CyberSecurity MALAYSIA

Securing Our Cyberspace

LAPORAN TAHUNAN | ANNUAL REPORT

2009

Setting the stage for Malaysians to be global citizens

Malaysians are increasingly living as 'global citizens' in a borderless world shaped and driven by the power of the internet. Many individuals already work, play and live as much - if not more so - in cyberspace as they do in their physical environments. Indeed, Malaysians are going online at a younger age. Many do so before they even learn how to ride a bicycle. The pace at which cyber technology is evolving will continue to transform the way we do business, entertain ourselves and interact with others. That we can do so with confidence rests on the capability and capacity of applications to secure and protect transactions and communications over cyberspace. On this score, cyber security is indispensable in transforming Malaysians into global citizens.

Menyediakan pentas bagi rakyat Malaysia untuk menjadi warga global

Rakyat Malaysia kian menjalani kehidupan sebagai 'warga global' di dunia tanpa batas yang dibentuk dan digerakkan oleh kekuatan internet. Ramai individu telah pun bekerja, bermain dan menjalani kehidupan di alam siber sebagaimana – atau mungkin lebih lagi daripada - yang mereka lakukan di dalam persekitaran fizikal mereka. Memang benar, semakin ramai rakyat Malaysia melayari alam siber di usia muda. Bahkan ramai yang melakukannya sebelum mereka belajar menunggang basikal. Kelajuan perkembangan teknologi siber akan terus mengubah cara kita menjalankan perniagaan, berhibur dan berinteraksi dengan satu sama lain. Ini kita lakukan dengan keyakinan yang diletakkan di atas kemampuan dan keupayaan aplikasi-aplikasi untuk memperolehi dan melindungi transaksi dan komunikasi di alam siber. Dalam skor ini, keselamatan siber sangat diperlukan untuk mengubah rakyat Malaysia menjadi warga global.

Contents Kandungan

Notice of the Fourth Annual General Meeting

Notice of Annual General Meeting

NOTICE IS HEREBY GIVEN THAT the Fourth 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 22 June 2010 to transact the following businesses:-

AS ORDINARY BUSINESS

1.	To receive the Audited Financial Statements for the financial year ended 31 December 2009 together with the Reports of the Directors and Auditors thereon;	Resolution 1
2.	To re-elect YBhg. Datuk Abang Abdul Wahap bin Abg Julai and YBhg. Datuk Dr Abdul Raman bin Saad who retires by rotation pursuant to Articles 49 and 51 of the Company's Articles of Association and who, being eligible, offer themselves for re-election;	Resolution 2
3.	To-reappoint Messrs Azman, Wong & Salleh as Auditors of the Company and to authorize the Directors to fix their remuneration;	Resolution 3

AS SPECIAL BUSINESS
To consider and, if thought fit, pass the following resolution:

4.	To approve the payment of the Directors' accumulated monthly allowances for the financial year ended 31 December 2009.	Resolution 4

BY ORDER OF THE BOARD

JAILANY BIN JAAFAR (LS8843)
Company Secretary

Selangor
01 June 2010

NOTES:
1. A proxy need not be a member of the CyberSecurity Malaysia PROVIDED that a member shall not be entitled to appoint a person who is not a member as his proxy unless that person is an advocate, an approved company auditor or a person approved by the Registrar of Companies.
2. The instrument appointing a proxy shall be in writing under the hand of the appointor or his attorney duly authorised in writing or if the appointor is a body corporate, either under seal or under hand of the officer or attorney duly authorised.
3. To be valid the proxy 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.

Notis Mesyuarat Agung Tahunan Keempat

Notis Mesyuarat Agung Tahunan

DENGAN INI DIBERITAHU BAHAWA Mesyuarat Agung Tahunan Keempat CYBERSERCURITY MALAYSIA akan diadakan selaras dengan Resolusi Pekeliling Ahli menurut Akta 20 Tataurusan Pertubuhan Syarikat pada atau sebelum 22 Jun 2010 untuk melaksanakan urusan-urusan berikut:

SEBAGAI URUSAN BIASA

1.	Untuk menerima Penyata Kewangan Telah Diaudit bagi tahun kewangan berakhir 31 Disember 2009 dan Laporan Pengarah dan Juruaudit mengenainya;	Resolusi 1
2.	Untuk memilih semula YBhg. Datuk Abang Abdul Wahap bin Abg Julai dan YBhg. Datuk Dr Abdul Raman bin Saad yang bersara mengikut giliran menurut Tataurusan 49 dan 51 Tataurusan Pertubuhan Syarikat dan, oleh kerana layak, menawarkan mereka untuk pemilihan semula;	Resolusi 2
3.	Untuk melantik semula Tetuan Azman, Wong & Salleh sebagai Juruaudit Syarikat dan membenarkan Pengarah-Pengarah untuk menetapkan imbuhan mereka;	Resolusi 3

SEBAGAI URUSAN KHAS
Untuk mempertimbangkan dan, jika difikirkan sesuai, meluluskan Resolusi Biasa berikut:

4.	Untuk meluluskan pembayaran Elaun Bulanan Terkumpul Pengarah bagi tahun kewangan berakhir 31 Disember 2009.	Resolusi 4

ATAS ARAHAN LEMBAGA

JAILANY BIN JAAFAR (LS8843)
Setiausaha Syarikat

Selangor
01 Jun 2010

NOTA:
1. Seorang proksi tidak semestinya ahli CyberSecurity Malaysia dengan SYARAT bahawa seseorang ahli hendaklah tidak layak untuk melantik seseorang yang bukan ahli sebagai proksi beliau melainkan individu tersebut adalah seorang peguam, seorang juruaudit syarikat yang diluluskan atau seorang individu yang telah diluluskan oleh Pendaftar Syarikat.
2. Suratcara pelantikan proksi hendaklah secara bertulis dengan ditandatangani oleh pelantik atau peguam beliau yang telah diberi kuasa sewajarnya secara bertulis atau jika pelantik tersebut merupakan sebuah badan korporat, sama ada di bawah meterai atau tandatangan pegawai atau peguam yang telah diberi kuasa sewajarnya.
3. Borang proksi yang telah dilengkapkan sewajarnya mestilah dihantar ke Pejabat Berdaftar CyberSecurity Malaysia di Aras 8, Blok A, Mines Waterfront Business Park, No. 3, Jalan Tasik, The Mines Resort City, Seri Kembangan 43300 Selangor Darul Ehsan, Malaysia tidak lewat dari empat puluh lapan (48) jam sebelum masa untuk mesyuarat diadakan.

