. SMBP was also recognised internationally when one of its employees received the (ISC)² Information Security Leadership Achievement (ISLA) Award 2010 from the International Information Systems Security Certification Consortium, Inc. (ISC)².

After months of preparation by SMBP and commitment from all departments and members of CyberSecurity Malaysia's management team, CyberSecurity Malaysia has successfully maintained the ISO/IEC 27001:2005 ISMS certification in 2010.

SMBP looks forward to the challenges in 2011 and beyond. With the support of other departments in CyberSecurity Malaysia, SMBP will continue to position itself at the forefront of ISMS and BCM implementation and increase the level of awareness in information security through the issuance of guidelines, best practices and eSecurity bulletin.

Operation's Review



1.4 Security Assurance

The Security Assurance Department (SA), under the Cyber Security Proactive Services Division of CyberSecurity Malaysia, is entrusted to provide national information assurance services in the areas of ICT products, critical systems and technologies.

In today's computing environment, trust has become the buzzword. A system is trusted when it behaves as expected. Absolute security condition is something that is very difficult to achieve. However, one can achieve a certain level of assurance that the system is trustworthy. In this age of digital uncertainty, information assurance demands organisational capability to protect their information system. Organization must be able to identify, detect and response to the threats, vulnerabilities and risks from cyber attacks.

Thus, the Security Assurance Department (SA) is entrusted to provide proactive measures in protecting information systems. SA has assembled a team of experienced and dedicated analysts with a combination of experience in vulnerability assessments, penetration testing, cyber security training and project management.

In 2010, SA delivers ICT security services via two units, namely, Malaysia ICT Security Evaluation Facility (MySEF) and the National Vulnerability Assessment Centre (MyVAC).

1.4.1 CyberSecurity Malaysia's Malaysian Security Evaluation Facility (CSM)

CyberSecurity Malaysia's Malaysian Security Evaluation Facility (CSM MySEF), under the Security Assurance Department is a test laboratory that carries out product security evaluation or testing based on Common Criteria (CC) international standard and product security assessment. Common Criteria (CC) and Common Methodology for Information Technology Security Evaluation (based on ISO/IEC 15408 and ISO/IEC 18045 respectively) are the recognized standards that are widely used for independent security evaluation in ICT products. In simple words, CC is the standard that can be used as a guideline for ICT product developers in ensuring the security features of their product are properly defined, developed and tested.

Services offered by CSM MySEF are:

Product Security Evaluation

CSM MySEF conducts testing on ICT product of various fields which include but not limited to networking, operating system, web application and smart card related products. In cases where special equipments are required, CSM MySEF may collaborate with other organizations having suitable equipments to facilitate the evaluation. Product evaluation in CC covers security testing on the security features of a product and reviewing product documentation to ensure its technical content is correct. Additionally, CSM MySEF also offers Protection Profile (PP) evaluation.

Product Security Assessment

CSM MySEF conducts product security assessment on ICT products which includes but not limited to smart card contactless hardware and smart card IC (integrated circuits). The assessment is based on best practices and by adapting several CC methodologies.

Protection Profile (PP) development

CSM MySEF develops Protection Profile (PP) for government agencies such as Jabatan Pendaftaran Negara (JPN) in addressing security requirements for products such as smart card readers.

International laboratory accreditation is important to ensure the quality of evaluation service delivered by a laboratory reaches or exceeds a certain standard. Thus, CSM MySEF went for MS ISO/IEC 17025 certification. By obtaining MS ISO/IEC 17025 certification, the test laboratory is competent to carry out tests which include testing and calibration using standard methods, non-standard methods and laboratory-developed methods.

To date, CSM MySEF has conducted 19 EAL1 - EAL4 evaluation projects in which 16 of them were under the Malaysian 2nd Economic Stimulus Package (ESP2) Financial Assistance Programme.

The FAP programme provides a form of financial assistance to the product developer for their product to obtain CC evaluation and certification. The ICT products that have been evaluated or are currently undergoing evaluation process include the following:

- Firewall
- Access Control Application
- Smart card operating system (OS)
- Digital Certificate Management System
- Log Management System
- 2D Barcode scanner and verifier system
- Video Surveillance Service Web and Mobile Application
- Data protection software for USB token and hard disk
- Biometric system
- Terminal Line Encryption software
- Tax agent e-Filing software
- Access Control Client Agent for Windows
- Various Web Applications

Operation's Review

The ESP2 projects were in partnership with local and international security consultants with the aim to boost the ICT security industry and to strengthen the relationship between CyberSecurity Malaysia and the consultants. The consultants are Secure-IP Sdn Bhd, Firmus Security Sdn Bhd, TekniMuda (M) Sdn Bhd, Your Creative Solutions (Netherland) and Laggui & Associates Inc (Philippines).

Adding to its function, CSM MySEF has also been appointed by the National Registration Department as their advisor for IT security. CSM MySEF became the technical advisor for smart card acceptance device (CAD) functional and security assessment in 2010. Several Memorandum of Understandings (MOUs) have been established with our local partners such as MIMOS Berhad, MCS Microsystem Sdn Bhd, stratsec.net Sdn Bhd and Malaysia Microelectronic Solutions Sdn. Bhd in conducting product security evaluation, testing and assessment.

CSM MySEF personnel are highly skilled and competent in various fields of ICT technology and security which include networking, operating system, smart card technologies, web application, Public Key Infrastructure, IT auditing and penetration testing. CSM MySEF personnel are certified with various international certifications such as CISSP, GCUX, GSEC, GPEN, GSNA and CEH.

The CSM (MySEF) was established under CyberSecurity Malaysia to execute Common Criteria evaluation and certification process. This initiative should be supported and promoted as one of the efforts to secure our information security environment. With this initiative, Malaysian ICT products can now gain local and international recognition.

1.4.2 Malaysia Vulnerability Assessment Center (MyVAC)

Malaysia Vulnerability Assessment Center or MyVAC provides on-site and off-site cyber security services for relevant Critical National Information Infrastructures (CNII) sectors.

For on-site services, MyVAC reviews the relevant CNII's Audit Report and acknowledges additional cyber security recommendations. The two (2) types of on-site services provided are as follows:

1. Vulnerability Assessment at the client's place. MyVAC uses the defense-in-depth approach to ensure the technical controls are taken care of.
2. Review client's existing VA report and provide our expert advice.

For off-site services, MyVAC provides relevant cyber security assessment report by conducting simulation assessment of current settings/configurations with relevant CNII sectors. The service provides external and internal penetration testing in verifying the vulnerabilities for clients' network and systems via internet.

In 2009 and 2010, the Vulnerability Assessment Services (VAS) was developed under the "Security Evaluation and Certification on ICT Products and Testing of Critical Security System", of the 2nd Economic Stimulus Package (ESP2). It is a collaborative project between The Chief Government Security Office (CGSO) and Malaysia Administration Modernisation and Management Planning Unit (MAMPU). This programme provides a form of financial assistance to 30 selected CNII sectors, including the Government Ministries, Agencies and Targeted Critical sectors to conduct vulnerability assessment of their corporate network and system.

This programme also include partnering with local security consultants with the aim to boost the ICT security industry and to strengthen the relationship between CyberSecurity Malaysia and these consultants. 15 security consultants were selected for this project i.e Diaspora Sdn Bhd, Intranium Sdn Bhd, Firmus Security Sdn Bhd, PriceWaterhouseCoopers, Extol MSC Sdn Bhd, KPMG Malaysia, BDO Consulting Sdn Bhd, iTania Sdn Bhd, I-Protocol Sdn Bhd, Janasys Sdn Bhd, Scan Associates Bhd, Intellimicro (M) Sdn Bhd, Tri-IT Sdn Bhd, Time Engineering Bhd and Millenium Radius Sdn Bhd.

MyVAC has successfully conducted vulnerability assessment services to 30 clients namely Ministry of Science, Technology & Innovation (MOSTI), Department of Immigration Malaysia, National Registration Department (JPN), Ministry of Internal Affairs (KDN), Parliament of Malaysia, Ministry of Health (MOH), Inland Revenue Board of Malaysia (LHDN), Malaysia Airport Technologies Sdn Bhd, Westports Malaysia, Tenaga Nasional Berhad, Petronas Penapisan Melaka Sdn Bhd and many more.

MyVAC also offers expert advice and review of client's existing vulnerability assessment report. Internal and external penetration testing are also conducted to verify the findings.

Other than VAS, MyVAC also conducts Control System Security Assessment (CSSA) services to Petronas Penapisan Melaka Sdn Bhd, partnering with security expert. This service focused to assess only on the System Control And Data Acquisition (SCADA)/Digital Control System (DCS).

Since MyVAC is given a mandate to conduct VAS project, MyVAC has initiated two (2) VAS Workshop for security consultants and for VAS clients. A total of 15 security consultants and 17 CNII sectors took part in the workshops and learnt on how to conduct the VAS and how to secure their ICT infrastructures/areas.

MyVAC has also successfully organized Vulnerability Assessment and Penetration Testing (VAPT) Training on Oct 2010 and Nov 2010 to all 30 clients that participated in ESP2 VAS project. The training provides both the theory and practical knowledge in conducting assessment and ways to rectify security vulnerabilities. Among the modules in VAPT including:

- Introduction to Information Security
- Server & Desktop Security Assessment
- Network & Wireless Security Assessment
- Web Application & Database Security Assessment
- Penetration Testing
- ICT Security Policy Review

In 2010, three of MyVAC staff obtained certification from the prestigious SANS (SysAdmin, Audit, Network, Security) Institute whereas nine of the staff obtained Certified Ethical Hacker (CEH) certification from EC-Council.

The vulnerability assessment exercise conducted to 30 clients has provided fruitful and beneficial insights on the health and condition of the country's critical organizations. It was an accomplished project that must be continued in mitigating the risks of cyber attacks. It also shows the security landscape and the readiness of CNIIs in implementing security controls in their critical infrastructure.

It was also found that the collaboration between the government and ICT security industry provides a healthy platform for industry growth. Through this collaboration, CNIIs were able to recognize and identify potential consultants for future security audits. It is imperative that the ICT infrastructure be periodically reviewed, and these consultants will be able to provide the security analysis to ensure the healthy infrastructure for the whole CNIIs.

Furthermore, the experience gained through VAS program shows that our local security consultants have the capabilities equal to international standards. Through similar projects such as VAS, these consultants can further improve their service delivery with guidance from CyberSecurity Malaysia.

In 2011, it is recommended that similar VAS projects and VAPT training to be continuously conducted for all CNIIs. This exercise provides a healthy platform for organizations to know the condition of their ICT infrastructure and minimize of known and unknown attacks.

In addition, MyVAC will establish the CSSA services since a number of the country's critical organization has and uses SCADA in managing their critical production system. Among the potential

Operation's Review

clients and CNILs that can greatly benefit from control systems security assessments are Oil and Gas Sector, Electricity Sector, Water Sector and Media and Communication Sector.

Apart from that, MyVAC was appointed by the *Jawatankuasa Pusat Sasaran Penting* (JPSP) to be the permanent Supervisory Team member in March 2011. The aim is to conduct cyber security assessment for *Tim Naziran Sasaran Penting* (TNSP) together with CGSO and TNSP members.

MyVAC also will develop Malaysia Trustmark as our new services in 2011 and above. Trustmark is a program that allows business that meet high standards to display a seal on e-commerce web sites. The objective of Malaysia Trustmark service is to raise confidence and trustworthiness of e-commerce in Malaysia and across borders by promoting safe electronic commerce environment.



1.5 Malaysian Common Criteria Certification Body

The Malaysian Common Criteria Certification Body (MyCB) was established in 2008 with the purpose of evaluating and certifying local ICT products and systems that meet the standards of ISO/IEC 15408 or known as Common Criteria. MyCB's formation as a certification body under CyberSecurity Malaysia was done in tandem with the nation's acceptance as a consuming member of the Common Criteria Recognition Arrangement (CCRA), an international standard for gaining recognition and assurance in ICT security.

In year 2010, MyCB has successfully completed the activities as stated below.

■ MyCC Financial Assistance

In 2009 – 2010, MyCB focused its activities on promoting the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme services through the provision of financial assistance, under the 2nd Economic Stimulus Package Fund, offered to local developers. More than 100 local companies applied for the financial assistance, however only 30 companies were selected because their products and systems have suitable security functions to be evaluated and certified under the MyCC Scheme. The process of evaluating and certifying the products and systems is on-going until Q2 2011.

We have also participated in seminars conducted at three different locations, as speakers, in order to promote the MyCC Financial Assistance:

1. 5th May 2010 at PTTC Ipoh, Perak.
2. 6th May 2010 at Vistana Hotel, Penang.
3. 1st July 2010 at Cititel Hotel, Penang

Operation's Review

■ **New Commercial License Malaysian Security Evaluation Facility (MySEF)**

Stratsec.net, an Australian based company has opened its branch in Malaysia and is known as stratsec.net Sdn Bhd. They have successfully been granted a license under the MyCC Scheme to operate as a Malaysian Security Evaluation Facility (MySEF).

■ **CCRA Authorising Participant – Shadow Certification Assessment**

Malaysia through CyberSecurity Malaysia, has been accepted as the Certificate Consuming Participant on 28 March 2007. To be recognised as a Certificate Authorising Participant, a national scheme and its components need to be established and assessed by CCRA. The MyCC Scheme application in March 2010, to become a Certificate Authorising Participant has been accepted by CCRA. The assessment of MyCC Scheme was conducted by CCRA from 29 November until 3 December 2010 before they finally recognised Malaysia as a CCRA Authorising Participant. It is expected that the formal result will be announced in 2011.

■ **Other commitments**

In 2010, MyCB had successfully hosted the CC Knowledge Sharing and 2nd Asian Information Security Evaluation and Certification (AISEC) meeting at Kuala Lumpur from 22 until 23 July 2010. The purpose of this event is to share experiences and knowledge in IT security evaluation and certification in Asian countries. Besides local agencies, academicians and industries, it is also participated by labs and Certification Bodies from Japan, Korea, India and Taiwan.

During the year, MyCB personnel participated in several international forums and meetings, both to represent Malaysia and to gain exposure in this critical field. Among the events were the Annual International Common Criteria Conference (ICCC) and Common Criteria Recognition Arrangement (CCRA) working groups meeting in Berlin and Turkey. At these events, MyCB provided the international community on the latest development and establishment of the MyCC Scheme and its various initiatives moving forward, including the following:

1. Successfully promoted the MyCC Scheme through MyCC Financial Assistance program
2. Successfully promoted the growth of security evaluation industry in Malaysia through the security evaluation consultancy services and evaluation facility provided for the industry.
3. Recognition as CCRA Authorising Participant for Malaysia. We are only one step away (waiting for approval). With this status, ICT products and systems certified by MyCC Scheme will be recognised in the global market.

For 2011, the rebranding for the department in accordance with its functions as an Information Security Certification Body (ISCB) and the extension of new services including certification will be carried out and completed accordingly. The new services provided will be:

- Information Security Management System (CSM27001) Scheme services.
- Malaysia Trustmark for Private Sectors (MTPS) Scheme services.



1.6 Cyber Security Research and Policy

In 2010, the Cyber Security Research and Policy Division was structured through the integration of the Strategic Policy Research Department, Cyber Media Research Department, and the Policy Implementation Coordination Department.

Beginning January 2011, the Cyber Security Research and Policy division has been renamed as the Multilateral and Government Engagement Division, and the three departments have been reshuffled to form only two key departments namely, Multilateral Engagement Department and Government Engagement Department. The Strategic Policy Research Department has been absorbed to the newly created Research Division.

The following are the review of the Strategic Policy Research Department, Cyber Media Research Department, and the Policy Implementation Coordination Department.

1.6.1 Strategic Policy Research

The core function of the Strategic Policy Research (SPR) Department is to develop cyber security strategic papers - such as research papers, proposals and reports. These documents provide the necessary information to the management and the stakeholders to make well-informed decisions

SPR provides strategic advices and feedbacks to the stakeholders and spearheads new cyber security initiatives. These include collaborations with relevant local and international parties, and implementation of cyber security technologies.

In doing the Cyber Security Research and Development, focus are given in the following areas:

- Cyber Security Acculturation and Outreach;
- Digital Forensics;
- Cyber incident management and mitigation; and
- Information Security Management System (ISMS)

Operation's Review

This has resulted in papers and articles presented and published for local and international platform such as:

No	Paper	Location
1	Malaysia's Approach in Cyber Security	Cyber Security Conference Steven's Institute, Washington DC,
2	Malaysia's Initiatives in Cyber Security	Orlando, Florida
3	Challenges In Ensuring a Safe and Secure Cyber Environment- Malaysia's Perspective	Bandung, Indonesia
4	Cyber Security Regional Collaboration	Singapore
5	Tri-Border Conference - Terrorist Use of Internet	Philippine
6	CENS-GFF (Centre of Excellence for National Security - Global Future Forum)	Singapore
7	Council for Security Operation in Asia Pacific Study Group Meeting	Danang, Vietnam

With regards to journal and articles, some of them are

No	Paper	Published
1	Challenges In Ensuring A Safe Secure Cyber Environment – Malaysia Perspectives	The 6th e-Indonesian Initiatives Journal on 5-7 April 2010
2	Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework	IEEE Xplore Digital Library ISBN 978-1-4244-7408-0, IEEE 2010
3	Protection of Critical National Information Infrastructure (CNII) against Cyber Terrorism: Development of Strategy and Policy Framework	IEEE Xplore Digital Library ISBN 978-1-4244-6446-3, IEEE 2010 ISI 2010, 23 – 26 May 2010, Vancouver, BC, Canada

In addition to papers and articles, in 2010, SPR is involved in international discussion platforms such as:

- Centre of Excellence for National Security - Global Future Forum) (CENS-GFF) held in Singapore,
- Council for Security Operation in Asia Pacific Study Group Meeting Danang, Vietnam

Major events involving the SPR in 2010 are:

■ Council for Security Cooperation in the Asia Pacific (CSCAP)

CSCAP's Study Groups and Experts Groups are the primary mechanism for CSCAP activity. These groups serve as a region-wide multilateral forum for consensus building and problem solving and often address specific issues and problems that are too sensitive for official dialogue. Through these Study Groups CSCAP conduct research and analyses data that will support and complement the efforts of regional governments and official multilateral dialogue mechanisms, such as the ASEAN Regional Forum (ARF), which routinely brings together senior foreign ministry and defense officials from around the Asia-Pacific region to discuss regional security issues and concerns.

For this study group, Cyber Security Malaysia's role is at the centre of the strategy to secure the cyber environment within the Asia Pacific region and Malaysia. Australia, India and Singapore have been appointed as the group co-chair.

The report derived from the study group will serve as the basis for the preparation of a draft for the CSCAP Memorandum to be submitted to the CSCAP Steering Committee for further consideration. The Memorandum will briefly highlight the possible scenario of a cyber threat in the Asia Pacific region, the probable security risks, and the proposal for a cybersecurity strategy to be considered by the ASEAN Regional Forum (ARF).

■ **Cyber War Forum 2010**

The forum is jointly organized by CyberSecurity Malaysia and the National Security Council. The forum aimed to examine cyber war as the trend of future conflict, its concept and associated attributes. There are 5 papers presented during the forum with a total number of 74 participants. The successful event started with the forum and ended with a roundtable discussion where all inputs from relevant government agencies were crafted and submitted in a proposal paper to the National Security Council.

■ **OIC-CERT**

The Organisation of the Islamic Conference - Computer Emergency Response Team (OIC-CERT) is a platform for member countries to explore and to develop collaborative initiatives and possible partnerships in matters pertaining to cyber security. The objective of these initiatives is to strengthen self reliant in cyber space. Currently the OIC-CERT consists of 20 teams from 18 member countries

List of MoU under OIC-CERT initiatives:

1. MoU with Ministry of Industry, Trade and New Technologies - Morocco
2. MoU with E-Worldwide Group
3. MoU with The United Emirates Computer Emergency Response

List of OIC-CERT Events:

1. The OIC-CERT Annual Conference & Annual General Meeting 2010
Venue : Kuala Lumpur Malaysia
Date : 29-30 October 2010
2. OIC-CERT Regional Workshop, Middle East
Host Country : Egypt
Date : 8-10 June 2010
3. OIC-CERT Regional Workshop, Africa
Host Country : Morocco
Date : 24-25 June 2010
4. OIC-CERT Regional Workshop, Asia
Host Country : Malaysia
Date : 28 - 29 October 2010

Operation's Review

1.6.2 Cyber Media Research

Cyber Media Research (CMR) Department's primary aim is to keep the stakeholders informed on the state of cyber security within the country to enable them to make informed policy decision in order to secure the nation's cyber space. CMR is responsible to prepare the necessary ministerial papers and reports pertaining to the development and issues regarding cyber security especially with regards to the cyber media.

In year 2010, CMR focused on the following activities:

- **Cyber Media Research and Analysis**

Provided strategic reports to our stakeholders on the state of cyber security in Malaysia. Among the reports provided are monthly reports to the Cabinet on cyber security incidents and special reports on specific cyber security issues to the Ministry of Science, Technology and Innovation and the National Security Council. CMR also provide responses to parliamentary questions, from both the Dewan Rakyat and Dewan Negara.

- **Collaboration with Law Enforcement Agencies in Mitigating Cyber Security Issues**

CMR served as the secretariat to a national committee on cyber security. To facilitate communications among members of this committee, CMR has successfully developed a secured portal as a platform for online forum to discuss issues and facilitate information sharing.

1.6.3 Policy Implimentation Coordination

The **Policy Implementation Coordination (PIC) Department** is dedicated to support the government in the implementation of the National Cyber Security Policy (NCSP) towards achieving its vision.

The NCSP vision is that "Malaysia's Critical National Information Infrastructure (CNII) shall be secured, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well-being and wealth creation".

To realize this vision, a National Cyber Security Coordination Committee (NC3) was formed with members from various ministries and agencies that oversee the operation of the CNII. PIC acts as the secretariat for this committee along with the Ministry of Science, Technology and Innovation (MOSTI).

For the year 2010, PIC successfully conducted the activities as listed below.

1. National Cyber Security Policy (NCSP) Implementation & Coordination

- As part of the preparation towards the NC3 No.1/2010 meeting, PIC conducted meetings with Thrust Drivers to discuss the way forward for each action plan.
 - Meeting with Kementerian Penerangan Komunikasi & Kebudayaan (KPKK); 7 Jan 2010
 - Meeting with Majlis Keselamatan Negara (MKN); 10 Feb 2010
 - Meeting with MOSTI; 11 Feb 2010
 - Meeting with Kementerian Penerangan Komunikasi & Kebudayaan (KPKK); 3 March 2010
 - Meeting with Kementerian Penerangan Komunikasi & Kebudayaan (KPKK); 16 March 2010

- A National Cyber Security Coordination Committee (NC3) Meeting No. 1/2010 was held on 24 March 2010, chaired by the Deputy Secretary General (Science) of MOSTI.
- Handover of the NCSP stewardship from MOSTI to MKN; 17 August 2010.

2. Risk Assessment Framework Study

Together with KPKK, PIC organised the preparation of Risk Assessment Framework and conducts the 2009 Risk Assessment Exercise. The 2009 Risk Assessment Report and outcome of the study were presented at the NC3 No. 1/2010 Meeting, 24 March 2010.

3. MS ISO/IEC 27001:2007 Information Security Management System (ISMS) Implementation

- The Jemaah Menteri has decided on 24 February 2010, through their Memorandum, that the Critical National Information Infrastructure (CNII) entities in Malaysia are to be MS ISO/IEC 27001:2007 Information Security Management System (ISMS) certified within 3 years from this date. The implementation of ISMS certification is to be coordinated by the ministries and regulatory agencies in charge of the National CNII and they have to make sure that CNIIs under their purview are to be ISMS certified within 3 years.
- A masterplan for the implementation of the above directive was presented and accepted at the NC3 1/2010 meeting, which comprises of three phases, i.e. (1) Develop the Momentum & Awareness, (2) Implementation & Monitoring, and (3) Initial Certification.
- Subsequently, PIC has been entasked with the role to spearhead a series of first phase activities (Develop the Momentum & Awareness) as below:
 - Prepared the "Guideline on Implementation of ISMS for Governing Agencies"
 - ISMS Workshop for Central Agency / Ministry / Regulator of Critical National Information Infrastructure (CNII) Sector; 26 April 2010.
 - ISMS Implementation Awareness Sessions for Water Sector, organized by National Water Services Commission and CyberSecurity Malaysia; 17 May 2010
 - ISMS Implementation Awareness Sessions for Food & Agriculture Sector, organized by Ministry of Agriculture and Agro-based Industry; 17 May 2010
 - ISMS Implementation Awareness Sessions & Workshop for Transportation Sector; organized by Ministry of Transport; 1 July 2010
 - ISMS Implementation Awareness Sessions for Agency under purview of Energy Commission; organized by Energy Commission; 19 August 2010.
- In collaboration with the Chief Government Security Office (CGSO) Prime Minister's Department, PIC (together with SMBP, I&C and SA) organized several Dialogue Sessions on Malaysia Key Point's Security & Protection Management and ISMS Implementation Awareness/Workshop. The workshop targeted key points' owners and operators. The dialogue session and ISMS workshops held are as below:
 - Central Zone – Federal Territory of Kuala Lumpur & State of Selangor; at PWTC; 9 Feb 2010
 - Federal Territory of Labuan & State of Sabah; at Kota Kinabalu; 11 May 2010
 - State of Sarawak, at Kuching; 9 August 2010
 - National Level, in Kuala Lumpur ; 28 Oct 2010 (in conjunction with CSM-ACE)
 - Mesyuarat Meja Bulat Ketua Pegawai Eksekutif Sasaran Penting, Kuala Lumpur; 28 Oct 2010 (in conjunction with CSM-ACE)

Operation's Review



1.7 Outreach

Outreach Department was entrusted with the huge responsibility of spreading awareness on internet safety to the general public. Through collaborations with selected parties, sponsors and organizations, the Outreach Department conducted exhibitions, talks, seminars, trainings and various other programs around Malaysia to help strengthen the ties between CyberSecurity Malaysia and the general public.

From the launching of our “CyberSAFE in Schools Program” to our Ambassador Program, the Outreach Department aims to continuously spread awareness on internet safety, educate and assist the public in understanding their roles and responsibilities when surfing the internet, and to ensure that the public’s online experience is a safe and enjoyable one.

Like any other security issues in Malaysia, cyber security issues are considered very crucial and important. According to the statistics of cybersecurity incidents reported to the Cyber999 Help Centre of CyberSecurity Malaysia, incidents of cyber crime in Malaysia jumped by 127% in 2010 or equivalent to 8,090 cases compared to 3,564 cases in 2009. Action must be taken to stop these issues from escalating further but this would require not only government intervention but also support from the private sector and other organisations that can curb these issues from spreading. Therefore, the Outreach Department is very keen on inducing any organisations to work with CyberSecurity Malaysia in which they can leverage from their Corporate Social Responsibility (CSR) programmes. This strategic partnership will not only benefit the company and the government but the general public as well.

In 2010, CyberSecurity Malaysia through its Outreach Department established a strategic partnership with GiatMARA, Worldwide Group and Bubble Flip. The following is the list of programmes that CyberSecurity Malaysia, through its Outreach Department was able to leverage from this strategic

partnership:-

GiatMARA

- Participated in programmes which were organised by CyberSecurity Malaysia such as CSM-ACE 2010 and Safer Internet Day 2010.
- CyberSecurity Malaysia produced a cyber safety syllabus that will be used by GiatMARA as one of its subjects.

Worldwide Group

- CyberSecurity Malaysia produced a children online safety guideline for Organisations of the Islamic Conference (OIC) countries which will be used as reference for cyber security awareness.

Bubble Flip

- CyberSecurity Malaysia developed cyber safe content for the public.

In year 2010, we have successfully concluded the activities as listed below.

■ **Programme with Raja Muda Perlis in conjunction with the launching of CyberSAFE in School**

The launching of CyberSAFE Programme in conjunction with the visit of DYTM Raja Muda Perlis Tuanku Syed Faizuddin Putra Jamalullail to Kota Marudu, Sabah was successfully executed by the Outreach Department of Cybersecurity Malaysia.

The first programme launched was the “How to create a Blog” competition. The objective of the programme was to educate and create awareness amongst students to ensure that they can send their message and information safely across to other online users.

The second programme launched was the Digital Content Competition. This programme was designed with the purpose of enhancing and sharpening the skills of the students in ways that would be used to deliver awareness messages to their peers on threats that the cyber world pose.

The CyberSAFE Awareness talk was designed to provide exposure to the students regarding threats within the cyber world and educate them on the various channels that they can use to overcome these threats. Students were educated on the various services provided by Cybersecurity Malaysia, one of them being Cyber999.

The program was attended by over 100 students from Sekolah Menengah Kebangsaan Kota Marudu 2, Kota Marudu, Sabah and students from other schools nearby.

■ **CyberSAFE in Schools**

The *CyberSAFE in Schools* Program was officially launched by Deputy Prime Minister of Malaysia, YAB Tan Sri Muhyiddin Yassin, at Kota Marudu, Sabah on 24 September 2010. Making its way from Sekolah Menengah Kebangsaan Kota Marudu 2, Kota Marudu, Sabah, the *CyberSAFE in Schools* programme objective is to reach out to all over Malaysia, spreading awareness on the importance of being safe while surfing the Internet. As cyber crimes have been on the rise with new threats being detected daily, the need to create awareness on safe online engagement is essential for students who make up the majority of internet users in the country.

CyberSAFE in Schools aim to reach out to all Malaysian in 2011 by holding talks, exhibitions and other fun filled, learning programs for the students. By having more students being aware of the threats that the cyber world poses, it will help them to be safer online and at the same time, protects them from falling victim to the increasing number of cyber crime activities. With the knowledge that they will gain from the *CyberSAFE in School* program, they will be able to share that knowledge with the people around them and continue to advocate the awareness of internet safety. Together with the help from respected parties, *CyberSAFE in School* will be able to set the standard of internet safety and awareness amongst students in Malaysia.

Operation's Review

■ CyberSAFE Ambassador Programme

The idea of CyberSAFE Ambassador Programme is to encourage the general public to voluntarily participate and share their experience, expertise and knowledge in cyber security with others. The CyberSAFE Ambassadors are selected from amongst students, teachers and parents. The newly appointed ambassadors will first embark on an ambassador training session provided by CyberSecurity Malaysia in order to ensure the dissemination of accurate information pertaining to cyber security in an interactive way. As of December 2010, there are 475 new registered ambassadors and most of them have already participated in events organised by CyberSecurity Malaysia.

■ Cyber Security Malaysia Conference & Exhibition (CSM-ACE 2010)

CSM-ACE 2010 was held on 26-28 October 2010 at the Kuala Lumpur Convention Centre under the theme "Securing our Digital City". The CSM-ACE 2010 was opened to everyone interested in information technology and cyber security.