Our Direction Halatuju Kami

Vision / Visi

To be a Globally Recognised, National Cyber Security Reference and Specialist Centre by 2020
Untuk Menjadi Sebuah Pusat Rujukan dan Pakar Keselamatan Siber Nasional Yang Diiktiraf di Peringkat Global Menjelang 2020

Mission / Misi

Creating and Sustaining a Safer Cyberspace to Promote National Sustainability, Social Well-Being and Wealth Creation
Mewujud dan Mengekalkan Alam Siber yang Lebih Selamat bagi Menggalakkan Kemapanan, Kemakmuran Sosial dan Penciptaan Kekayaan Negara

Key Result Areas (KRA) / Bidang Keberhasilan Utama

- National Cyber Security Enhancement
  Peningkatan Keselamatan Siber Nasional
- National Cyber Security Capability & Capacity Building
  Pembinaan Keupayaan Keselamatan Siber & Pembangunan Kapasiti Nasional
- International Cooperation & Recognition
  Kerjasama dan pengiktirafan di peringkat antarabangsa
- Financial Management & Accountability
  Pengurusan Kewangan dan Kepertanggungjawaban
- Quality Service Delivery
  Penyerahan Perkhidmatan Berkualiti
- Learning Organisation
  Peningkatan tahap pengetahuan dan pembelajaran organisasi
- Branding
  Penjenamaan

Strategic Goals / Matlamat Strategik

- To increase trust and confidence in using indigenous products and expertise
  Mengukuhkan kepercayaan dan keyakinan untuk menggunakan pelbagai produk dan kepakaran tempatan
- To obtain adequate funding and effectively use them to meet core objectives
  Mendapatkan dana yang mencukupi dan menggunakannya secara efektif untuk mencapai objektif teras.
- To strengthen the position of Malaysia globally in cyber security
  Memantapkan kedudukan Malaysia di persada keselamatan siber dunia
- To increase public awareness of our specialised cyber services
  Menambahkan kesedaran orang ramai terhadap perkhidmatan siber khas kami
- To ensure adequate number of cyber security professionals
  Memastikan bilangan profesional keselamatan siber yang mencukupi
- To enhance the state of cyber security readiness of the nation
  Meningkatkan tahap kesediaan keselamatan siber negara
- To raise national awareness in cyber security
  Meningkatkan kesedaran keselamatan siber nasional
- To promote empowered work teams with positive attitude, innovative workforce and strong teamwork
  Menggalakkan pengwujudan pasukan kerja yang bersikap positif, tenaga kerja yang berinovasi dan semangat berpasukan yang teguh
- To improve customer satisfaction
  Memperbaiki tahap kepuasan pelanggan

What We Believe In

Our Core Values are being a Trusted, Impartial, and Proactive Specialist Service Provider in Cyber Security.

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.

Keyakinan Kami

Nilai Teras Kami adalah untuk Menjadi Penyedia Perkhidmatan Pakar dalam Keselamatan Siber Yang Dipercayai, Saksama dan Proaktif

Dipercayai
Mengekalkan kelaziman sosial, etika dan organisasi; mematuhi kod tatalaku dan prinsip-prinsip etika profesional.

Saksama
Memberikan pertimbangan, nasihat dan membuat keputusan berdasarkan kepada ciri-ciri profesionalisma yang tinggi, tidak berat sebelah dan berdasarkan kepada fakta serta rasional yang jelas; sentiasa mengelakkan sebarang kepentingan peribadi atau konflik kepentingan.

Proaktif
Mengambil tindakan segera untuk menyelesaikan objektif; menjangka cabaran dan mengenalpasti penyelesaian; mengambil tindakanuntuk mencapai matlamat mengatasi apa yang diperlukan.

How We Got Here Langkah Kami

2006
7 April 2006
To address the growing cyber threats in critical areas, the National Information Technology Council (NITC) Meeting 1/2006 agreed that the National Cyber Security Policy (NCSP) be adopted, with NISER to begin the transformation process to become the Malaysian Cyber Security Centre and given the additional mandate to assist the government in implementing the NCSP.

Bagi menangani ancaman siber yang semakin membimbangkan di bidang-bidang kritikal, Mesyuarat Majlis Teknologi Maklumat (NITC) 1/2006 bersetuju bahawa Dasar Keselamatan Siber Nasional (NCSP) perlu diterima pakai, dengan NISER memulakan proses transformasi untuk menjadi Pusat Keselamatan Siber Malaysia dan diberi mandat tambahan untuk membantu kerajaan melaksanakan NCSP.

2005
28 September 2005
As part of MIMOS Berhad's rationalisation exercise, the Malaysian Cabinet decided for NISER to be separated from MIMOS, and established as a Company Limited by Guarantee, owned by the Government of Malaysia, under the purview of MOSTI.

Sebagai sebahagian daripada langkah rasionalisasi MIMOS Berhad, Kabinet Malaysia telah memutuskan supaya NISER diasingkan daripada MIMOS, dan beroperasi sebagai sebuah Syarikat Berhad mengikut Jaminan, yang dimiliki oleh Kerajaan Malaysia, di bawah kawal selia MOSTI.

2001
10 April 2001
NISER was officiated by the then Deputy Minister YAB Dato' Seri Abdullah Ahmad Badawi.

NISER telah dirasmikan oleh Timbalan Perdana Menteri ketika itu, YAB Dato' Seri Abdullah Ahmad Badawi.

1998
24 January 1998
National ICT Security and Emergency Response Centre (NISER) was born when the National IT Council (NITC) directed an agency to be formed to address ICT security issues in Malaysia. MyCERT became part of NISER.

Pusat Keselamatan dan Tindak balas Kecemasan ICT Negara (NISER) telah lahir apabila Majlis IT Negara (NITC) mengarahkan sebuah agensi dibentuk bagi menangani isu keselamatan ICT di Malaysia. MyCERT menjadi sebahagian daripada NISER.

1997
13 January 1997
The Malaysia Computer Emergency Response Team (MyCERT) was established to address computer security issues amongt Malaysian internet user.

Pasukan Tindak balas Kecemasan Komputer Malaysia (MyCERT) ditubuhkan untuk menangani isu keselamatan komputer di kalangan pengguna internet Malaysia.

2007

30 March 2007

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

NISER secara rasmi diberi nama baru sebagai CyberSecurity Malaysia dan didaftar dengan Suruhanjaya Syarikat Malaysia (SSM).

20 August 2007

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

CyberSecurity Malaysia telah dilancarkan secara rasmi oleh Perdana Menteri Malaysia semasa Mesyuarat NITC 1/2007 di Cyberjaya.

2008

25 July 2008

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

CyberSecurity Malaysia telah mendapat pensijilan ISO/IEC 27001:2005 iaitu standard Pengurusan Keselamatan Sistem Maklumat (ISMS).

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).

Kerajaan telah melantik CyberSecurity Malaysia sebagai Badan Persijilan tunggal untuk skim penilaian and persijilan berasaskan kepada MS ISO/IEC 15408:2005 Teknologi Maklumat – Teknik Keselamatan – Kriteria Penilaian Bagi Keselamatan IT. Badan Persijilan ini dikenali sebagai Badan Persijilan Kriteria Bersama Malaysia (MyCB).

2009

2 November 2009

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

Perkhidmatan CyberSecurity Malaysia telah diperluaskan dengan pelancaran Pejabat Baru Wilayah Utara di 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.

CyberSecurity Malaysia telah melancarkan Pusat Bantuan Cyber999 di Pusat Konvensyen Kuala Lumpur bersempena dengan acara Cyber Security Malaysia || SecureAsia@ KL . Pusat Bantuan Cyber999 adalah perkhidmatan yang ditawarkan oleh CyberSecurity Malaysia untuk menangani isu keselamatan atau insiden yang dihadapi pengguna komputer dan internet.

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.

CyberSecurity Malaysia telah melancarkan Pusat Penyelidikan Malware di Hotel Royale Chulan, Kuala Lumpur bersempena dengan acara Hari Keselamatan Komputer Sedunia. Pusat ini dibina untuk mengendalikan penyelidikan dan pembangunan dalam mengurangkan ancaman malware, serta menyediakan maklumat mengenai ancaman yang akan muncul kepada pihak yang berkepentingan.

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 everthing that we do.

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

SERVICE, QUALITY and RELATIONSHIPS.

SERVICE

In delivering our service to you, we adopt values that inform 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 ensuring 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.

RELATIONSHIPS

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.

Piagam Pelanggan

Janji Kami Kepada Anda

Visi kami adalah untuk menjadi Pusat Rujukan Keselamatan Siber Kebangsaan yang diiktiraf di persada antarabangsa dan menjadi Pusat Kecemerlangan Kepakaran menjelang tahun 2020.

Untuk menjadi impian ini satu realiti, kami berhasrat untuk menjadikan anda, Pelanggan Kami, sebagai keutamaan di dalam setiap aktiviti kami.

Kami berhasrat untuk melaksanakannya dengan memberikan tumpuan kepada tiga bidang yang penting iaitu: **PERKHIDMATAN, KUALITI dan PERHUBUNGAN.**

PERKHIDMATAN

Semasa menyampaikan perkhidmatan kepada anda, kami akan menerapkan nilai-nilai berinformasi berkaitan dengan kaedah tatakerja kami dan akan sentiasa memastikan tahap profesionalisma diaplikasikan semana kami melaksanakan tugasan tersebut.

Kami berinovasi
Kami memastikan bahawa satu kaedah penyelesaian tidak semestinya sesuai bagi semnua permasalahan. Setiap organisasi mempunyai permasalahannya sendiri yang unik, oleh itu kami sentiasa bersikap praktikal dan inovatif apabila menyelesaikan sebarang permasalahan yang berciri peribadi khusus kepada anda.

Kami proaktif
Kami sentiasa mengambil inisiatif untuk berfikiran maju ke hadapan dan progresif apabila menangani permasalahan semasa melaksanakan tugasan, kerana kami mengetahui bahawa di dalam industri ini, hanya inilah prinsip pelaksanaan tugasan yang diterima.

Kami bersedia untuk bertindak
Sesuai dengan matlamat kami untuk menjadikan ruang siber anda selamat dan terlindung, kami memastikan bahawa kami sentiasa bersedia untuk menangani sebarang permasalahan, tidak kira bagaimana sukar dan kompleks, di dalam pelbagai keadaan dan tidak kira siapa pun yang memanggil.

KUALITI

Kami sentiasa berusaha untuk mencapai tahap yang lebih tinggi di dalam penyampaian mutu perkhidmatan kami, kerana kami memahami bahawa ini sahaja caranya untuk sentiasa menjadi yang terunggul di dalam industri ini.

Kami adil
Tidak kira bagaimana besar atau kecil sesuatu permasalahan itu, kami akan menanganinya dengan adil. Kami akan memberikan sokongan secara adil dan saksama, memberikan khidmat nasihat dan informasi tanpa diskriminasi atau prejudis.

Kami pakar
Kami memastikan anda mendapat manfaat yang maksimum semasa berurusan, kerana kami pakar di dalam bidang ini, jadi anda pastinya tidak akan dipesongkan oleh isu-isu yang boleh menggugat prestasi kami.

Kami cekap
Demi memastikan dan mengekalkan tahap perkhidmatan yang terbaik untuk anda, kami sentiasa berusaha untuk menyampaikan maklumat dan nasihat secara tepat dan memberikan perkhidmatan yang dipercayai pada setiap masa.

PERHUBUNGAN

Di sebalik dunia teknikal di mana kami beroperasi, salah satu faktor yang menjadi tunggak kejayaan kami ialah Perhubungan dan Ikatan yang terjalin di antara kami dengan pelanggan dan ke semua warga kerja CyberSecurity Malaysia. Ianya merupakan teras yang memacu kami ke arah kejayaan.

Kami bekerjasama
Setiap seorang daripada warga kerja kami memainkan peranan di dalam menangani permasalahan anda. Kami berkongsi kemahiran dan pengalaman agar anda dapat menikmatan faedah daripada kepakaran yang kami miliki.

Kami menjiwai
Kami berbangga dengan tugasan yang kami lakukan dan kerjasama yang kami hulurkan kepada pelanggan. Dengan usahasama yang padu kami yakin akan berupaya untuk menjamin keselamatan ruangan siber negara kita.

Kami boleh dipercayai
Segala aktiviti kami bermatlamatkan kepada anda. Kami berada di sini untuk menjamin keselamatan dan kepentingan anda dan orang ramai. Di dalam melaksanakan matlamat ini, kami berharap agar anda boleh memberikan sepenuh kepercayaan dan keyakinan kepada kami.

Message by the Minister of Science, Technology & Innovation

Malaysia under Prime Minister YAB Dato' Sri Mohd Najib Tun Haji Abdul Razak has outlined the way forward with a New Economic Model (NEM) to transform a resource-led and efficiency-driven economy into a knowledge-based and innovation-led economy.

Under the NEM, Malaysia will build its engines of growth around high value industries and key sectors that have the scale and power to lift the nation from a middle-income to a high-income economy. At the same time, this platform for growth also seeks to develop a well-balanced society that enjoys a high quality of life.

Information and communication technologies (ICT) form one of the pillars to support these aspirations as it has the potential to drive the economy up the value chain - first as an industry on its own, and second, as an enabler that can raise the productivity and competitiveness of other industries.

In this regard, cyber security plays a critical role by ensuring the integrity of the online exchange of information and communication that has become such a pervasive and indispensible aspect of our lives.

It is through the assurance of cyber security that we can build and sustain a culture of innovation among the ICT players as well as other industries. It is also through the protective net provided by cyber security that we can maintain the values essential to the spiritual and moral development of our next generation.

Indeed, the success of CyberSecurity Malaysia in performing its role is one of the reasons behind the growth of MSC Malaysia within our borders and its current aspirations to export Made-in-Malaysia ICT products and services overseas.

I am confident that CyberSecurity Malaysia will continue to overcome all future challenges in securing our cyberspace for the nation and its people.

YB Datuk Seri Dr. Maximus Johnity Ongkili, JP
Minister of Science, Technology and Innovation

Kata Aluan daripada Menteri Sains, Teknologi dan Inovasi

Malaysia di bawah kepimpinan Perdana Menteri YAB Dato' Sri Mohd Najib Tun Haji Abdul Razak, telah menggariskan hala tuju Negara melalui pembentukan Model Ekonomi Baru (MEB) bagi mengubah ekonomi yang berasaskan sumber dan kecekapan kepada ekonomi berasaskan pengetahuan dan inovasi.