Various engaging and entertaining activities were conducted within the 3 days event such as the ambassador convention, Google-Fu workshop, Self Defence Challenge, forum and exhibition which attracted participations from 9 different schools and many organisations from the private and government sector.

■ Safer Internet Day 2010 (SID 2010)

Subsequent to the Outreach Department participation in the annual Safer Internet Forum at Luxembourg in 2009, CyberSecurity Malaysia has been appointed by INSAFE as the lead organisation for SID 2010 in Malaysia. The SID 2010 was held on 9 February 2010 at Putra World Trade Centre, Kuala Lumpur under the theme "Think before you post" and focuses on methods of managing images online and dealing with privacy in a digital environment.

■ Malaysia Innovative 2010

Malaysia Innovative is an annual program initiated by MOSTI and is co-organised by all government agencies under MOSTI. Outreach Department has leveraged its CyberSAFE Program throughout Malaysia in conjunction with Malaysia Innovative 2010 programme.

■ CyberSAFE Programme

CyberSAFE Programme acts as the umbrella program, for the Outreach Department. There are many sub-programs organised under CyberSAFE Programme which consist of *CyberSAFE in Schools*, *CyberSAFE Ambassador Program*, *CyberSAFE Awareness Talk* and *CyberSAFE On-line Presence*. Through these programs, Outreach Department has managed to deliver its message of cyber security to the public effectively and efficiently. For instance, in 2010, a stragerring number of 30,257 participants participated in these programs.

■ On-line Presence

In order to ensure information and message concerning cyber security is disseminated in an effective and interactive way to the targeted audience, Outreach Department has embarked on several initiatives to promote CyberSAFE on-line. CyberSAFE on-line presence consists of:-

■ CyberSAFE Portal

It is the first on-line presence for CyberSAFE programmes and was launched in August 2009. This internet safety awareness portal is dedicated to five categories of user group which consists of kids, youths, parents, adults and organisations. Each group can easily look up tips, guidelines, interactive quizzes and games depending on the type of information they are looking for from this portal.

- **CyberSAFE Facebook**

CyberSAFE Facebook is one of the online media used by the Outreach Department via an on-line presence to create friendly environment for interactive communication. From CyberSAFE Facebook, audience can get more info on current issues and cases faced by their friends by viewing videos, photos, updated post and through online chatting

- **CyberSAFE Youtube**

From the CyberSAFE Youtube page, the public can view and experience event engagement that CyberSecurity Malaysia conducted throughout the year. In order to encourage Malaysian to be more IT savvy, various digital content competitions like mini clip and short videos can also be leveraged from the CyberSAFE Youtube.

- **CyberSAFE Twitter**

CyberSAFE Twitter is a platform created by CyberSecurity Malaysia's Outreach Department to allow our followers to be aware of our activities and upcoming events close to real-time. Furthermore, it is also used to allow our followers to raise any questions or seek any advice pertaining to cyber security issues.

Below are the summaries of participants involved in CyberSAFE Programs 2010:-

Total	
No of Schools	54
No of Teachers	940
No of Students	11,913
No of Adults	17,404
No of Organisations	46
Total Participants	30,257

Below is the summary of CyberSAFE Programs in Schools (by region) in 2010:-

Central Region	Wilayah Persekutuan	7 schools
	Selangor	10 schools
	Negeri Sembilan	2 schools
Northern Region	Kedah	3 schools
	Perak	10 schools
Southern Region	Melaka	2 schools
	Johor	2 schools
East Coast Region	Pahang	3 schools
	Terengganu	1 school
Sabah & Sarawak	Sabah	10 schools
	Sarawak	4 schools

Operation's Review

In 2011, the Outreach Department plans to focus all effort on continuing the CyberSAFE Programme and target more participation from the general public and private organizations. We believe in order to continue educating the people and creating awareness pertaining to cyber security issues, there must be a comprehensive plan and continuous effort from all parties. Hence, below are the programs and activities that the Outreach Department will emphasize on:-

- CyberSAFE in Schools
- CyberSAFE Partner Engagement
- CyberSAFE On-line Presence
- CyberSAFE Public Program
- CyberSAFE Content
- CyberSAFE Roadshow



1.8 Information Security Professional Development

Information Security Professional Development (ISPD) spearheads CyberSecurity Malaysia's efforts to share knowledge and experience with industry experts to provide relevant training to other organizations.

ISPD introduced additional courses in 2010 to fulfill its commitment to produce more Information Security Professionals within our country in response to the rising trend in cyber threats. ISPD also initiated a Malaysian Information Security Professionals networking programme to enhance knowledge sharing among the professionals and acquire recognition within the professional community. In view of the need to nurture more Information Security Professional in Malaysia ISPD has also initiated a protem committee through the formation of Information Security Professional Association Malaysia (ISPA.My) which is currently awaiting the approval from the Registration of Society. Through the establishment of the association, Information Security Professionals will be able to update their knowledge, maintain CPE points and contribute knowledge and capability building to the public. In addition, ISPD is also able to attract a substantial number of law enforcement agencies from other countries such as the police agency from Saudi Arabia to send their staff to participate in courses conducted by CyberSecurity Malaysia.

As an organization entrusted to ensure the security of cyber space in Malaysia, our expertise and services are widely sought after to provide training on the development of the Computer Emergency Response Team (CERT), Information Security Management System (ISMS), Business Continuity Management (BCM), Wireless Technology, Penetration testing, SCADA and Digital Forensics.

ISPD has also seen an increase in the number of Information Security professionals from 924 in the year 2009 to 1704 in the year 2010.

Operation's Review

ISPD builds alliances with local and international organizations to extend cooperation and collaboration towards the development of Information Security Professionals in Malaysia. In 2010, ISPD exchanged a Memorandum of Understanding (MoUs) on training and education collaborations with the SANS Institute of United States and the British Standards Institute (BSI).

Through our collaboration with (ISC)2, ISPD has conducted 4 CISSP & 4 SSCP examinations, 2 CISSP and 1 SSCP Review Seminars respectively. These partnerships provide a platform for ISPD to organize workshops, conferences and preparation to obtain certification. Our partnership with SANS Institute has successfully nurtured another group of internationally certified security professionals while the certification programs from DRI International and British Standards Institution have effectively produced another 12% of local domain experts in the respective fields.

In addition to the above activities, CyberSecurity Malaysia also conducted specialized training programmes for Institut Latihan Kehakiman Dan Perundangan (ILKAP) on Digital Evidence Handling & Acceptance of Expert Witness testimony in Court, events organized by the Chief Government Security Office (CGSO) on Information Security Management, Bank Negara Malaysia's Certified Financial Investigator and the Saudi Arabia's enforcement agencies on Digital Forensic programs.

With the intense focus on capacity building for the nation and to extend its outreach internationally, ISPD has attracted the Saudi Arabia's Enforcement Agencies to participate in our Digital Forensic Training Programs in October 2010. At the same time, we have produced more competency training programs to cater for the increasing needs of security training.

ISPD looks forward to the challenges and interesting engagements in 2011 and beyond. With the support of other departments in CyberSecurity Malaysia, ISPD will continue to position itself at the forefront in its task to safeguard the nation from cyber security threats.



1.9 Northern Region Branch

Since its establishment in November 2009, CyberSecurity Malaysia's, Northern Region Branch (Northern Region) has been operating from Perak Techno-Trade Centre (PTTC), Meru Raya, Ipoh, Perak.

The Northern Region's primary aim is to promote the services offered by CyberSecurity Malaysia especially in the state of Perak and also in Northern Region states such as Penang, Kedah and Perlis.

Since its operations in Ipoh, Perak, we have been working together with the local organizations, private sectors, the government and also local universities. We have been conducting road shows to introduce and promote CyberSecurity Malaysia's services in Perak.

We also forge close working collaboration with the Perak State Government that leads to the signing of an MOU with the Perak State Government on 26th October, 2010 during CSM-ACE 2010 program that was held at the Kuala Lumpur Convention Centre. The MOU was signed by YB Dato' Seri Dr. Abdul Rahman b Hashim (State Secretary of Perak) representing the Perak State Government and CyberSecurity Malaysia, was represented by our CEO, YBhg. Lt Col Dato' Prof. Husin Jazri (Retired). This event was witnessed by the Chief Minister of Perak, YAB Dato' Seri Dr. Zambry Abdul Kadir. (See photo above)

Through the signing of the MOU, the Perak State Government and CyberSecurity Malaysia collaboratively agreed to ensure the materialization of several key matters such as:

- Pilot 'Securing Digital City' in Ipoh, Perak.
- Assist in Vulnerability Assessment Services (VAS), for Perak State Government .
- Assist in training the team for the Perak State Government's first-line emergency response.
- To improve knowledge on cyber security awareness in schools, organizations and the public
- To assist in increasing the number of information security professionals in Perak.

Operation's Review

For the year 2010, we have successfully completed and achieved the activities as stated below.

■ MyCC Financial Assistance

For the year 2010, the total number of products successfully registered under MyCC Financial Assistance program stood at 112 products.

Almost 50% from the total number of products have been successfully registered by us in the Northern Regional Office. The total number of products registered for MyCC Financial Assistance from Northern Regional Office stands at 47 products.

We conducted seminars in three locations in order to promote MyCC Financial Assistance:

1. 5th May 2010 at PTTC Ipoh, Perak.
2. 6th May 2010 at Vistana Hotel, Penang.
3. 1st July 2010 at Cititel Hotel, Penang.

■ Digital Forensics Services

We collaborated with Digital Forensics Department, Mr. Aswami Fadillah Mohd Ariffin to conduct talk sessions in order to promote the Digital Forensics services to the relevant parties. Among the parties involved are as listed below:

1. Perak Chief Police Office on 17th February 2010.
2. Police Headquarters Ipoh Branch on 16th April 2010.
3. Ipoh Road Transport Department on 29th July 2010.
4. Ipoh Immigrations Department on 29th July 2010.
5. National Audit Department on 6th August 2010.

Besides that, we at the Northern Regional Office and Digital Forensics Department participated in roadshows organized by Kelab Anak Malaysia held at:

1. Taiping Municipal Council Hall on 5th -7th March 2010.
2. Manjung Municipal Council Hall on 11th -13th March 2010.
3. Indera Mulia Stadium on 2nd – 4th April 2010.

The talk sessions and roadshows successfully introduced CyberSecurity Malaysia's services especially our Digital Forensics Department to all the governmental departments in Perak and also to the Perak residents.

■ Civil Society Council

A Civil Society Council was formed to enable all community segments to gather and exchange views on various issues especially ones that can generate inspirations towards the acquisition of peace and prosperity to Perak. What was promised was on the 3Qs: (i) Quality Income; (ii) Quality Opportunity; and (iii) Quality Living.

CyberSecurity Malaysia was represented by Ms. Carrine Teoh, she also sits in the advisory panel. All selected members propose a solution to achieve the 3Qs, through seven main groups and will deliberate on strategies, programs, projects and activities that can give impacts to the development of Perak Amanjaya, thus creating opportunity for relevant parties to deliver achievable inputs and impacts to the community within the short- and medium-terms.

The benefit to CyberSecurity Malaysia is that we are able to promote and introduce CyberSecurity Malaysia to the Civil Society Council and also to the Perak State Government.

■ CyberSAFE Awareness

CyberSAFE programme actively promoted and conducted programs in the Northern Regional Office. The approaches used were an extension of briefings and talks to schools, universities, government offices and private sectors. Most of the briefings and talks conducted were via invitations. Apart from that, we engaged in booths set-up activities whenever an ICT program and event is organised in Perak. Most of these activities were conducted in collaboration with KPerak Inc. and Kelab Anak Malaysia.

CyberSAFE talks and briefings conducted are as follows:

- Sekolah Menengah Sains Teluk Intan – 14 May 2010
- Institut Pendidikan Guru Kampus Ipoh – 21 May 2010
- Dewan Orang Ramai, Pangkor Perak – 12 Julai 2010
- Kolej Islam Darul Ridzuan – 14 Ogos 2010
- Sekolah Menengah Klian Pauh – 25 September 2010
- Sekolah Siputeh – 2 Oktober 2010 (Booth & talks)
- Sekolah Men. Tun Perak – 10 November 2010
- Sekolah Menengah Pangkalan – 11 November 2010
- Sekolah Keb Dato Kamaruddin Batu Kurau – 12 November 2010
- Sekolah Kebangsaan Khir Johari, Sg. Sumum (Booth & talks)
- Sekolah Kebangsaan Seri Iskandar – 15 November 2010.

The benefits gained by CyberSecurity Malaysia through the CyberSAFE programmes conducted are:

- Able to increase the level of awareness amongst the participants on computer and internet security issues when downloading certain information through the internet.
- Increase safety awareness on social networking sites such as Facebook and others.
- Introduce CyberSecurity Malaysia and its services to the participants.

Achievements of Northern Region Office in 2010:

- MOU with Perak State Govt
- Successfully promoted the MyCC Financial Assistance program in the Northern Region through seminars
- Successfully obtained 47 products applicants for MyCC Financial Assistance from the Northern Region
- Successfully promoted the Digital Forensics services in the Northern Region
- Successfully promoted and conducted CyberSAFE programs in Northern Region
- Successfully increased the level of cyber safety awareness in Northern Region
- CyberSecurity Malaysia was appointed as the Advisory Panel for the Civil Society Council of Perak

For this year, 2011, KPerak Inc. has agreed to collaborate with CyberSecurity Malaysia to promote Digital Forensics Training. KPerak Inc. has also agreed to build a Digital Forensics Training Lab in collaboration with CyberSecurity Malaysia to market and conduct Digital Forensic Trainings in Perak.

As a continuation to the MOU with Perak State Government, we have sent a proposal to the State Government on 1st March 2011. Amongst the services proposed to the State Government includes:

1. Vulnerability Assessment Services (VAS)
2. Wireless Security Assessment Services
3. Data Sanitization Policy
4. Initial Establishment of Perak CERT
5. Training and Capacity Building Policy Reference.

In 2011, KPerak Inc. also started collaboration with CyberSecurity Malaysia Northern Region Branch to pilot Securing Digital City initiative in Perak.

Operation's Review

2. Key Events in 2010

2.1 Awards and Recognition

■ THE ASEAN YOUTH AWARDS

On 24 Disember 2010, CyberSecurity Malaysia was conferred a Special Recognition Award for its Corporate Social Responsibility Programs (CSR) by the ASEAN Youth Collaboration Committee and the Philippine National Youth Commission in conjunction with the 16th ASEAN Youth Day celebration conducted in Manila, Philippine on 19th December 2010.

The award was conferred as recognition towards the various beneficial CSR programmes conducted by CyberSecurity Malaysia. The CSR programmes organized includes a special project conducted for the Poor Citizens and Orphans from the Bait Al-Amin Charity Organisation in Parit, Perak Darul Ridzuan. The program, which is called Tunas Cemerlang, invited scholars from Petronas Technological University (UTP) as mentors that extend their care to the needy. Recognition was also conferred to the Projek Kumpulan Harapan that aims to motivate and inspire seven categories of special community group such as the underprivileged, orang asli, mat rempit, hard core poor, orphans and the elderly. Kumpulan Harapan first project was conducted with the participation of 50 youths from the Batu Pahat district, Johor, in which various charitable activities were conducted such as "gotong royong", talks on CyberSAFE, motivational session and Sharing of Knowledge.