Di bawah MEB, Malaysia akan membina jentera-jentera pertumbuhan di sekitar industri yang bernilai tinggi dan sektor-sektor utama yang mempunyai skala dan kekuatan untuk mengangkat negara daripada ekonomi berpendapatan pertengahan kepada berpendapatan tinggi. Pada masa yang sama, platform pertumbuhan ini turut mensasarkan pembangunan masyarakat seimbang yang menikmati kualiti kehidupan yang tinggi.

Teknologi Maklumat dan Komunikasi atau ICT membentuk salah satu tiang untuk menyokong aspirasi ini kerana ianya mempunyai potensi untuk memacu ekonomi dalam rangkaian yang lebih tinggi – pertama di dalam industrinya sendiri, dan kedua, sebagai penggerak yang boleh meningkatkan produkitiviti serta daya saing industri lain.

Sehubungan dengan itu, keselamatan siber memainkan peranan yang penting dalam memastikan integriti penukaran informasi dan komunikasi dalam talian yang kini kian pesat dan amat diperlukan di dalam kehidupan kita.

Melalui jaminan keselamatan siber, kita boleh membina dan mengekalkan suatu budaya inovasi di kalangan pemain ICT dan industri yang lain. Melalui perlindungan jaringan yang diberikan oleh keselamatan siber jugalah kita dapat mengekalkan nilai-nilai yang diperlukan untuk pembangunan kerohanian dan moral generasi di masa hadapan.

Sesungguhnya, kejayaan CyberSecurity Malaysia memainkan peranannya di sebalik perkembangan MSC Malaysia di dalam persempadanan kita serta aspirasi terkini bagi mengekspot produk-produk dan perkhidmatan-perkhidmatan ICT "Buatan Malaysia".

Saya yakin, CyberSecurity Malaysia akan terus mengatasi segala cabaran yang mendatang di dalam melindungi ruang siber kita untuk Negara serta rakyatnya.

YB Datuk Seri Dr. Maximus Johnity Ongkili, JP
Menteri Sains, Teknologi dan Inovasi

Message by the Deputy Minister of Science, Technology and Innovation

Let me take this opportunity to congratulate CyberSecurity Malaysia on its many successes and achievements both at the national and international levels. Indeed, I am proud to say that the agency under the Ministry of Science, Technology and Innovation has come a long way since its incorporation in 2007.

Let me also say that it is no exaggeration that CyberSecurity Malaysia is regarded as an unsung hero in the development of the nation's online culture. Without CyberSecurity Malaysia, we would not be among the leading countries in terms of internet usage and development of the ICT industry.

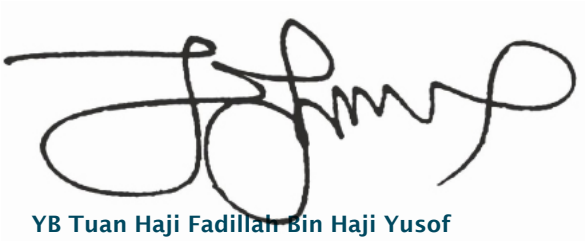
On this score, it is heartening to note that we are ranked among the top 20 nations for cyber security by the Vienna-based Institute of Management Development (IMD), ranking higher than developed countries such as the United States, United Kingdom, Norway and emerging economies like China and India.

It is noteworthy that we are recognised as a leader in our field by the member nations of the Organisation of Islamic Conference (OIC) and it is for this reason that we are currently the Chair of the OIC Computer Emergency Response Team (OIC-CERT).

I would also like to congratulate CyberSecurity Malaysia for the successful launch of the Cyber999 Help Centre as the nation's firewall against cyber threats as well as the CyberSecurity Malaysia Malware Research Centre.

I am gratified to note that Malaysian companies and individuals are extensively using CyberSecurity Malaysia's other services to support their growth and development which includes the Malaysian Common Criteria Certification and Malaysian ICT Security Evaluation Facilities (MySEF).

On behalf of the Ministry, I would like to thank the management and staff of CyberSecurity Malaysia for their services and support in our nation building process.



YB Tuan Haji Fadillah Bin Haji Yusof
Deputy Minister of Science, Technology and Innovation

Kata Aluan daripada Timbalan Menteri Sains, Teknologi dan Inovasi

Saya ingin mengambil kesempatan ini untuk mengucapkan tahniah kepada CyberSecurity Malaysia di atas kejayaan dan pencapaiannya sama ada di peringkat kebangsaan dan juga antarabangsa. Sesungguhnya, saya berbangga melihat pencapaian agensi di bawah Kementerian Sains, Teknologi dan Inovasi ini yang telah berkembang jauh semenjak penubuhannya pada 2007.

Saya juga ingin menyatakan bahawa anggapan CyberSecurity Malaysia sebagai perwira di dalam membangunkan budaya dalam talian di Negara ini bukanlah sesuatu yang harus di pandang rendah. Tanpa Cybersecurity Malaysia, kita tidak akan menjadi di antara Negara utama dunia dari segi penggunaan internet serta perkembangan industri ICT.

Dalam pada itu, kita berbangga kerana Malaysia telah diletakkan di antara 20 Negara teratas di bidang keselamatan siber oleh Institute of Management Development (IMD) yang beribu pejabat di Vienna, Austria, di mana kita telah berada pada kedudukan yang lebih tinggi berbanding negara-negara seperti Amerika Syarikat, United Kingdom, Norway dan Negara-negara kebangkitan ekonomi seperti Cina dan India.

Kami berbangga melalui CyberSecrurity Malaysia, Malaysia turut diiktiraf sebagai pemimpin di dalam bidang keselamatan siber oleh ahli-ahli Pertubuhan Persidangan Negara Islam (OIC) dan disebabkan oleh pengiktirafan ini juga maka Malaysia kini merupakan Pengerusi kepada Pasukan Tindak balas Kecemasan Komputer OIC (OIC-CERT).

Saya juga ingin mengucapkan tahniah kepada CyberSecurity Malaysia di atas kejayaan pelancaran Pusat Bantuan Cyber999 sebagai penghadang Negara dari ancaman siber, dan juga Pusat Penyelidikan Malware.

Saya turut berbangga melihat syarikat-syarikat Malaysia dan individu menggunakan perkhidmatan-perkhidmatan yang disediakan oleh CyberSecurity Malaysia secara meluas di mana ianya telah menyokong pertumbuhan dan pembangunan yang merangkumi Malaysian Common Criteria Certification Body (MyCB) dan Malaysian ICT Security Evaluation Facilities (MySEF).

Bagi pihak MOSTI, saya merakamkan ucapan terima kasih kepada pengurusan serta kakitangan CyberSecurity Malaysia di atas khidmat dan sokongan yang telah diberikan di dalam proses pembangunan Negara kita.

YB Tuan Haji Fadillah Bin Haji Yusof
Timbalan Menteri Sains, Teknologi dan Inovasi

Chairman's Statement

I am pleased to report that CyberSecurity Malaysia has continued to record impressive performance in providing its core information security services to the public and private sectors in the year ending 2009.