The conferment of the award was accepted by YABhg. General Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed, Chairman of CyberSecurity Malaysia in Manila during the 16th ASEAN Youth Day. A representative from CyberSecurity Malaysia also presented a CSR Project paper during the forum that was chaired by Christopher Lawrence S Arnuco, Head and CEO for the Philippine National Youth Commission.

The 16th ASEAN Youth Day is an annual event conducted by the ASEAN Youth Cooperation Commission (CAYC). CAYC was established in September 1975 and subsequently, every year each ASEAN member will take turn to host the event. Malaysia played host in 2009 during the World Computer Security Day, in which CyberSecurity Malaysia conducted a special session that deliberated on cyber security issues to the ASEAN Cyber Volunteer team. The seminar successfully brought together volunteering youth from ASEAN countries to congregate and acquire an in-depth knowledge and exposure on the latest advancement in the ICT world and developed a mutually beneficial relationship and network with participants from various ASEAN countries which could further narrow the digital gap between youths within the ASEAN Countries.



The ASEAN Youth Awards. General Tan Sri Dato' Seri Mohd Azumi bin Mohamed (Retired), Chairman of CyberSecurity Malaysia, received the award on behalf of CyberSecurity Malaysia.

■ AWARDS RECEIVED BY EMPLOYEES OF CYBERSECURITY MALAYSIA IN 2010

A number of employees of CyberSecurity Malaysia received recognition from various quarters, locally and internationally. The awards are listed below:

- i) Harold F. Tipton Lifetime Achievement Award by (ISC)2, USA in 2010: awarded to YBhg. Lt Col Dato' Prof. Husin Jazri (Retired) – Chief Executive Officer, CyberSecurity Malaysia
- ii) Chief Security Officer (CSO) ASEAN Award 2010, received by YBhg. Lt Col Dato' Prof. Husin Jazri (Retired) at the CSO conference & Award 2010 held at Ho Chi Minh City, Vietnam.
- iii) PIKOM Leadership Awards 2010 - ICT Personality of the Year 2010: Awarded to Lt. Col. Dato' Husin Jazri (Retired) – Chief Executive Officer, CyberSecurity Malaysia
- iv) Senior Information Security Professional Honoree at the Fourth Annual (ISC)2 Asia-Pacific Information Security Leadership Achievements Program in 2010: Awarded to Mr. Zahri bin Yunus, Lt. Col. Asmuni bin Yusof (Retired), Ms. Maslina binti Daud.
- v) Managerial Professional for an Information Security Project Honoree at Fourth Annual (ISC)2 Asia-Pacific Information Security Leadership Achievements Program in 2010: Awarded to Mr. Mohd Shamir b Hashim.
- vi) Information Security Practitioner Honoree at Fourth Annual (ISC)2 Asia-Pacific Information Security Leadership Achievements Program in 2010: Awarded to Ms. Norhazimah binti Abdul Malek.



CEO, YBhg. Lt Col Dato' Prof. Husin Jazri (Retired) receiving CSO ASEAN Award 2010 - Vietnam



Harold F. Tipton Lifetime Achievement Award by (ISC)2, USA in 2010: awarded to YBhg. Lt Col Dato' Prof. Husin Jazri (Retired) – Chief Executive Officer, CyberSecurity Malaysia



The five distinguished honorees of the (ISC)2 Information Security Leadership Award (ISLA) 2010 from CyberSecurity Malaysia, with YBhg. Lt Col Dato' Prof. Husin Jazri (Retired), recipient of the Harold F. Tipton Lifetime Achievement Award.

2.2 CyberSecurity RSA Seminar 2010

8 & 9 February – Located at the Putra World Trade Centre, CyberSecurity Malaysia and RSA successfully conducted CyberSecurity RSA seminar that was held for the first time in Malaysia. The seminar, which was themed “Where The Experts Talk Security 2010” held discussions on the threats that poses risk to the safety of critical information. In addition, the seminar also deliberated on the activity flow of cyber crimes and how it is conducted in the cyber world. Several other high profile activities were also conducted during the seminar such as:

Operation's Review

- InfoSecurity Professional Networking Session titled “Shifting Cyber Landscape: Gearing Towards Innovation”. Two prominent speakers were invited to deliver their speech namely Professor Fred Piper from Royal Holloway University, a respected specialist in the field of Cryptography and Dr Gobi Kurup, Head Technology Officer, EXTOL MSC. The event became a platform for local information security practitioners and even for institutions to share information, exchange ideas and discuss on the challenges in information security at the global and international arena. A total of 154 participants came together to discuss issues on information security during the seminar.
- The Safer Internet Day 2010 (SID2010) with the theme of “Personal Image Management Online” that boasted the slogan of “Think Before You Post” had its inaugural inception in Malaysia. The event was conducted with the objective to enhance and improve awareness on internet safety among youth and children and enabling them to filter malicious and incorrect information in the internet.



CyberSecurity RSA Seminar

A total of 100 participants from local agencies attended the seminar. Seven topics were tabled by local and international speakers. The seminar also mustered wide coverage from both print and digital media.

CyberSecurity Malaysia active participation in the organisation and hosting of this prestigious seminar also portrays the recognition of foreign countries on CyberSecurity Malaysia expertise in the field of information security in tandem with our prime objective of becoming a “Centre of Excellence”

2.3 The Third Cyber Crisis Exercise, X-Maya 3

On the 5th of August 2010, the National Security Council and CyberSecurity Malaysia joined hands to coordinate and conduct the country's third annual Cyber Crisis Exercise, codenamed X-MAYA 3, a simulated and coordinated exercise to assess the cyber security emergency readiness of Malaysia's Critical National Information Infrastructure (CNII) to cope with cyber attacks.

The exercise saw the participation of 34 organisations from nine Critical National Information Infrastructure (CNII) sectors – namely Health, Water, Banking and Finance, Information and Communications, Energy, Transport, Defense and Security, Government and Agriculture. This was an increase over the X-Maya 2 exercise which was held in December 2009, which involved 28 CNII organisations.

The economic and governance activities of the country have drastically changed in line with the wider use of ICT. Due to this, efforts related to national security must take into account the threats from cyberspace. The economy's reliance on Information and Communications Technology (ICT) and communications networks requires us to ensure that the CNII is secured and protected from threats. We must address these threats effectively as there are a range of ICT-dependent public services which are critical components in maintaining social, economic and political stability, and national security in general.

This annual drill is a very hands-on exercise for all the participants, and the experience can be used to improve internal procedures and provide feedback to enhance the National Cyber Crisis

Management Plan (NCCMP). This will further improve the nation's readiness in dealing with wide-scale cyber crisis incidents.

The X Maya 3 received a very positive response from various organisations.

CyberSecurity Malaysia provided the technical support and infrastructure for the exercise this year as it had done in the previous two exercises. The agency leveraged on its experiences in coordinating the Asia Pacific Computer Emergency Response Team Annual Cyber Exercise (APCERT Drill) as well as experiences in dealing with cyber security incidents through its Cyber999 Help Centre and Malware Research Centre initiatives.



The National Cyber Drill or X-Maya exercise gives a thorough examination of the related CNII organisations to strengthen national emergency response by ensuring that the proper procedures and mechanisms are in place for effective monitoring of the CNII, incident reporting and response, communications dissemination and business continuity management.

2.4 Strategic Collaboration Agreement with stratsec.net Australia for

On 4 August 2010, CyberSecurity Malaysia, signed a formal agreement with stratsec Australia, one of the leading providers of independent information security consulting and testing services in Australia and South East Asia. With the agreement, this will be the first time an Australian company or a commercially-based security evaluation facility will set up operations under the Malaysian Common Criteria Evaluation and Certification Scheme (MyCC Scheme).

The signing ceremony between the CEO of CyberSecurity Malaysia, YBhg. Lt Col Dato' Prof. Husin Jazri (Retired) and the CEO of stratsec Peter Lilley on August 4, 2010 in Canberra, was witnessed by Datuk Seri Dr. Maximus Johnity Ongkili, Minister of Science, Technology and Innovation (MOSTI) and Mr Jon Stanhope MLA, Chief Minister of the Australian Capital Territory.



CyberSecurity Malaysia signed a formal agreement with stratsec.net Sdn. Bhd. (stratsec.net), an MSC status company of which the holding company is in Australia.

The agreement will help grow a world class IT security evaluation facility in Malaysia and provide increased opportunities for Malaysian ICT product developers. The collaboration with stratsec will help to position Malaysia for the future - by providing a strong branding for "Made in Malaysia" ICT products - due to compliance with well-known and recognized international standards ISO/IEC 15408. As a result of a strong MALAYSIA BRAND, consumer confidence and market demand for Malaysian-made ICT products will be greatly increased.

CyberSecurity Malaysia has been working with stratsec since 2007 to define and implement the MyCC Scheme. Throughout this relationship, CyberSecurity Malaysia and stratsec remained firmly committed to the development of a local specialist IT security industry in Malaysia. The final

Operation's Review

agreement between CyberSecurity Malaysia and stratsec will increase assurance between Australian and Malaysian trade and highlight such beneficial relationships to existing businesses.

CyberSecurity Malaysia hopes to attract more Australian ICT security businesses to enter the South East Asian market by promoting the development of a vibrant local ICT security capability in Malaysia.

2.5 Cyber Security Malaysia Awards, Conference and Exhibition 2010 (CSM-ACE 2010)

25-29 October – CyberSecurity Malaysia successfully organized the Cyber Security Malaysia Awards, Conference and Exhibition 2010 (CSM-ACE) at the Kuala Lumpur Convention Centre. The event was officiated by YB. Datuk Haji Fadillah bin Haji Yusof, Deputy Minister of Science, Technology and Innovation. The event was also graced by the presence of YAB. Dato' Seri Dr. Zambry Abdul Kadir – Chief Minister of Perak, YABhg. General Tan Sri Dato' Seri Panglima Mohd Azumi Mohamed (Retired) – Chairman of CyberSecurity Malaysia, Lt. Col. Dato' Prof. Husin Jazri (Retired) – Chief Executive Officer of CyberSecurity Malaysia, and the Heads of government agencies as well as the private sectors.



CSM-ACE 2010 launching ceremony

During the officiation ceremony, an exchange of Memorandum of Understanding also took place between CyberSecurity Malaysia and:

- State Government of Perak
- eWorldWide Group (UAE),
- Knowledge Information Security Industry Association (Korea Selatan/ South Korea),
- BSI Management Systems (Singapore),
- Taiwan Information Security Centre,
- Giat MARA /and
- Universiti Pertahanan Nasional Malaysia.

The exchange of documents was officially witnessed by YB. Deputy Minister of Science, Technology and Innovation.

Themed “Securing Our Digital City”, CSM-ACE 2010 managed to bring together a total of 3,200 participants representing various government agencies, corporations, higher learning institutions, school students and even participants from abroad. CSM-ACE was also able to assemble 40 local and overseas cyber security experts to sit in a forum and present their paperworks according to their respective field of expertise.

Among the programmes conducted within the CSM-ACE 2010 are:

- Policy, Legal & Governance
- Technical programs and forums
- Business Continuity Planning (BCP) & Information Security Management Services (ISMS)
- Exhibition of Information Safety 2010
- Cyber Security Malaysia Awards 2010

Several satellite events were also conducted during the CSM-ACE 2010, such as:

- Workshop and Conference of Computer Emergency Response Team – Organisation of Islamic Conference (OIC-CERT)
- Cyber Entrepreneurships – Threats & Trends Workshop,
- International BCM Conference,
- Cyber SAFE @ CSM-ACE 2010,
- Digital Forensic Forum,
- Cyber War Forum and Cyber War Concept Round Table Discussion
- ISACA 25th Anniversary Dinner, and
- National Key Points Seminar 2010 and Key Points Chief Executive Officer Round Table Discussion 2010

The Malaysia Cyber Security Awards 2010

For the second consecutive year, in conjunction with CSM-ACE 2010, CyberSecurity Malaysia once again organized the Malaysia Cyber Security Awards 2010. The ceremony was graced by YB Datuk Seri Dr. Maximus Johnnity Ongkili, Minister of Science, Technology and Innovation. Malaysia Cyber Security Awards main objective of initiation is to recognize the valuable contributions made by individuals and corporations in the field of cyber security.

The lists of award recipients are as below:

- Managed Security Service Provider of the Year - SCAN Associates Berhad
- Education and Training Provider of the Year - EC Council
- Safety Outreach Provider of the Year - Jabatan Pendaftaran Negara
- Innovative Company of the Year - Extol MSC Berhad and Heitech Padu Berhad
- Information Security Project of the Year - Sime Darby Holdings and Malaysia Airlines System
- Information Security Organization of the Year - Malaysia Airports Technologies Sdn Bhd
- Information Security Visionary of the Year – CXO - Faridah Abdul Rahman, Malaysia Airlines dan Prof Dr Mohamed Ridza Wahiddin, MIMOS
- Information Security Visionary of the Year – Academician – Prof. Abu Bakar Munir of Universiti Malaya
- Deputy Minister's Award - Faridah Abdul Rahman, Malaysia Airlines and Prof. Dr. Mohamed Ridza Wahiddin, MIMOS
- Minister's Award – Prof. Abu Bakar Munir, Universiti Malaya.



Malaysia Cyber Security Awards

CSM-ACE 2010 also received a multitude of coverage and mentions in various mass media such as Bernama TV & Radio, Radio Televisyen Malaysia (RTM), Astro Awani, Berita Harian, Utusan Malaysia, New Straits Times, The Star, Nanyang Siang Pau, Harian Metro and Kosmo. Not to mention the coverage in magazines such as Majalah PC, Majalah Remaja, OIC Today Magazine, Outsourcing Malaysia Magazine and Computerworld Malaysia Magazine.

Through CSM-ACE, CyberSecurity Malaysia is able to provide a platform for professionals around the world to discuss and share their views and ideas on issues related to cyber security. In addition, CSM-ACE 2010 provided and created new business and networking opportunities for companies that exhibited their products during the event.

Operation's Review

Satellite events that were conducted during the CSM-ACE 2010:

■ CSM-ACE 2010 – Cyber War Forum

27 October – CyberSecurity Malaysia in collaboration with National Security Council (MKN) jointly organised the Cyber War Forum 2010. YABhg. General Tan Sri Dato' Seri Panglima Mohd Azumi Mohamed (Retired), Chairman of CyberSecurity Malaysia delivered his welcoming remark during the forum to 74 participants. The objective of the forum is to promote the analysis of cyber war as a trend of overcoming future conflicts, issues and challenges.

A total of 5 papers were presented during the forum.

Listed are the paperworks that were presented at the Forum:

- National Preparedness In Managing & Responding to Cyber Crisis by Ir. Md. Shah Nuri Md. Zain, Secretary of the Cyber & Space Security Policy Division, National Security Council.
- Analysis on Cyber War As the Trend of Future Conflict by En. Sazali Sukardi, Head of Strategic Policy Research, CyberSecurity Malaysia.
- Global Crisis - The Need for Regional Collaboration by Prof. Benoit Morel, Carnegie Mellon University.
- Cyber War – Estonia's Experiences by Mr. Kenneth Geers, Cooperative Cyber Defence Centre of Excellence, Estonia.
- Cyber War and International Law by Prof. Madya Lt. Col. Ahmad Ghazali (Bersara), National Defense University Malaysia.

In the evening, a round table discussion on cyber war concept was conducted. The discussion was chaired by Ir. Md. Shah Nuri Md. Zain. During the session, CyberSecurity Malaysia tabled the cyber war concept paper based on the feedback received. CyberSecurity Malaysia was advised to conduct a follow-up discussion on the concept highlighted.

■ Organization of the Islamic Conference – Computer Emergency Response Team (OIC-CERT) Conference & Workshop 2010

28-29 October – held at the Kuala Lumpur Convention Centre, the OIC-CERT Conference and Workshop was officiated by YB. Datuk Haji Fadillah bin Haji Yusof, Deputy Minister of Science, Technology and Innovation. The launching of the event was also witnessed by En Mohamed Abdulrahman Elbusefi, a representative from the Organisation of Islamic Conference and YABhg. General Tan Sri Dato' Seri Panglima Mohd Azumi Mohamed (Retired).



OIC-CERT Conference and workshop at CSM-ACE 2010

During the event YB Datuk Haji Fadillah bin Haji Yusof also launched The Child Online Protection Handbook - Malaysia edition that was published in collaboration between CyberSecurity Malaysia and eWorldWide Group, UAE.

The paperwork presentation session and list of panellists are as follows:

- Securing the Digital Society - Way Forward by Prof. Benoit Morel, Carnegie Mellon University, USA.
- The Challenges That Lies Ahead

Panellists 1:

- Salma Abbasi, EWWG, UAE
- Shehzad Ahmad, DK-CERT, Denmark
- Clayton Jones, (ISC)2®, Asia Pacific
- Sean Lim, EC-Council
- Emerging Threats on Information Society

Panellists 2:

- Dr. Alireza Keshavarz, Shiraz University, Iran
- Kayne Naughton, Shadowserver Foundation, Australia
- Julia Cheng, TWISC, Taiwan
- Developing and Maintaining Cooperation Models

Panellists 3:

- Ammar Jaffri, PISA-CERT, Pakistan
- Yurie Ito, ICANN, USA
- Adli Abd Wahid, APCERT / CyberSecurity Malaysia, Malaysia

■ **OIC-CERT Steering Committee Meeting.**

Six of the seven Member Countries sent in their delegates to attend the OIC-CERT Steering Committee Meeting. CyberSecurity Malaysia chaired the meeting that discussed on the OIC-CERT direction and future activities.

■ **30 October – OIC-CERT 2nd Annual General Meeting (AGM)**

10 from the total of 18 member countries attended the meeting that was chaired by CyberSecurity Malaysia. Several resolutions was tabled focusing on the creation of new membership category for OIC-CERT, Proposal of future project was also presented and deliberated for member's consent.

National Key Points Seminar 2010

28 October – National Key Points Seminar 2010 themed “Protection of National Key Points in the Cyber World” conducted in collaboration with the Ministry of Internal Affairs (KDN), The Chief Government Security Office (CGSO) and CyberSecurity Malaysia.

The seminar aimed to attract participation from owners and operators of Critical National Information Infrastructure (CNII) and focused on the sharing of knowledge and latest direction and instruction to protect CNII. The seminar was attended by 270 officers from the CNII sector.



OIC-CERT Annual General Meeting

The seminar was officiated by YBhg. Dato' Sri Mahmood bin Adam, Secretary General of the Ministry of Internal Affairs. Also present to grace the ceremony was YBhg Dato' Johari bin Hj Jamaluddin, National Security Council's Director General and YBhg. Lt Col Dato' Prof. Husin bin Jazri (Retired), Chief Executive Officer of CyberSecurity Malaysia.

Operation's Review

A total of 6 paperworks were presented during the seminar:

- Estonia Experience : Lesson Learned oleh/by Mr Kenneth Geers, Cooperative Cyber Defence Centre of Excellence, Estonia
- Critical National Information Infrastructure Protection by Mr Steve Anson, Managing Director, Forward Discovery Middle East FZ-LLC
- The roles of the Central Committee on Key Points (Jawatankuasa Pusat Sasaran Penting (JPSP)) with regards to the National Key Points by YBhg. Dato' Sri Mahmood bin Adam
- Challenges and threats to the national critical system by Pn Nor' Azuwa binti Muhamad Pahri, CyberSecurity Malaysia
- Information Security Governance Petronas Berhad by En Ainuddin bin Jantan, Petronas Berhad
- Information Security Governance: Telekom Berhad by YBhg. Dato' Sri Zamzamzairani bin Mohd Isa, Telekom Malaysia Berhad



National Key Points Seminar 2010 themed "Protection of National Key Points in the Cyber World at CSM ACE 2010"

Key Points Chief Executive Officers Round Table Meeting 2010

28 October - Chief Executive Officers Round Table Meeting on Key Points 2010 was conducted in collaboration between KDN, CGSO and CyberSecurity Malaysia. The Meeting was chaired by YBhg. Dato' Sri Mahmood bin Adam, Secretary General, Ministry of Internal Affairs.

The meeting with the theme of "Protection of Key Points in the Cyber Worlds - Future Challenges," was conducted to provide a platform for knowledge sharing between the government and private sector in the improvisation and strengthening of National Key Points.

2.6 Safer Internet Day



9 February - In conjunction with the "Safer Internet Day" celebration, CyberSecurity Malaysia conducted a cyber security awareness seminar targeted specifically to youth. The seminar was conducted at the Putra World Trade Centre during the CyberSecurity RSA seminar and attended by 135 participants from Giat Mara, Persatuan Gabungan Pelajar Melayu Semenanjung, Non Government Agencies (NGO) and the public community in general. The objective of the seminar is to provide

exposure and awareness to youth in our country on the aspect of cyber security. CyberSecurity Malaysia delivered three papers during the seminar namely "What happened in Phuket...", "Social Engineering and Internet Habits" and "Mobile Internet Safety".

Through this seminar, CyberSecurity Malaysia was able to expand its working collaboration with the Technology Education Division, Ministry of Education, and worked towards enhancing Internet user's awareness in the field of cyber security in Malaysia.

2.7 World Computer Security Day (WCSD)

30 November - CyberSecurity Malaysia led the WCSD celebration this year by holding a special talk session with the media. The celebration was successfully conducted on 30th November 2010 at the Royal Chulan Hotel, Kuala Lumpur in which the main objective of the event was to provide education and awareness to the general public on the safety aspect of the Internet. A total of 14 media delegates attended the talk including BERNAMA (wire), Lowyat.net, OIC Today, The Star, BERNAMA Radio 24, Computerworld Malaysia and Utusan Malaysia.



November 30 is the
World Computer Security Day
Be Smart, Be Safe

2.8 Corporate Social Responsibility (CSR) Projects

■ CSR project at Bait Al-Amin, Parit Perak

Since 2008, CyberSecurity Malaysia has embarked into various CSR Projects to bridge the gap between the city and suburban communities specifically with Bait Al-Amin, an orphanage in Parit, Perak. CyberSecurity Malaysia in collaboration with University Petronas, Tronoh set a mission to help the orphans achieve better results in school by using the mentor-mentee programme. The mission was a success when the school's principal reported that the students have achieve better results in thier exams ever since.



The children of Bait Al-Amin with representatives from CyberSecurity Malaysia, University Petronas and Jusco Ipoh.

Impact Coverage and Criticality:

- Emphasizing on giving the opportunity to local communities especially the orphans to grow their understanding of ICT access and usage.
- It is understood that the internet communications will affect social changes in strengthening human capital.
- The ICT knowledge and skills are essential towards nurturing Malaysia's next generation of leaders.
- With the effort of continuing to financially support this project, CyberSecurity Malaysia's contribution to the nation is more observable. Plus, the orphans will be more IT-literate and knowledgeable in Cyber world.

Operation's Review



The participants with YB Dato' Noraini Ahmad representative from CyberSecurity Malaysia

■ CSR project – “Memperkasakan Belia Harapan”

This CSR project specifically aims to motivate and inspire “7 underserved communities” with activities like CyberSAFE and motivational sharing session. The 7 communities identified are:

- i) OKU (handicapped)
- ii) Orang asli
- iii) Mat Rempit
- iv) Delinkuen (delinquent)
- v) Miskin Tegar (hard core poor)
- vi) Anak Yatim (orphans)
- vii) Warga Tua (elderly)

2.9 Malaysia Innovative 2010 (MI2010) Southern Zone and Musical Creativity Night

CyberSecurity Malaysia was tasked to lead the organisation of Malaysia Innovative 2010 (MI2010) Southern Zone and Musical Creativity Night at Universiti Tun Hussein Onn (UTHM), Batu Pahat on 25 and 26 September 2010. The event became the benchmark for other agencies under MOSTI to emulate especially in the organization of their own Musical Creativity Night.

Sekolah Kebangsaan Seri Utama from Batu Pahat was selected as the winner of Musical Creativity Night for MI2010 Southern Zone and represented Southern Zone to the Festival Kreativiti MI2010 at Bukit Jalil. The school eventually became a national champion at the aforesaid event on 25 November 2010.



The final moments of Musical Creativity Night for Southern Zone

Participation in Exhibition for MI2010 at:

1. Festival MI2010 Bukit Jalil from 24- 26 November 2011
2. MI2010 Central Zone, MITC Melaka from 13 - 14 November 2011
3. MI2010 Sarawak Zone, Kuching from 23 - 24 Oct 2010
4. MI2010 Eastern Zone, TTC Kuala Terengganu from 30 - 31 July 2010
5. MI2010 Sabah Zone, Universiti Malaysia Sabah from 28 - 30 May 2010
6. MI2010 Northern Zone, Dewan wawasan Kangar from 27 - 28 February 2010

INFORMATION SECURITY PROFESSIONAL DEVELOPMENT



www.cyberguru.my

Strategic Partnership 2010

Partnership with APCERT

Australia
Bangladesh
Brunei Darussalam
China
Chinese Taipei
Hong Kong
India
Indonesia
Japan
Korea
Malaysia
Mongolia
The Philippines
Singapore
Sri Lanka
Thailand
Vietnam

Partnership with OIC-CERT

Bangladesh
Brunei
Egypt
Indonesia
Iran
Jordan
Libya
Malaysia
Morocco
Nigeria
Oman
Pakistan
Saudi Arabia
Syria
Tunisia
Turkey
United Arab Emirates

Partnership with other CERT Countries

Brazil [Brazilian National Computer Emergency Response Team (CERT.br)]
Netherlands [Computer Emergency Response Team for the Dutch Government (GOVCERT.NL)]
Norway [Norwegian Computer Emergency Response Team (NorCERT)]
Russia [Computer Security Incident Response Team of Russian Federation]

Partnership with International Institutions

Cyber Development Corps ASEAN Youth Council
Disaster Recovery Institute (DRI)
European Network and Information Security Agency (ENISA)
Forum of Incident Response and Security Teams (FIRST)
International Information Systems Security Certification Consortium, Inc., (ISC)²
Inter-American Committee Against Terrorism (CICTE)
International Youth Centre and IESCO
Korea Institute of Criminology

Common Criteria Recognition Arrangement

Australia and New Zealand
Austria
Canada
Czech Republic
Denmark
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Republic of Korea
Malaysia
The Netherlands
Norway
Pakistan
Singapore
Spain
Sweden
Turkey
The United Kingdom
The United States

National Strategic Partnership

.MyDomain Registry
Asia E University
Bahagian Pematuhan ICT, MAMPU
HeiTech Padu
Institut Sosial Malaysia
IPTA, IPTS kawasan Petra Jaya
Kolej Yayasan Pelajaran Melaka
Malaysia Airlines System Berhad
MIMOS
Multimedia Development Corporation
Multimedia University
Pejabat Ketua Keselamatan Kerajaan
Perpustakaan Negara Malaysia
RHB Bank
SK Batang Benar dan PIBG
University of Malaya

8 partnerships – Local

i-Pocket Sdn Bhd. (April 2010)- Security assurance services for Common Criteria Evaluation Program
Vads Berhad (April 2010)- Customer contact unit
Perbadanan Putrajaya (April 2010)- Destroy government secrets privy to the former on discarded/unused computer hard-disks
UTEM Melaka (23rd June)- Collaboration in research on IPV4 and IPV6
Stratsec.net Sdn Bhd (6 July 2010)- Malaysian Common Criteria Evaluation and Certification (MYCC) program
Kolej Yayasan Melaka (KYM) (18 April 2010)- Collaboration on Tunas Cemerlang
National Defense University (26 Oct 2010)- Strategic Partnership on Centre of Excellent
The Perak State Government (26 Oct 2010) - Knowledge Sharing and Technical Assistance Collaborative

5 partnerships – International

Department of Post, Telecommunications and New Technologies, Ministry of Industry, Trade and New Technologies, The Kingdom of Morocco (21 Jan 2010)- Establishment of One Stop Coordination Centre of Morocco
e Worlwide Group (28th June 2010) - To establish a general framework for cooperation in the field of cyber security
AECERT (5th July 2010) – CERT exchange program
Korea Information Security Agency (KISA) (27 Oct 2010) - Promotion on development of IT security industry
Taiwan Information Security Center National Cheng-Kung University (26 Oct 2010) - To exchange knowledge and expertise by both parties.

Cyber Forensics Investigations CYBER CSI

CYBER FORENSICS AND INVESTIGATIONS

Uncovering Truth Beyond Digital Imagination

Nowadays, due to the growth of incidents and demands for data recovery and investigation, CyberSecurity Malaysia is extending its digital forensics services to organizations requiring this professional service. Immediate response is to stabilize the involved computers, protecting and recovering the data evidence within. This is based on the systematic foundations of digital forensics methodology, which involves digital evidence **collection, preservation, analysis** and **presentation**. A variety of operation can be under taken such as hard disk data analysis, retrieval of deleted file, intrusion tracking and discovery.

Corporate Governance

STATEMENT OF CORPORATE GOVERNANCE

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

BOARD RESPONSIBILITIES

The Board maps out and reviewed CyberSecurity Malaysia's strategic plans on an annual basis to ensure CyberSecurity Malaysia's operational directions and activities are aligned with the goals of its establishment by the Government of Malaysia. The Board considers in depth, and if thought fit, approves for implementation key matters affecting CyberSecurity Malaysia which include matters on action plans, annual budget, major expenditures, acquisition and disposal of assets, human resources policies and performance management. The Board also review 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 obtained the prior approval from the Minister of Domestic Trade and Consumer Affairs (MDTCA).

At least half of the total composition of the Members of the Board must be from the government sector and are to be appointed by the Minister of Science, Technology and Innovation. The remaining members may be from the commercial or other relevant sectors that has 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.

Corporate Governance

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 meeting of the Board are tabled for review by the Members of the Board. At these Board meetings, the Members of the Board also evaluate business and operational propositions and corporate proposals that require Board's approval.

The agenda for every Board meeting, together with comprehensive management reports, proposal papers and supporting documents, are furnished to all Directors for their perusal, so that the Directors have ample time to review matters to be deliberated at the Board's meeting and at the same time to facilitate decision making by the Directors.

As at the end of the financial year 2010, five (5) Board Meetings were held.

APPOINTMENT AND RE-ELECTION OF THE BOARD MEMBERS

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

YBhg. Dato' Madinah binti Mohamad, Director of CyberSecurity Malaysia is not subject to retirement since she is representing MOSTI. YBhg. 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. Encik Ir. Md. Shah Nuri bin Md. Zain and Puan Rubaiah binti Hj Hashim who are the Directors holding office for a term of two (2) year, which terms is expiring pursuant to Articles 31 of the Articles of Association of CyberSecurity Malaysia. They offer themselves for re-election as a Director and will be considered for approval by the Members of CyberSecurity Malaysia at the Fifth Annual General Meeting 2011.

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 objective of CyberSecurity Malaysia. The prescribing and maintenance of a system of internal controls, however, provides a reasonable assurance of effective and efficient operations, and compliance with laws and regulations, as well as with internal procedures and guidelines.