The level of awareness on cyber threats and the need for cyber security has risen tremendously among the Government, industry and business, and the general public in the relatively short period since CyberSecurity Malaysia was officially recognised in 2007.

It is widely acknowledged that the increase in transactions and activities on the Internet has exposed Malaysians to cyber invasions and other risks. To deal with such threats, CyberSecurity Malaysia has expanded its incident response services for the public by establishing the Cyber999 Help Centre. The Cyber999 Help Centre is fully operational and has been offering its services since it was launched in July 2009 during The CyberSecurity Malaysia || SecureAsia @ Kuala Lumpur 2009 Conference & Exhibition.

Kenyataan Pengerusi

Dengan sukacitanya saya ingin memaklumkan bahawa CyberSecurity Malaysia berjaya meneruskan rekod prestasi yang memberangsangkan dalam menyediakan teras perkhidmatan keselamatan maklumat kepada sektor awam dan swasta bagi tahun berakhir 2009.

Tahap kesedaran terhadap ancaman siber dan keperluan memiliki keselamatan siber menunjukkan peningkatan ketara di kalangan sektor kerajaan, industri dan perniagaan serta masyarakat umum sejak CyberSecurity Malaysia diiktiraf secara rasmi pada 2007.

Adalah diakui umum bahawa peningkatan transaksi dan aktiviti menerusi Internet telah mendedahkan rakyat Malaysia terhadap pencerobohan dan lain-lain risiko. Dalam usaha menangani ancaman sedemikian, CyberSecurity Malaysia telah memperluaskan perkhidmatan tindak balas insidennya dengan menubuhkan Pusat Bantuan Cyber999. Pusat Bantuan Cyber999 kini beroperasi sepenuhnya dan telah menawarkan perkhidmatannya sejak dilancarkan pada Julai 2009 semasa Persidangan dan Pameran CyberSecurity Malaysia || SecureAsia @ Kuala Lumpur 2009.

In the area of computer emergency response services, CyberSecurity Malaysia's research capability to analyse malicious software and provide the appropriate counter measures has culminated in the establishment of the CyberSecurity Malaysia Malware Research Centre. This research centre was officially launched by The Honourable Datuk Seri Dr Maximus Johnity Ongkili, Minister of Science Technology and Innovation at the World Computer Security Day - WCSD Malaysia 2009 in Kuala Lumpur.

In the international arena, CyberSecurity Malaysia achieved a significant milestone when its proposal followed by a dedicated effort to establish the Organisation of Islamic Conference Computer Emergency Response Team ("OIC-CERT") was accepted for implementation by the Organisation of the Islamic Conference ("OIC"). Arising from this initiative, collaborations were established with an initial pool of OIC member countries providing assistance and expertise to establish and operate their national computer emergency response teams.

Efforts by the Government to secure Malaysia's Critical National Information Infrastructure ("CNII") were also strongly supported by CyberSecurity Malaysia through its implementation of vulnerability assessment services. Major CNII institutions have given their cooperation and trust by agreeing to an assessment of their critical network infrastructure by CyberSecurity Malaysia.

CyberSecurity Malaysia's digital forensic capabilities and expertise received statutory acknowledgement when its digital forensic analysts were gazetted as "expert witness" by the Government under Section 399 of the Criminal Procedure Code. A full-fledged multimedia digital forensic laboratory was established and became fully operational in 2009, thus further enhancing CyberSecurity Malaysia's position as the leading digital forensic expert in Malaysia.

Dalam bidang perkhidmatan tindakbalas kecemasan komputer, keupayaan penyelidikan CyberSecurity Malaysia dalam menganalisa perisian berbahaya dan menyediakan langkah-langkah pencegahan sewajarnya membawa kepada penubuhan Pusat Kajian Malware CyberSecurity Malaysia. Pusat kajian ini dirasmikan oleh Menteri Sains, Teknologi dan Inovasi, Yang Berhormat Datuk Seri Dr Maximus Johnity Ongkili, pada Hari Keselamatan Komputer Sedunia - WCSD Malaysia 2009 di Kuala Lumpur.

Di arena antarabangsa, CyberSecurity Malaysia mencatat pencapaian bersejarah yang penting apabila cadangan yang disusuli usaha bersungguh-sungguh untuk menubuhkan Pasukan Tindak balas Kecemasan Komputer Persidangan Pertubuhan Islam ("OIC-CERT") diterima oleh Persidangan Pertubuhan Islam ("OIC") untuk dilaksanakan. Bertitik-tolak dari sini, kerjasama dibentuk dengan beberapa negara anggota OIC bagi menawarkan bantuan dan kepakaran ke arah membentuk dan menggerakkan pasukan tindakbalas kecemasan komputer kebangsaan masing-masing

CyberSecurity Malaysia turut menyokong usaha Kerajaan menubuhkan Prasarana Maklumat Kritikal Kebangsaan ("CNII") Malaysia menerusi pelaksanaan perkhidmatan penilaian kelemahan. Institusi utama CNII telah memberi kerjasama dan kepercayaan dengan membenarkan CyberSecurity Malaysia melakukan penilaian terhadap prasarana rangkaian kritikal masing-masing.

Keupayaan dan kemampuan forensik digital CyberSecurity Malaysia menerima pengiktifan statutori apabila penganalis forensik digitalnya diwartakan sebagai "saksi pakar" oleh Kerajaan di bawah Seksyen 399 Kanun Prosedur Jenayah. Sebuah makmal lengkap forensik digital dan multimedia lengkap turut diwujudkan. Makmal tersebut telah beroperasi sepenuhnya pada tahun 2009 sekali gus memperkukuhkan kedudukan CyberSecurity Malaysia sebagai perintis kepakaran forensik digital di Malaysia.

“

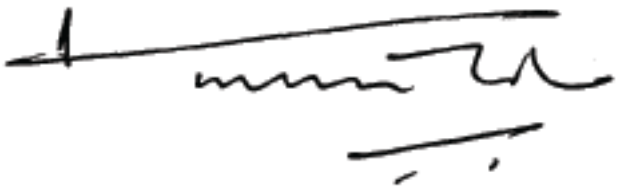
CyberSecurity Malaysia’s digital forensic capabilities and expertise received statutory acknowledgement when its digital forensic analysts were gazetted as “expert witness” by the Government under Section 399 of the Criminal Procedure Code.

”

I am pleased to put on record that CyberSecurity Malaysia has continued to fulfill the objectives of its establishment.

Looking ahead, CyberSecurity Malaysia expects to face mounting challenges to cyber security in the years to come. To prepare for this, we recognise that we need to cope in two essential areas: technology and human capital.

I would like to convey the Board of Directors’ gratitude and appreciation to the Ministry of Science, Technology & Innovation (MOSTI), the Ministry of Finance (MOF) and other relevant government bodies which have given their support and contribution to CyberSecurity Malaysia in 2009 and to our international affiliates and colleagues for their continuous commitment in assisting CyberSecurity Malaysia’s efforts in Information Security. May CyberSecurity Malaysia continue to flourish and prosper to become a globally recognised National Cyber Security Specialist Centre!