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

The internal risk control and management programmes prescribed by the Board include policies and procedures on risk 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.



Certified • Recognised • Assured

www.cybersecurity.my/mycc



Corporate Office:

CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888

Regional Office:

CyberSecurity Malaysia, Level 19, Perak Techno-Trade Center, Bandar Meru Raya, Off Jln. Jelapang, 30020 Ipoh, Perak Darul Ridzuan | Tel: +605 - 528 2088 | Fax: +605 - 528 1905

Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

Financial Statement

Corporate Information

Board of Directors

- General Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired) - Chairman
- Dato' Madinah binti Mohamad
- Lt Col Dato' Prof. Husin bin Jazri (Retired)
- Datuk Abang Abdul Wahap bin Abg Julai
- Datuk Dr. Abdul Raman bin Saad
- Puan Rubaiah binti Hashim
- Encik Ir. Md. Shah Nuri Md. Zain
- Puan Rohani binti Mohamad

Registered Office

Level 8, Block A, Mines Waterfront
Business Park
No. 3 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

Administrative and Correspondence Address

Level 4, Block C, Mines Waterfront
Business Park
No. 3 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

Company Secretary

Jailany bin Jaafar

Auditors

Azman, Wong, Salleh & Co.
(AF: 0012)
Chartered Accountants

Functional and Presentation Currency

Ringgit Malaysia (RM)

Financial Statement

Directors' Report

The Directors have pleasure in submitting their report and the audited financial statements of the Company for the year ended 31 December 2010.

1. PRINCIPAL ACTIVITY

The principal activities of the Company are the provision of Cyber National Security Services namely Cyber Emergency Services, Security Quality Management Services, Cyber Security Research and Policy Services and Security Professional Development and Outreach Services

There have been no significant changes in these activities during the year.

2. LIMITED LIABILITY

The Company was incorporated under the Companies Act, 1965 on 14 March 2006 as a company limited by guarantee, not having a share capital and not for profit. Currently, the Company has 2 members. In the event that the Company is wound up, a member or a person who was a member twelve months prior to that event is liable to contribute to the assets of the Company a sum not exceeding Ringgit Malaysia One Hundred (RM100).

3. RESULTS

Net surplus of income for the year

RM
(68,098)

4. RESERVES AND PROVISIONS

There were no material transfers to or from reserves or provisions during the year ended 31 December 2010

5. DIRECTORS OF THE COMPANY

- General Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired) - Chairman
- Lt Col Dato' Prof. Husin bin Jazri (Retired)
- Puan Rubaiah binti Hashim
- Encik Ir Md Shah Nuri Md Zain
- Datuk Abang Abdul Wahap bin Abg Julai
- Datuk Dr. Abdul Raman bin Saad
- Dato' Madinah binti Mohamad
- Puan Rohani binti Mohamad

Since the end of the last financial year, no director of the Company has received or become entitled to receive any benefit (other than a benefit included in the aggregate amount of emoluments received or due and receivable by the directors shown in the financial statements, or the fixed salary of a full time employee of the Company) by reason of a contract made by the Company or a related corporation with the director or with a firm of which the director is a member, or with a company in which the director has a substantial financial interest.

Neither during nor at the end of the financial year was the Company a party to any arrangements whose object was to enable the directors to acquire benefits by means of the acquisition of shares in or debentures of the Company or any other body corporate.

6. OTHER STATUTORY INFORMATION

- (a) Before the statement of comprehensive income and statement of financial position of the Company were made up, the directors took reasonable steps:-
- i. to ascertain that action had been taken in relation to the writing off of bad debts and the making of allowance for doubtful debts and have satisfied themselves that all known bad debts had been written off and that adequate allowance had been made for doubtful debts; and
 - ii. to ensure that any current assets, other than debts, which were unlikely to realise in the ordinary course of business their values as shown in the accounting records of the Company had been written down to an amount which they might be expected so to realise
- (b) At the date of this report:-
- i. the directors are not aware of any circumstances which would render the amounts written off for bad debts or the amount of the allowance for doubtful debts in the financial statements of the Company inadequate to any substantial extent;
 - ii. the directors are not aware of any circumstances which would render the values attributed to the current assets in the financial statements of the Company misleading or inappropriate;
 - iii. the directors are not aware of any circumstances which have arisen that would render adherence to the existing method of valuation of assets or liabilities of the Company misleading;
 - iv. the directors are not aware of any circumstances which would render any amount stated in the financial statements misleading;
 - v. there does not exist any charge on the assets of the Company which has arisen since 31 December 2010 which secures the liabilities of any other person; and
 - vi. there does not exist any charge on the assets of the Company which has arisen since 31 December 2010 which secures the liabilities of any other person; and
- (c) No contingent or other liability has become enforceable or is likely to become enforceable within the period of twelve months after the end of the financial year which, in the opinion of the directors, will or may substantially affect the ability of the Company to meet its obligations as and when they fall due.

In the opinion of the directors :-

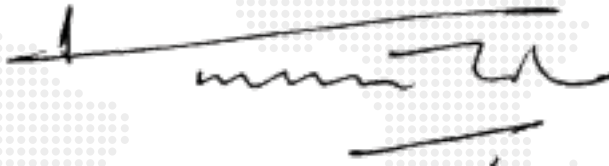
1. the results of the Company's operations during the financial year were not substantially affected by any item, transaction or event of a material and unusual nature; and
2. there has not arisen in the interval between the end of the financial year and the date of this report any item, transaction or event of a material and unusual nature likely to substantially affect the results of the operations of the Company for the financial year in which this report is made.

Financial Statement

7. AUDITORS

The auditors, Azman, Wong, Salleh & Co., have expressed their willingness to accept reappointment.

In accordance with a resolution of the Board of Directors dated



GENERAL TAN SRI DATO' SERI PANGLIMA MOHD AZUMI BIN MOHAMED (RETIRED)



YBHG. LT COL DATO' PROF. HUSIN BIN JAZRI (RETIRED)

Kuala Lumpur,
Date: 2 June 2011

STATEMENT OF FINANCIAL POSITION AS AT 31 DECEMBER 2010

		2010	2009
	Note	RM	RM
ASSETS			
Non Current Assets			
Property, plant and equipment	6	29,907,889	27,607,629
Intangible assets	7	3,207,060	3,345,713
		33,114,949	30,953,342
Current Assets			
Trade receivables	8	1,160,847	660,945
Other receivables		961,728	1,115,492
Short term deposits with licensed banks	9	5,000,000	8,000,000
Cash and bank balances		1,724,233	16,205,211
		8,846,808	25,981,648
Total Assets		41,961,757	56,934,990
RESERVES AND LIABILITIES			
Reserves			
Accumulated reserves		1,509,686	1,577,784
Non Current Liabilities			
Government grants	10	40,237,037	53,656,081
Current Liabilities			
Other payables and accruals		164,120	1,345,298
Tax payable	11	50,914	355,827
		215,034	1,701,125
Total Reserves and Liabilities		41,961,757	56,934,990

**STATEMENT FOR COMPREHENSIVE INCOME FOR THE YEAR ENDED
31 DECEMBER 2010**

		2010	2009
	Note	RM	RM
INCOME FROM GRANT	12	47,985,108	34,141,928
OPERATING REVENUE	13	1,892,843	1,235,951
OTHER INCOME	14	213,924	172,623
		50,091,875	35,550,502
STAFF COST		(21,399,354)	(14,664,163)
DIRECTORS' EMOLUMENTS		(540,948)	(363,288)
DEPRECIATION AND AMORTISATION		(4,406,540)	(2,673,287)
RENTAL		(4,323,685)	(3,705,352)
OTHER OPERATING EXPENSES		(19,438,534)	(12,721,102)
(DEFICIT)/SURPLUS OF INCOME BEFORE TAXATION	15	(17,184)	1,423,310
TAXATION	11	(50,914)	(355,827)
TOTAL COMPREHENSIVE (DEFICIT)/SURPLUS FOR THE YEAR		(68,098)	1,067,483

**STATEMENT OF CHANGES IN RESERVES FOR THE YEAR ENDED
31 DECEMBER 2010**

	Accumulated Reserves
	RM
As at 1 January 2009	510,301
Total comprehensive surplus for the year	1,067,483
Balance at 31 December 2009	1,577,784
Total comprehensive deficit for the year	(68,098)
Balance at 31 December 2010	1,509,686

STATEMENT OF CASH FLOW STATEMENT FOR THE YEAR ENDED 31 DECEMBER 2010

	2010 RM	2009 RM
CASH FLOWS FROM OPERATING ACTIVITIES		
Surplus/(deficit) of income before tax	(17,184)	1,423,310
Adjustments for:		
Depreciation of property, plant and equipment	3,474,728	2,087,048
Amortisation of intangible assets	931,810	586,239
Interest income	203,653	176,909
Grant income recognised	(47,985,108)	(34,141,928)
Operating loss before working capital changes	(43,374,917)	(31,291,732)
Changes in working capital :-		
Increase in trade receivables	(499,902)	(537,970)
Decrease/(Increase) in other receivables	153,764	(498,921)
(Increase)/decrease in other payables	(1,181,178)	350,031
	(44,902,233)	(31,978,592)
Operating government grants (Note 10b)	12,144,000	13,800,000
Interest received	(203,653)	(176,909)
Tax Paid	(355,827)	-
Net cash used in operating activities	(33,334,897)	(16,932,191)
CASH FLOWS FORM INVESTING ACTIVITIES		
Purchase of property, plant and equipment	(5,774,988)	(21,483,858)
Purchase of intangible assets	(793,157)	(2,701,146)
Net cash used in investing activities	(6,568,145)	(24,185,004)
CASH FLOWS FROM FINANCING ACTIVITY		
Development government grants received (Note 10a)	22,422,064	55,895,445
NET (DECREASE)/INCREASE IN CASH AND CASH EQUIVALENTS	(17,480,978)	14,778,250
CASH AND CASH EQUIVALENTS AT BEGINNING OF THE	24,205,211	9,426,961
CASH AND CASH EQUIVALENTS AT END OF YEAR	6,724,233	24,205,211
CASH AND CASH EQUIVALENTS COMPRISE:-		
Fixed deposit	5,000,000	8,000,000
Cash and bank balances	1,724,233	16,205,211
	6,724,223	24,205,221

NOTES TO THE FINANCIAL STATEMENT - 31 DECEMBER 2010

1. PRINCIPAL ACTIVITIES

The principal activities of the Company are the provision of Cyber National Security Services namely Cyber Emergency services, Security Quality Management Services, Cyber Security Research and Policy Services and Information Security Professional Development and Outreach Services.

There have been no significant changes in these activities during the year

2. GENERAL INFORMATION

The financial statements of the Company were authorised for issue on 2 June 2011 by the Board of Directors.

The Company is a company limited by guarantee, not having a share capital, not for profit, incorporated and domiciled in Malaysia. Currently, the Company has 2 members. In the event that the Company is wound up, a member or a person who was a member twelve months prior to that event is liable to contribute to the assets of the Company a sum not exceeding Ringgit Malaysia One Hundred (RM100).

The Company acts as an agency under Ministry of Science, Technology and Innovation ("MOSTI").

The address of the registered office is located at Level 8, Block A, Mines Waterfront Business Park, No. 3, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan.

The principal place of operations is located at Level 4, Block C, Mines Waterfront Business Park, No. 3, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan.

3. FINANCIAL RISK MANAGEMENT POLICIES

The Company's risk management policies seek to ensure that adequate financial resources are available for the development of its operations while managing its liquidity and credit risk

Liquidity risk

The Company practises prudent liquidity risk management to minimise the mismatch between financial assets and liabilities. Since the Company's operations are fully funded by the Government of Malaysia, the element of risk is low.

Credit risk

The Company's risk exposure is attributable to receivables in respect of trading activities which are principally conducted on cost recovery basis. As the Company is not involved in trade, the exposure to credit risk is minimal.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

4.1 Basis of preparation

The financial statements of the Company have been prepared in accordance with Financial Reporting Standards ("FRSs") and the Companies Act, 1965 in Malaysia. At the beginning of the current financial year, the Company adopted applicable new and revised FRSs and IC Interpretations which are mandatory for financial periods beginning on or after 1 January 2010 as described in Note 4.2.

The financial statements have been prepared on the historical cost basis except as disclosed in the accounting policies below.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.2 Changes in accounting policies

The accounting policies adopted are consistent with those of the previous financial year except as follows:

On 1 January 2010, the Company adopted the following new and amended FRSs and IC Interpretations mandatory for annual financial periods beginning on or after 1 January 2010, where applicable.

New and Revised FRSs and Interpretations

FRS 4	Insurance Contracts
FRS 7	Financial Instruments : Disclosures
FRS 8	Operating Segments
FRS 101	Presentation of Financial Statements (Revised)
FRS 123	Borrowing Costs (Revised)
FRS 139	Financial Instruments : Recognition and Measurement
IC Interpretation 9	Reassessment of Embedded Derivatives
IC Interpretation 10	Interim Financial Reporting and Impairment
IC Interpretation 11	FRS 2 - Group and Treasury Share Transactions
IC Interpretation 13	Customer Loyalty Programmes
IC Interpretation 14	FRS 119 - The Limit on a Defined Benefit Asset, Minimum Funding Requirements and their Interaction
TR i - 3	Presentation of Financial Statements of Islamic Financial Institutions

Amendments to FRSs and Interpretations

FRS 1	First-time Adoption of Financial Reporting Standards
FRS 2	Share-based Payment - Vesting Conditions and Cancellations
FRS 7	Financial Instruments : Disclosures
FRS 127	Consolidated and Separate Financial Statements : Cost of an Investment in a Subsidiary, Jointly Controlled Entity or Associate
FRS 132	Financial Instruments : Presentation - Puttable Financial Instruments and Obligations Arising on Liquidation
FRS 138	Intangible Assets - Additional consequential amendments arising from revised FRS 3
FRS 139	Financial Instruments : Recognition and Measurement

Amendments to FRSs Classified as "Improvement to FRSs (2009)"

FRS 5	Non-current Assets Held for Sale and Discontinued Operations - Disclosures of non-current assets (or disposal groups) classified as held for sale or discontinued operations
FRS 7	Financial Instruments : Disclosures - Presentation of finance costs
FRS 8	Operating Segments - Disclosure of information about segment assets
FRS 107	Statement of Cash Flows - Classification of expenditure on unrecognised assets
FRS 108	Accounting Policies, Changes in Accounting Estimates or Errors - Status of implementation guidance
FRS 110	Events After the Reporting Period - Dividends declared after the end of the reporting period
FRS 116	Property, Plant and Equipment - Recoverable amount; and sales of assets held for rental
FRS 117	Lease - Classification of leases of land and buildings

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.2 Changes in accounting policies (contnd)

Amendments to FRSs Classified as “Improvement to FRSs (2009)” (contnd)

FRS 118	Revenue - Costs of originating a loan; and determining whether an entity is acting as a principal or as an agent
FRS 119	Employee Benefits : <ul style="list-style-type: none">- Curtailment and negative past service cost;- Plan administration costs;- Replacement of term ‘fall due’; and- Guidance on contingent liabilities
FRS 120	Accounting for Government Grants and Disclosure of Government Assistance: <ul style="list-style-type: none">- Government loans with a below market rate of interest; and- Consistency of terminology with other FRSs
FRS 123	Borrowing Costs - Components of borrowing costs
FRS 127	Consolidated and Separate Financial Statements - Measurement of subsidiary held for sale in separate financial statements
FRS 128	Investments in Associates : <ul style="list-style-type: none">- Required disclosures when investments in associates are accounted for at fair value through profit or loss; and- Impairment of investment in associate
FRS 129	Financial Reporting in Hyperinflationary Economies : <ul style="list-style-type: none">- Description of measurement basis in financial statements; and- Consistency of terminology with other FRSs
FRS 131	Interests in Joint Ventures - Required disclosures when interests in jointly controlled entities are accounted for at fair value through profit or loss
FRS 134	Interim Financial Reporting - Earnings per share disclosures in interim financial reports
FRS 136	Impairment of Assets : <ul style="list-style-type: none">- Disclosure of estimates used to determine recoverable amount; and- Unit of accounting for goodwill impairment test
FRS 138	Intangible Assets : <ul style="list-style-type: none">- Advertising and promotional activities;- Unit of production method of amortisation; and- Measuring the fair value of an intangible asset acquired in a business combination
FRS 140	Investment Property : <ul style="list-style-type: none">- Property under construction or development for future use as investment property;- Consistency of terminology with FRS 108; and- Investment property held under lease

The adoption of the above FRSs and IC Interpretations did not result in significant changes to the Company’s accounting policies and have no significant financial impact on the amounts reported in the financial statements except as discussed below:-

FRS 101 Presentation of Financial Statements

Prior to the adoption of the revised FRS 101, the components of the financial statements presented consisted of a balance sheet, an income statement, a statement of changes in reserves, a cash flow statement and notes to the financial statements. With the adoption of the revised FRS 101, the components of the financial statements presented consist of a statement of financial position, a statement of comprehensive income, a statement of changes in reserves, a statement of cash flows and notes to the financial statements. This standard does not have any impact on the financial position and results of the Company.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.3 New FRSs and IC Interpretations issued but not yet effective

The Company has not early adopted the following FRS and IC Interpretations which have been issued by MASB but are not yet effective for this set of financial statements:

		Effective for annual periods beginning on or after
New and Revised FRSs and Interpretations		
FRS 1	First-time Adoption of Financial Reporting Standards (Revised)	1 July 2010
FRS 3	Business Combinations (Revised)	1 July 2010
FRS 127	Consolidated and Saperate Financial Statements (Revised)	1 July 2010
IC Interpretation 4	Determining whether and Arrangement contains a Lease	1 January 2011
IC Interpretation 12	Service Concession Arrangements	1 July 2010
IC Interpretation 15	Agreements for the Constructions of Real Estate	1 January 2012
IC Interpretation 16	Hedges of a Net Investment in a Foreign Operation	1 July 2010
IC Interpretation 17	Distribution of Non-cash Assets to Owners	1 July 2010
IC Interpretation 18	Transfers of Assets from Customers	1 January 2011
Amendment to FRSs and Interpretations		
FRS 1	First-time Adoption of Financial Reporting Standards - Limited Exemption from Comparative FRS 7 Disclosure for First-time Adopters	1 January 2011
FRS 2	- Additional Exemptions for First-time Adopters Share-based Payment - Group Cash-settled Share-based Payment Transactions	1 January 2011
FRS 5	Non-current Assets Held for Sale and Discontinued Operations	1 July 2010
FRS 7	- Plan to sell the controlling interest in a subsidiary Financial Instruments : Disclosures	1 January 2011
FRS 132	- Improving Disclosures about Financial Instruments Financial Instruments : Presentations	
FRS 138	- Classification of Rights Issues	1 March 2010
FRS 138	Intangible Assets - Additional consequential amendments arising from revised FRS 3	1 July 2010
IC Interpretation 9	Reassessment of Embedded Derivatives - Scope of IC Interpretation 9 and revised FRS 3	1 July 2010
Amendment to FRSs Classified as "Improvement to FRSs (2009)"		
FRS 2	Share-based Payment : Scope of FRS 2 and revised FRS 3	1 July 2010
(2010)"	Amendment to FRSs Classified as "Improvement to FRSs	1 January 2011
FRS 1	First-time Adoption of Financial Reporting Standards - Accounting policy changes in the year of adoption; - Revaluation basis as deemed cost; and - Use of deemed cost for operations subjects to rate regulation	1 January 2011
FRS 3	Business Combinations (Revised) - Measurement of non-controlling interests; and - Un-replaced and voluntarily replaced share-based payment awards	

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.3 New FRSs and IC Interpretations issued but not yet effective (contd)

Amendment to FRSs Classified as “Improvement to FRSs (2010)” (contd)

4.2 Changes in accounting policies

FRS 7	Financial Instruments : Disclosures	
	- Clarification of disclosures; and	1 January 2011
	- Transition requirements for contingent consideration from a business combination that occurred before the effective date of the revised FRS (Consequential amendments arising from Improvements to FRSs (2010) - FRS 3)	1 January 2011
FRS 101	Presentation of Financial Statements - Clarification of statement of changes in equity	1 January 2011
FRS 121	The effects of Changes in Foreign Exchange Rates	
	- Transition requirements for amendments arising as a result of FRS 127, Consolidated and Saperate Financial Statements	1 January 2011
FRS 128	Investment in Associates	1 January 2011
	- Transition requirements for amendments arising as a result of FRS 127, Consolidated and Saperate Financial Statements	
FRS 131	Interests in Joint Ventures	
	- Transition requirements for amendments arising as a result of FRS 127, Consolidated and Saperate Financial Statements	1 January 2011
FRS 132	Financial Instruments : Presentation	
	- Transition requirements for contingent consideration from a business combination that occurred before the effective date of the revised FRS (Consequential amendments arising from Improvements to FRSs (2010) - FRS 3)	1 January 2011
FRS 134	Interim Financial Reporting - Significant events and transactions	1 January 2011
FRS 139	Financial Instruments : Presentation	
	- Transition requirements for contingent consideration from a business combination that occurred before the effective date of the revised FRS (Consequential amendments arising from Improvements to FRSs (2010) - FRS 3)	1 January 2011
IC Interpretation 13	Customer Loyalty Programmes - Fair value of award credit	1 January 2011

4.4 Financial Instruments

Non-derivatives financial instruments

Non-derivatives financial instruments comprise trade and other receivables, bank balances, other payables and accruals.

A financial instrument is recognised if the Company becomes a party to the contractual provisions of the instrument. Regular way purchases or sales are purchases or sales of financial assets that require delivery of assets within the period generally established by regulation or convention in the marketplace concerned. All regular way purchases and sales of financial assets are accounted for at trade date, i.e, the date that the Company commits itself to purchase or sell the assets.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.4 Financial Instruments (contd)

Non-derivatives financial instruments

Non-derivative financial instruments are recognised initially at fair value plus, for instruments not at fair value through profit or loss, any directly attributable transaction costs. Subsequent to initial recognition and classification, non-derivative financial instruments are measured as described below.

	Available classification	Measurement rule
Financial assets	Fair value through profit or loss	Fair value with changes in fair value recognised in profit or loss
	Held-to-maturity	Amortised cost, using the effective interest method
	Loans and receivables	Amortised cost, using the effective interest method
	Available for sale	Fair value with changes in fair value recognised in other comprehensive income
Financial liabilities	Fair value through profit or loss	Fair value with changes in fair value recognised in profit or loss
	Other financial liabilities	Amortised cost, using the effective interest method

Financial assets are derecognised if the Company's contractual rights to the cash flows from the financial assets expire or if the Company transfers the financial asset to another party without retaining control or transfers substantially all the risks and rewards of the asset. On derecognition of a financial asset in its entirety, the difference between the carrying amount and the sum of the consideration received and any cumulative gain or loss that had been recognised in the statement of comprehensive income is recognised in profit or loss.

Financial liabilities are derecognised if the Company's obligations specified in the contract expire or are discharged or cancelled. When an existing financial liability is replaced by another from the same lender on substantially different terms, or the terms of an existing liability are substantially modified, such an exchange or modification is treated as a derecognition of the original liability and the recognition of a new liability and the difference in the respective carrying amount is recognised in profit or loss.

Financial assets and liabilities are offset and the net amount is presented in the statement of financial position when, and only when, the Company has a legal right to offset the amounts and intends either to settle on a net basis or to realise the asset and settle the liability simultaneously.

The Company has the following categories of non-derivative financial instruments :-

Loans and receivables

Loan and receivables are financial assets with fixed or determined payments that are not quoted in an active market. Such assets include the Company's trade and other receivables as well as cash and cash equivalents.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.4 Financial Instruments (contd)

Non-derivatives financial instruments (contd)

The Company has the following categories of non-derivative financial instruments (contd) :-

Loans and receivables (contd)

The assets are recognised initially at fair value plus any directly attributable transaction costs. Subsequent to initial recognition, loans and receivables are measured at amortised cost using the effective interest method, less any impairment losses.

Other financial liabilities

The Company's other financial liabilities include other payables and accruals.

4.5 Impairment of Assets

Financial Assets (including receivables)

A financial asset not carried at fair value through profit or loss is assessed at each reporting date to determine whether there is objective evidence that it is impaired. A financial asset is impaired if objective evidence indicates that a loss event has occurred after the initial recognition of the asset, and that the loss event had a negative effect on the estimated future cash flows of that asset that can be estimated reliably.

Objective evidence that financial assets are impaired include (although not limited to) the following event: default or delinquency by a debtor, restructuring of an amount due to the Company on terms that the Company would not consider otherwise, indications that a debtor or issuer will enter bankruptcy, and the disappearance of an active market for the security.

Financial assets are generally assessed for impairment on an individual basis. However, for certain categories of financial assets, such as trade receivables, assets that are assessed not to be impaired individually are subsequently assessed for impairment on a collective basis based on similar risk characteristics. Objective evidence of impairment for a portfolio of receivables could include the Company's past experience of collecting payments, an increase in the number of delayed payments in the portfolio past the average credit period and observable changes in national or local economic conditions that correlate with default on receivables.

An impairment loss in respect of a financial asset measured at amortised cost is calculated as the difference between its carrying amount, and the present value of the estimated future cash flows discounted at the asset's original effective interest rate. Losses are recognised in the statement of comprehensive income and reflected in an allowance account against receivables. Interest on the impaired asset continues to be recognised through the unwinding of the discount.

All impairment losses are recognised in the statement of the comprehensive income. Impairment losses in respect of the financial assets measured at amortised cost are reversed if the subsequent increase in fair value can be related objectively to an event occurring after the impairment loss was recognised.

Non-financial Assets

The carrying amounts of the Company's non-financial assets are reviewed at each reporting date to determine whether there is any indication of impairment. If any such indication exists, the assets' recoverable amounts are estimated.

The recoverable amount of asset is the greater of its value in use and its fair value less costs to sell. In assessing value in use, the estimated future cash flows are discounted to their present value using a pre-tax discount rate that reflects current market assessments of the time value of money and the risks specific to the asset.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.5 Impairment of Assets (contd)

Non-financial Assets (contd)

Impairment losses recognised in prior years are assessed at each reporting date for any indications that the loss has decreased or no longer exists. An impairment loss is reversed if there has been a change in the estimates used to determine the recoverable amount. An impairment loss is reversed to the extent that the asset's carrying amount does not exceed the carrying amount that would have been determined, net of depreciation or amortisation, if no impairment loss had been recognised. Impairment losses are recognised in the statement of comprehensive income.

4.6 Property, plant and equipment

Property, plant and equipment are stated at cost less accumulated depreciation and impairment losses, if any.

Freehold land is not depreciated. Depreciation on property, plant and equipment is calculated on a straight line basis to write down the costs of assets to their residual values over the estimated useful lives of the assets. The annual rates of depreciation used for this purpose are as follows:-

Furniture and Fittings	10%
Office Equipment	10%
IT Equipment	20%
Renovation and Improvement	10%
Motor Vehicles	10%

When property, plant and equipment is disposed, the resultant gain or loss on disposal is determined by comparing the disposal proceeds with the carrying amount and is included in the statement of comprehensive income.

Residual values and useful lives of assets are reviewed, and adjusted, if appropriate, at each balance sheet date.

4.7 Intangible Assets

This relates to computer software licences, unique software products and software development costs.

Acquired computer software licences are capitalised on the basis of the costs incurred to acquire and bring to use the specific software. These costs are amortised over their estimated useful lives, not exceeding a period of 5 years.

Costs that are directly associated with identifiable and unique software products controlled by the Company, and that will probably generate economic benefits exceeding costs beyond one year, are recognised as intangible assets and amortised over 5 years.

Computer software development costs recognised as assets are amortised over 5 years using the straight line basis.

Costs associated in maintaining computer software programmes are recognised as an expense when incurred.

4.8 Receivables

Trade receivables are stated at invoiced amount less allowance for doubtful debts. Allowance for doubtful debts is made based on estimates of possible losses which may arise from non-collection of certain receivable accounts at the end of the financial year. Bad debts are written off when identified.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.9 Provision for Liabilities

Provisions are made when the Company have a present legal or constructive obligation as a result of past events, when it is probable that an outflow of resources will be required to settle the obligation, and when a reliable estimate of the amount can be made.

4.10 Income Taxes

Income tax on the profit or loss for the year comprises current and deferred tax. Current tax is the expected amount of income taxes payable in respect of the taxable profit for the year and is measured using the tax rates that have been enacted at the balance sheet date.

Deferred tax is provided for, using the liability method, on temporary differences at the balance sheet date between the tax bases of assets and liabilities and their carrying amounts in the financial statements. In principle, deferred tax liabilities are recognised for all taxable temporary differences and deferred tax assets are recognised for all deductible temporary differences, unused tax losses and unused tax credits to the extent that it is probable that taxable profits will be available against which the deductible temporary differences, unused tax losses and unused tax credits can be utilised.

Deferred tax is measured at the tax rates that are expected to apply in the period when the asset is realised or the liability is settled, based on tax rates that have been enacted or substantially enacted at the balance sheet date.

4.11 Employee Benefits

Short term benefits

Wages, salaries and bonuses are recognised as an expense in the year in which the associated services are rendered by employees of the Company. Short term accumulating compensated absences such as paid annual leave are recognised when services are rendered by employees that increase their entitlement to future compensated absences, and short term non-accumulating compensated absences such as sick leave are recognised when the absences occur.

Defined contribution benefits

As required by law, the Company makes contributions to the Employees Provident Fund ("EPF"). The contributions are recognised as an expense in the income statement as incurred.

4.12 Income Recognition

Certification and registration, seminar and training fees, and interest income are recognised on an accruals basis.

4.13 Recognition of Grants

Development grants in respect of capital expenditure receivable from the Government of Malaysia are credited to the Government Grants Account - Development Fund. The amounts utilised are recognised in the statement of comprehensive income over the life of the tangible/intangible assets acquired by the annual transfer of an amount equal to the depreciation/amortisation charge.

Development grants received for deliverables under the RMK 9 projects are recognised in the statement of comprehensive income in the same period as the related expenses which they are

Operating grants receivable from the Government of Malaysia are credited to the Government Grants Account - Operating Fund and recognised in the statement of comprehensive income in the same period as the related expenses which they are intended to compensate. Operating grants utilised for capital expenditure are credited to the Government Grants Account - Operating Fund. The amount utilised are recognised in the statement of comprehensive income over the life of the tangible/intangible assets acquired by the annual transfer of an amount equal to the depreciation/amortisation charge.

4. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTD)

4.14 Cash and Cash Equivalents

Cash represents cash and bank balances while cash equivalents are short term, highly liquid placements that are readily convertible to cash with insignificant risks to changes in value.