General Dato’ Seri Panglima Mohd Azumi bin Mohamed (Retired)
Chairman
CyberSecurity Malaysia

Dengan sukacitanya, saya ingin merakamkan di sini bahawa CyberSecurity Malaysia telah memenuhi matlamat penubuhannya.

Memandang jauh, keselamatan siber di jangka akan lebih mencabar pada tahun-tahun akan datang. Sebagai persediaan, kami mengenal pasti dua bidang utama yang perlu diberi perhatian iaitu teknologi dan modal insan.

Saya ingin merakamkan rasa terhutang budi dan penghargaan Lembaga Pengarah kepada Kementerian Sains, Teknologi dan Inovasi (MOSTI), Kementerian Kewangan (MOF) dan agensi kerajaan berkenaan yang memberi sokongan dan sumbangan kepada CyberSecurity Malaysia pada 2009 dan kepada sekutu dan rakan sekerja antarabangsa kami atas komitmen berterusan dalam membantu usaha CyberSecurity Malaysia dalam bidang Keselamatan Maklumat.

Semoga CyberSecurity Malaysia terus berkembang dan maju ke arah menjadi Pusat Rujukan dan Pakar Keselamatan Siber Kebangsaan yang diiktiraf di peringkat global!

> “Keupayaan dan kemampuan forensik digital CyberSecurity Malaysia menerima pengiktifan statutori apabila penganalisis forensik digitalnya diwartakan sebagai “saksi pakar” oleh Kerajaan di bawah Seksyen 399 Kanun Prosedur Jenayah.”

Jeneral Dato’ Seri Panglima Mohd Azumi bin Mohamed (Bersara)
Pengerusi
CyberSecurity Malaysia

Board Members Ahli Lembaga Pengarah

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

General 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 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.

Lt. Col. Husin Bin Jazri (Retired), CISSP, CBCP
Director and Chief Executive Officer

Husin has served as Chief Executive Officer and Board Member since the inception of CyberSecurity Malaysia. When he joined the National ICT Security and Emergency Response Centre (NISER now known as CyberSecurity Malaysia) in 2000, he brought with him more than 20 years' experience in information and communications security from his service with the Malaysian Armed Forces' Signal Corps. Husin was a former Chairman of the Malaysia IT Security Association and the Asia Pacific Computer Emergency Response Team (APCERT). Among his current posts are Chairperson of the Organisation of Islamic Countries - Computer Emergency Response Team (OIC-CERT), and Chairman of the Malaysian Vocational Advisory Committee – Information and Communication Technology (ICT), Department of Skills Development, Ministry of Human Resources. Husin was awarded the prestigious (ISC)² Information Security Leadership Achievements (ISLA) Award 2009 for Exemplary Leadership and Dedications in Enhancing the IT Security Workforce (Category: Senior IT Security Professional).

Dato' Madinah Binti Mohamad
Director

Dato' Madinah 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).

Datuk Dr Abdul Raman Bin Saad
Director

Datuk Dr Abdul Raman 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. He is the co-head of ARSA Lawyers Shariah Finance Law Department and an advisor for eMedina, an e-government initiative in Saudi Arabia.

Datuk Dr Abdul Raman holds an Honours Degree in Law from the University of Singapore 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).

Board Members Ahli Lembaga Pengarah

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 Division (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 Division (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.

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 has been 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).

Lembaga Pengarah

* Dato' Madinah binti Mohamad and Datuk Dr Abdul Rahman bin Saad are not in this photograph.
* Dato' Madinah binti Mohamad dan Datuk Dr Abdul Rahman bin Saad tiada di dalam gambar ini.

Jeneral Dato' Seri Panglima Mohd Azumi Bin Mohamed (Bersara)
Pengerusi

Jeneral Dato' Seri Panglima Mohd Azumi bin Mohamed (Bersara) dilantik sebagai Pengerusi Lembaga Pengarah pada Julai 2009. Seorang pegawai tentera dengan kerjaya ketenteraan cemerlang selama 37 tahun, perkhidmatannya bersama Angkatan Tentera Malaysia merangkumi pelbagai kapasiti termasuk sebagai Komander Briged Payung Terjun ke-10, Komander Bahagian Infantri Pertama dan Panglima Angkatan Tentera sebelum bersara pada Disember 2004. Semasa berkhidmat, beliau turut berkhidmat dengan Misi Permerhati Iraq/Kuwait Pertubuhan Bangsa-Bangsa Bersatu (PBB) selepas Perang Teluk Pertama. Beliau diberi pengiktirafan antarabangsa oleh Perancis dan PBB, menerima anugerah French Award Officer Ordre National du Merite dan Pingat PBB untuk Pengamanan Antarabangsa. Selain kelulusan ketenteraan daripada Officer Cadet School di Portsea, Australia, Australian Army Infantry Centre dan US Army Infantry Centre di Fort Benning, beliau juga memiliki Sarjana Sains Sumber Alam dan Strategi dari National Defense University di Washington DC dan Diploma Ijazah Strategi dari Australian Capital Accreditation Agency. Sejak bersara, Jeneral Dato' Seri Panglima Mohd Azumi bin Mohamed (Bersara) dilantik sebagai ahli Panel Penasihat Perpaduan Negara dan ahli lembaga beberapa syarikat senarai awam dan swasta.

Lt. Kol. Husin Bin Jazri (Bersara), CISSP, CBCP
Pengarah & Ketua Pegawai Eksekutif

LT. Kol. Husin bin Jazri (Bersara) berkhidmat sebagai Ketua Pegawai Eksekutif dan Ahli Lembaga sejak penubuhan CyberSecurity Malaysia. Apabila menyertai Pusat Tindak balas Kecemasan dan Keselamatan ICT Kebangsaan (NISER kini dikenali sebagai CyberSecurity Malaysia) pada 2000, beliau membawa bersama lebih 20 tahun pengalaman di dalam bidang keselamatan maklumat dan komunikasi melalui perkhidmatannya dengan Signal Corps Angkatan Tentera Malaysia. Beliau merupakan mantan Pengerusi Persatuan Keselamatan IT Malaysia dan Pasukan Tindak balas Kecemasan Komputer Asia Pasifik (APCERT). Di antara jawatan yang dipegangnya kini adalah Pengerusi Pasukan Tindak balas Kecemasan Komputer - Organisasi Persidangan Islam (OIC-CERT), dan Pengerusi Jawatankuasa Penasihat Vokasional Malaysia – Informasi dan Teknologi Maklumat (ICT), Jabatan Pembangunan Kemahiran, Kementerian Sumber Manusia. Beliau dianugerahkan pengiktirafan berprestij (ISC)² Information Security Leadership Achievements (ISLA) Award 2009 for Exemplary Leadership and Dedications in Enhancing the IT Security Workforce (Category: Senior IT Security Professional).