4.15 Functional and Presentation Currency

Items included in the financial statements of the Company are measured using the currency of the primary economic environment in which the entity operates ("functional currency"). The financial statements are presented in Ringgit Malaysia, which is the Company's functional and presentation currency.

4.16 Contingencies

A contingent liability or asset is a possible obligation or asset that arises from past events and whose existence will be confirmed only by the occurrence or non-occurrence of uncertain future event not wholly within the control of the Company.

Contingent liabilities or assets are not recognised in the statement of financial position of the Company.

5. CRITICAL ACCOUNTING ESTIMATES AND JUDGEMENTS

The preparation of financial statements in conformity with the FRSs requires management to exercise their judgement in the process of applying the Company's accounting policies and which may have significant effects on the amounts recognised in the financial statements. It also requires the use of accounting estimates and assumptions that effected the reported amounts of assets and liabilities and disclosure of contingent asset and liabilities at the date of the financial statements and the results reported for the reporting period and that may have significant risk of causing a material adjustment to the carrying amounts of assets and liabilities within the next financial year. Although these judgements and estimates are based on the management's best knowledge of current events and actions, actual may differ.

The estimates and underlying assumptions are reviewed on an ongoing basis. Revisions to accounting estimates are recognised in the period in which the estimate is revised if the revision affects only that period, or in the period of revision and future periods if the revision affects both current and future periods.

(a) Key sources of estimation uncertainty

(i) Impairment of receivables

The Company assesses at each reporting date whether there is any objective evidence that a financial asset is impaired. To determine whether there is a objective evidence of impairment, the Company considers factors such as the probability of insolvency or significant financial difficulties of the debtor and default or significant delay in payments.

5. CRITICAL ACCOUNTING ESTIMATES AND JUDGEMENTS (CONTD)

(a) Key sources of estimation uncertainty (contd)

(i) Impairment of receivables (contd)

Where there is objective evidence of impairment, the amount and timing of future cash flows are estimated based on historical loss experience for assets with similar credit risk characteristics. The carrying amount of the Company's receivables at the reporting date is disclosed in Note 8.

(ii) Estimated Useful Lives of Property, Plant and Equipment

The Company reviews annually the estimated useful lives of property, plant and equipment based on factors such as business plans and strategies, expected level of usage and future technological developments. Future results of operations could be materially affected by changes in these estimates brought about by changes in the factors mentioned. A reduction in the estimated useful lives of property, plant and equipment would increase the recorded depreciation and decrease the net book value of property, plant and equipment.

6. PROPERTY, PLANT AND EQUIPMENT

2010	Freehold Land	Renovation & Improvement	Furniture & Fittings	IT Equipment	Office Equipment	Motor Vehicles	Total
Cost:	RM	RM	RM	RM	RM	RM	RM
At 1 January	12,582,265	5,413,613	1,436,036	8,938,520	1,928,016	776,742	31,075,192
Additions	-	547,365	118,128	4,407,663	511,481	190,351	5,774,988
As at 31 December	12,582,265	5,960,978	1,554,164	13,346,183	2,439,497	967,093	36,850,180
Accumulated Depreciation:							
At 1 January	-	912,253	259,223	2,103,267	155,804	37,016	3,467,563
Charge for the year	-	579,341	151,295	2,428,585	221,971	93,536	3,474,728
As at 31 December	-	1,491,594	410,518	4,531,852	377,775	130,552	6,942,291
Net Book Value At 31 December 2010	12,582,265	4,469,384	1,143,646	8,814,331	2,061,722	836,541	29,907,889
2009							
Cost:							
At 1 January	-	3,340,684	920,480	4,802,446	527,723	171,926	9,763,259
Additions	12,582,265	2,072,929	515,556	4,136,074	1,400,293	776,741	21,483,858
Write Off	-					(171,925)	(171,925)
As at 31 December	12,582,265	5,413,613	1,436,036	8,938,520	1,928,016	776,742	31,075,192
Accumulated Depreciation:							
At 1 January	-	498,403	153,282	674,486	65,805	10,030	1,402,006
Charge for the year	-	413,850	105,941	1,428,781	89,999	48,477	2,087,048
Elimination of write off	-	-	-	-	-	(21,491)	(21,491)
As at 31 December	-	912,253	259,223	2,103,267	155,804	37,016	3,467,563
Net Book Value At 31 December 2009	12,582,265	4,501,360	1,176,813	6,835,253	1,772,212	739,726	27,607,629

7. INTANGIBLE ASSETS

	2010	2009
	RM	RM
Cost :		
At 1 January	4,264,124	1,562,978
Addition	793,157	2,701,146
At 31 December	5,057,281	4,264,124
Accumulated amortisation		
At 1 January	918,411	332,172
Charge for the year	931,810	586,239
At 31 December	1,850,221	918,411
Carrying value at 31st December	3,207,060	3,345,713

This relates to application software acquired and used for Cyber Forensic and Customer Relations Management.

8. TRADE RECEIVABLES

	2010	2009
	RM	RM
Trade receivables (Third parties)	1,160,847	660,945
Less: Impairment loss on trade receivables	-	-
Trade receivables, net	1,160,847	660,945

The normal credit term of trade receivables is 45 days (2009:45 days). Trade receivables are recognised at their original invoice amounts which represents their fair value on initial recognition.

The ageing analysis of the Company's trade receivables is as follows:

	2010	2009
	RM	RM
Neither past due nor impaired	65,905	131,045
1 to 30 days past due not impaired	983,699	316,080
31 to 60 days past due not impaired	21,280	105,852
More than 61 days past due not impaired	89,963	107,968
	1,160,847	660,945
Impaired	-	-
	1,160,847	660,945

Receivables that are neither past due nor impaired

Trade debtors that are neither past due nor impaired are creditworthy debtors with good payment records with the Company. None of the Company's trade receivables that are neither past due nor impaired have been renegotiated during financial year.

Receivables that are past due nor impaired

The Company has trade receivables amounting to RM1,070,884 (2009: RM552,977) that are past due at the reporting date but not impaired.

9. SHORT TERM DEPOSITS WITH LICENSED BANKS

The effective weighted average interest rate of the short term deposits during the year was 1.8% (2009: 2.0%) per annum. The maturity period of the deposits range from 7 to 122 days (2009: 7 to 120 days).

10. GOVERNMENT GRANTS

	Note	2010 RM	2009 RM
Development Fund	(a)	40,234,688	51,919,199
Operating Fund	(b)	2,349	1,736,882
		40,237,037	53,656,081

(a) Development Fund

	2010 RM	2009 RM
At 1 January	51,919,199	17,140,662
Add: - Grants received from the Government of Malaysia	22,422,064	55,895,445
	74,341,263	73,036,107
Less: Transfer to Income Statement		
- Depreciation for property, plant and equipment	(2,577,072)	(1,351,485)
- Amortisation for intangible assets	(565,426)	(360,490)
- Operational expenses	(30,964,077)	(19,404,933)
	(34,106,575)	(21,116,908)
As at 31 December	40,234,688	51,919,199

This represents grants received from the Government of Malaysia for the purposes of purchasing intangible assets, property, plant and equipment and deliverables under the RMK 9 projects.

(b) Operating Fund

	2010 RM	2009 RM
At 1 January	1,736,882	961,902
Add: - Grants received from the Government of Malaysia	12,144,000	13,800,000
	13,880,882	14,761,902
Less: Transfer to Income Statement		
- Depreciation for property, plant and equipment	(897,658)	(735,563)
- Amortisation for intangible assets	(366,385)	(225,749)
- Operational expenses	(12,614,490)	(12,063,708)
	(13,878,533)	(13,025,020)
As at 31 December	2,349	1,736,882

This represents grants received from the Government of Malaysia for the purposes of financing the Company's daily operations and acquiring intangible assets, property, plant and equipment.

11. TAXATION

The effective weighted average interest rate of the short term deposits during the year was 1.8% (2009: 2.0%) per annum.

	2010 RM	2009 RM
Tax charge for the year	50,914	355,827

11. TAXATION (CONTD)

The Company is incorporated as a non-profit company limited by guarantee and is fully funded by grants from the Government of Malaysia. The Company was granted a 100% tax exemption on statutory income except for dividend for a period of 3 years pursuant to Paragraph 5 and 6 Schedule 7A of the Income Tax Act 1967 effective from 2006 to 2008.

With effect from the current year, the Company is subject to Income Tax Order (Exemption) (No.22) 2006 wherein only grants/subsidies are tax exempt.

The reconciliation between tax applicable to profit before tax and current year's tax expense is as follows:

	2010 RM	2009 RM
Surplus/(deficit) before tax	(17,184)	1,423,310
Tax calculated at statutory tax rate of 25% (2009: 25%)	(4,296)	355,827
· expenses financed by grants which are disallowed for deductions	47,938,490	34,141,928
· government grants which are tax exempt	(47,985,108)	(34,141,928)
Tax expense	(50,914)	355,827

12. INCOME FROM GRANTS

	2010 RM	2009 RM
Development fund (Note 10(a))	34,106,575	21,116,908
Operating fund (Note 10(b))	13,878,533	13,025,020
	47,985,108	34,141,928

13. OPERATING REVENUE

This represents certification and registration and seminar and training fees.

14. OTHER INCOME

	2010 RM	2009 RM
Tender and documentation fees	3,900	10,450
Gain/(loss) or foreign exchange	6,371	(14,736)
Interest income	203,653	176,909
	213,924	172,623

15. (DEFICIT)/SURPLUS OF INCOME BEFORE TAXATION

This is stated after charging:-

(a) Audit fees	15,000	15,000
Depreciation of property, plant and equipment	3,474,728	2,087,048
Amortisation of intangible assets	931,810	586,239

15. (DEFICIT)/SURPLUS OF INCOME BEFORE TAXATION (CONTD)

	2010 RM	2009 RM
Rental		
- Office Space	2,985,886	2,331,962
- Motor Vehicles	204,328	171,323
- Space area, hall and room	101,978	402,125
- Office equipments	269,994	140,964
- Parking lot	274,892	242,675
- Others	486,607	416,303
Director's emoluments		
- Director's remuneration	450,349	310,789
- Director's fees	90,599	52,499
b) Employees benefit cost	21,399,354	14,664,163

The employees benefit costs excludes director's emoluments and includes contribution to the Employees Provident Fund of RM2,275,312 (2009: RM1,301,798).

16. CONTINGENT LIABILITIES

In June 2010, Mohamad Jabir Bin Aman (trading as Kusuba Enterprise) filled a summons against the Company for having failed to pay to Kusuba Enterprise claimed that they have successfully carried out and completed the agreed services.

The date for the trial has not been determined yet.

17. FAIR VALUE OF FINANCIAL INSTRUMENTS

The following are classes of financial instruments that are not carried at fair value. However, in view of the short term nature of these instruments, their respective carrying amounts approximate their fair value.

	Note
Trade receivables	8
Other receivables	-
other payables and accruals	-

STATEMENT BY DIRECTORS

We, JEN DATO' SERI PANGLIMA MOHD AZUMI BIN MOHAMED (RETIRED) and LT COL DATO' HUSIN BIN JAZRI (RETIRED), being two of the Directors of CYBERSECURITY MALAYSIA , do hereby state that in the opinion of the directors, the financial statements set out on pages 4 to 24 are drawn up in accordance with the Financial Reporting Standards and the provisions of the Companies Act, 1965 in Malaysia so as to give a true and fair view of the state of affairs of the Company as at 31 December 2010 and of its results and cash flows for the year ended on that date.

In accordance with a resolution of the Board of Directors dated



GENERAL TAN SRI DATO' SERI PANGLIMA MOHD AZUMI BIN MOHAMED (RETIRED)



YBHG. LT COL DATO' PROF. HUSIN BIN JAZRI (RETIRED)

Kuala Lumpur,
Date: 2 June 2011

STATUTORY DECLARATION

I, LT COL HUSIN BIN JAZRI (RETIRED), the director primarily responsible for the financial management of CYBERSECURITY MALAYSIA, do solemnly and sincerely declare that the financial statements set out on pages 4 to 24 are in my opinion correct and I make this solemn declaration conscientiously believing the same to be true, and by virtue of the provisions of the Statutory Declarations Act, 1960.



YBHG. LT COL DATO' PROF. HUSIN BIN JAZRI (RETIRED)

Subscribed and solemnly declared by the abovenamed YBHG. LT COL DATO' PROF. HUSIN BIN JAZRI (RETIRED) at Kuala Lumpur on 2 June 2011

Before me,

COMMISSIONER FOR OATHS



LG 4.2, Wisma KWSG,
Jalan Kampung Attap,
50460 Kuala Lumpur

**INDEPENDENT AUDITORS' REPORT TO THE MEMBERS OF
CYBERSECURITY MALAYSIA**
(Company No.: 726630-U)

Report on the Financial Statements

We have audited the financial statements of CyberSecurity Malaysia, which comprise the statement of financial position as at 31 December 2010, and the statement of comprehensive income, statement of changes in reserves and statement of cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information, as set out on pages 4 to 24.

Directors' Responsibility for the Financial Statements

The Directors of the Company are responsible for the preparation of financial statements that give a true and fair view in accordance with Financial Reporting Standards and the Companies Act, 1965 in Malaysia, and for such internal control as the Directors determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with approved standards on auditing in Malaysia. Those standards require that we comply with ethical requirements and plan and perform the audit to obtain reasonable assurance whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on our judgement, including the assessment of risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, we consider internal controls relevant to the Company's preparation of financial statements that give a true and fair view in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Company's internal controls. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by the Directors, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements have been properly drawn up in accordance with Financial Reporting Standards and the Companies Act, 1965 in Malaysia so as to give a true and fair view of the financial position of the Company at 31 December 2010 and of its financial performance and cash flows for the year then ended.

Report on Other Legal and Regulatory Requirements

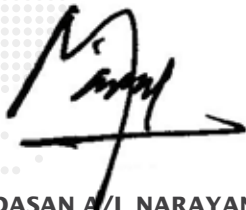
In accordance with the requirements of the Companies Act, 1965 in Malaysia, we also report that in our opinion the accounting and other records and the registers required by the Act to be kept by the Company have been properly kept in accordance with the provisions of the Act.

Other Matters

This report is made solely to the members of the Company, as a body, in accordance with Section 174 of the Companies Act, 1965 in Malaysia and for no other purpose. We do not assume responsibility to any other person for the content of this report.



AZMAN, WONG, SALLEH & CO
AF: 0012
Chartered Accountants



SIVADASAN A/L NARAYANAN NAIR
1420/12/11(J)
Chartered Accountant

Kuala Lumpur,
Date: 2 June 2011

Information Security and Organizational Continuity Management



Worthy Investment for Prevention

Editorial Committee

Advisor : Zahri Hj. Yunos
Chief Operating Officer

1. Mohd. Shamil Mohd Yusoff
Head, Corporate Branding & Media Relations
2. Sandra Isnaji
Manager, Corporate Branding & Media Relations
3. Zul Akmal Manan
Executive, Corporate Branding & Media Relations
4. Zaihasrul Ariffin
Graphic Designer, Secure Technology Services
5. Mohd Haffezal Md Yahaya
Graphic Designer, Secure Technology Services
6. Nurul 'Ain Zakariah
Graphic Designer, Secure Technology Services
7. Azlin Samsudin
Executive, Legal and Secretarial
8. Abd. Rouf Mohammed Sayuti
Head, Internal Audit
9. Arbain Sahir
Executive, Procurement and Logistic
10. Azman bin Ismail
Head, Finance
11. Mohd Sharizuan Mohd Omar
Photography Club

(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.



An agency under MOSTI



Corporate Office:

CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my