*** Dato' Madinah Binti Mohamad**
Pengarah

Dato' Madinah binti Mohamad dilantik sebagai Pengarah Lembaga pada Julai 2009. Beliau adalah Ketua Setiausaha Kementerian Sains, Teknologi dan Innovasi dan penggiat utama di dalam usaha pelaksanaan Dasar Bioteknologi, Dasar IT dan Dasar Sains, Teknologi dan Inovasi Kebangsaan. Sepanjang kerjayanya, beliau berpengalaman sebagai Pegawai Tadbir dan Diplomatik di Kementerian Luar Negeri pada 1981 sebelum dinaikkan pangkat ke Jabatan Perkhidmatan Awam, Kementerian Pembangunan Negara dan Luar Bandar, Kementerian Kerja Raya dan Jabatan Perpaduan Negara dan Intergrasi Nasional.

Dato' Madinah adalah pemegang Sarjana Muda Sains Politik dari Universiti Sains Malaysia (USM) dan Sarjana Pembangunan Sumber Manusia dari Universiti Putra Malaysia (UPM).

*** Datuk Dr Abdul Raman Bin Saad**
Pengarah

Datuk Dr Abdul Raman bin Saad dilantik menganggotai Lembaga pada Jun 2009. Seorang peguambela dan peguamcara sejak 1977, beliau memiliki pengalaman luas bertugas dengan Khidmat Undang-Undang dan Kehakiman Malaysia sebagai Majistret, Timbalan Pendakwa Raya dan Penolong Pengarah bagi Bantuan Guaman sebelum menjadi pengamal persendirian. Beliau diiktiraf sebagai antara penasihat undang-undang berberpengalaman luas di bidang undang-undang korporat dan perdagangan, undang-undang teknologi maklumat dan komunikasi serta Kewangan Syariah. Beliau adalah Ketua bersama Jabatan Kewangan Syariah Peguam-Peguam ARSA dan penasihat untuk eMedina, sebuah inisiatif e-kerajaan di Arab Saudi.

Datuk Dr Abdul Raman bin Saad adalah pemegang Ijazah dengan Kepujian Undang-Undang dari University of Singapore dan Sarjana Undang-Undang (dengan pengkhususan Undang-Undang Elektronik) dari University of Melbourne, Australia. Beliau juga merupakan pemegang ijazah kedoktoran jurusan Pentadbiran Perniagaan dari Midwest Missouri University, Amerika Syarikat. Beliau turut menjadi pengarah Universiti Teknikal Malaysia Melaka.

Datuk Haji Abang Abdul Wahap Bin Haji Abang Julai
Pengarah

Datuk Haji Abang Abdul Wahap bin Haji Abang Julai dilantik ke dalam Lembaga pada Mei 2009. Beliau memiliki kerjaya cemerlang bersama Polis Diraja Malaysia selama 37 tahun sebelum bersara sebagai Pengarah Jabatan Siasatan Jenayah Narkotik pada 2007.

Beliau juga pernah berkhidmat sebagai Timbalan Pengarah Latihan Dalam Pengurusan di Ibu Pejabat Bukit Aman Kuala Lumpur dan Timbalan Pesuruhjaya Polis Sarawak. Sebagai menghargai perkhidmatannya, beliau dianugerahkan 'Pingat Panglima Gagah Pasukan Polis', anugerah tertinggi untuk pegawai-pegawai polis.

Kini, beliau berkhidmat sebagai Pengarah Bebas bukan eksekutif untuk beberapa syarikat di Sarawak dan aktif dengan Kontinjen Sarawak Sukan Malaysia (SUKMA)

Datuk Haji Abang Abdul Wahap bin Haji Abang Julai adalah pemegang Ijazah Undang-Undang dari Universiti Islam Antarabangsa Malaysia (IIUM) dan Diploma Lanjutan Sains Polis dari Universiti Kebangsaan Malaysia (UKM).

Ir Md Shah Nuri Bin Md Zain
Pengarah

Encik Ir Md Shah Nuri bin Md Zain dilantik menganggotai Lembaga pada April 2008. Beliau adalah Setiusaha Kedua di Bahagian Dasar Keselamatan Angkasa dan Siber di bawah Majlis Keselamatan Negara Jabatan Perdana Menteri. Beliau berkhidmat dengan Kerajaan lebih 20 tahun sebagai Felo Penyelidikan untuk MIMOS Bhd, diikuti sebagai jurutera di Jabatan Kerja Raya di bawah Kementerian Kerja Raya.

Encik Ir Md Shah Nuri adalah pemegang Ijazah Sains Kejuruteraan Elektrik dari Connecticut State University, Amerika Syarikat.

Rubaiah Binti Hashim
Pengarah

Puan Rubaiah binti Hashim dilantik menyertai Lembaga pada April 2008. Beliau adalah Setiusaha Kedua di Bahagian Komunikasi (Prasarana, Aplikasi & Teknologi) Kementerian Penerangan, Komunikasi dan Kebudayaan. Beliau berkhidmat dengan Kerajaan selama lebih 25 tahun dalam pelbagai kapasiti termasuk penganalisis sistem bagi Kementerian Perusahaan Awam dan Kementerian Pelajaran, kemudian sebagai Pembantu Setiausaha Prinsipal dan diikuti Setiausaha Rendah kepada Bahagian Komunikasi (Prasarana dan Aplikasi Elektronik) Kementerian Tenaga, Air dan Komunikasi.

Puan Rubaiah binti Hashim adalah pemegang ijazah Sarjana Muda Sains dengan Kepujian jurusan Matematik dan Aplikasi IT dari University of Wales Institute of Science and Technology (UWIST), United Kingdom.

Rohani Binti Mohamad
Pengarah

Puan Rohani binti Mohamad dilantik menganggotai Lembaga pada Januari 2010. Beliau adalah Setiausaha Kedua di Bahagian Pengurusan Teknologi Maklumat di Kementerian Kewangan. Berkhidmat sebagai pegawai awam selama lebih 25 tahun, beliau ditempatkan di Bahagian Keselamatan ICT di Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri, Bahagian Teknologi Maklumat dan Unit Koridor Raya Multimedia di Bahagian Pengurusan Pentadbiran, Perbendaharaan Malaysia, Kementerian Tanah dan Pembangunan Koperasi dan Unit Perancangan Ekonomi (EPU).

Puan Rohani binti Mohamad adalah pemegang ijazah Sarjana Muda jurusan Statistik dan Penyelidikan Operasi dari Institute of Science and Technology, University of Manchester, United Kingdom dan Diploma Analisis Sistem dari Universiti Teknologi MARA (UiTM).

Cyber999

WHAT IS CYBER999

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

Securing Our Cyberspace

Mode of reporting

Web Reporting
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

Best Brand Internet Security 2008 & 2009

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

CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

Management Committee Jawatankuasa Pengurusan

Lt. Col. Husin Bin Jazri (Retired), CISSP, CBCP
Chief Executive Officer

As Chief Executive Officer, Husin has been at the helm of CyberSecurity Malaysia since its inception. He is a Certified Business Continuity Professional (CBCP) by Disaster Recovery Institute (DRI), USA; a Certified Information Systems Security Professional (CISSP) by the International Information Systems Security Certification Consortium Inc. (ISC)².; and a member of the Board of the (ISC)². He is a recipient of the prestigious (ISC)² Information Security Leadership Achievements (ISLA) Award 2009 for Exemplary Leadership and Dedication in Enhancing the IT Security Workforce (Category: Senior IT Security Professional). Husin 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).

Ketua Pegawai Eksekutif
Sebagai Ketua Pegawai Eksekutif, Husin telah berada dalam pucuk pimpinan CyberSecurity Malaysia sejak ia ditubuhkan. Beliau adalah pemegang Sijil Profesional Kesinambungan Perniagaan (CBCP) oleh Disaster Recovery Institute (DRI), Amerika Syarikat; Sijil Profesional Keselamatan Sistem Maklumat (CISSP) oleh International Information Systems Security Certification Consortium Inc. (ISC)².; dan ahli Lembaga (ISC)². Beliau juga adalah penerima anugerah berprestij (ISC)² Information Security Leadership Achievements (ISLA) Award 2009 for Exemplary Leadership and Dedications in Enhancing the IT Security Workforce (Category: Senior IT Security Professional). Husin adalah pemegang Ijazah Sarjana Muda Kejuruteraan dari University of Hartford, Connecticut, Amerika Syarikat; Diploma Lepasan Ijazah Sistem Analisis dari Universiti Teknologi MARA (UiTM); Sarjana Sains dengan Kepujian di dalam Keselamatan Maklumat dari Royal Holloway University of London, United Kingdom; dan Sarjana Pentadbiran Perniagaan dari Universiti Putra Malaysia (UPM).

Zahri Bin Yunos
Chief Operating Officer

Zahri has been appointed as 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. Zahri is a key person in ensuring the successful delivery of various achievements attained by CyberSecurity Malaysia. He is a certified Associate Business Continuity Professional (ABCP) by the Disaster Recovery Institute International (DRII), 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.

Ketua Pegawai Operasi
Zahri telah dilantik sebagai Ketua Pegawai Operasi sejak tahun 2007. Zahri secara aktif terlibat di dalam pembentukan Panel Pakar (POE) NISER (Pusat Tindak balas Kecemasan dan Keselamatan ICT Kebangsaan) dan Persidangan Pertubuhan Islam-Pasukan Tindakbalas Kecemasan Komputer (OIC-CERT), yang melonjakkan imej Malaysia di persada antarabangsa di dalam bidang keselamatan siber. Zahri merupakan teraju utama di dalam memastikan pelbagai kejayaan yang dikecapi oleh CyberSecurity Malaysia. Beliau memiliki Sijil Profesional Bersekutu Kesinambungan Perniagaan (ABCP) oleh Disaster Recovery Institute International (DRII), Amerika Syarikat. Beliau juga memegang Sarjana Sains Kejuruteraan Elektrik dari Universiti Teknologi Malaysia (UTM) dan Sarjana Muda Sains Komputer Sains dari Fairleigh Dickinson University, New Jersey, Amerika Syarikat.

Mohd Roslan Bin Ahmad
Head, Corporate Services Division

Mohd. Roslan has led the Corporate Services Division since 2007 with a portfolio that includes the departments of Finance, Administration & Physical Security, Procurement, and Knowledge Resource Centre. He is a certified Safety and Health Officer (SHO) from the National Institute of Occupational Safety and Health (NIOSH) Malaysia. Mohd. Roslan holds a Master of Management 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).

Ketua, Bahagian Khidmat Korporat
Mohd Roslan telah memimpin Bahagian Perkhidmatan Korporat sejak 2007 dengan portfolio yang meliputi jabatan-jabatan Kewangan, Pentadbiran & Keselamatan Fizikal, Perolehan, dan Pusat Sumber Ilmu. Beliau adalah Pegawai Keselamatan dan Kesihatan (SHO) bertauliah dari Institut Keselamatan dan Kesihatan Pekerjaan Negara (NIOSH) Malaysia. Mohd Roslan adalah pemegang Sarjana Pengurusan dari Open University Malaysia (OUM), Sarjana Muda Kejuruteraan Sivil dari University of Hartford, Connecticut, Amerika Syarikat dan Diploma Lepasan Ijazah Analisis Sistem dari University Technology MARA (UiTM).

Mohd Shamir Bin Hashim
Head, Cyber Security Research & Policy Division

Mohd. Shamir has been the Head of Cyber Security Policy Research Division since 2007. He is a core member of the secretariat team to implement Malaysia's National Cyber Security Policy (NCSP) and also a national committee that mitigates cyber media incidences. He was involved in the establishment of the Organisation of Islamic Conference – Computer Emergency Response team (OIC-CERT). Mohd. Shamir is a certified Professional in Critical Infrastructure Protection from the Critical Infrastructure Institute, Canada. He holds a Bachelor of Science in Civil Engineering from the University of Missouri-Kansas City, USA.

Ketua, Bahagian Penyelidikan Keselamatan Siber dan Dasar
Mohd Shamir telah menjadi Ketua Bahagian Penyelidikan Polisi Keselamatan Siber sejak 2007. Beliau adalah orang kuat pasukan secretariat untuk melaksanakan Dasar Keselamatan Siber Nasional (NCSP dan juga jawatankuasa kebangsaan yang mengurangkan insiden media siber. Beliau terlibat di dalam penubuhan Persidangan Pertubuhan Islam-Pasukan Tindakbalas Kecemasan Komputer (OIC-CERT). Mohd. Shamir adalah ahli Profesional bertauliah Perlindungan Prasarana Kritikal dari Critical Infrastructure Institute, Kanada. Beliau memiliki Sarjana Muda Sains Kejuruteraan Sivil dari University of Missouri-Kansas City, Amerika Syarikat.

Roshdi Bin Ahmad
Head, Strategy Management Division

Roshdi has been with CyberSecurity Malaysia since 2007 and now leads four departments which include Corporate Planning & Strategy, Corporate Event, PR & Protocol, Corporate Branding & Media Relations, and Innovation & Commercialisation. 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).

Ketua, Bahagian Pengurusan Strategi
Roshdi telah bersama CyberSecurity Malaysia sejak 2007 dan kini mengetuai empat jabatan termasuk Perancangan Korporat dan Strategi; Majlis Korporat, PR & Protokol; Penjenamaan Korporat dan Perhubungan Media; dan Inovasi dan Pengkomersilan. Beliau telah menguruskan dan memperoleh pelbagai projek ICT dan mempunyai pengalaman yang luas di dalam disiplin-disiplin yang berlainan terutamanya strategi korporat, pemasaran dan operasi. Beliau memiliki Ijazah Sarjana Muda (Kepujian) Pengajian Perniagaan (Pemasaran) dari Universiti Teknologi MARA (UiTM) dan Diploma Perniagaan Tani dari Universiti Putra Malaysia (UPM).

Management Committee Jawatankuasa Pengurusan

Dr. Solahuddin Bin Shamsuddin
Head, Security Quality Management Division

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 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).

Ketua, Bahagian Pengurusan Keselamatan Kualiti
Dr. Solahuddin mengetuai Bahagian Perkhidmatan Pengurusan Kualiti Keselamatan yang merangkumi jabatan-jabatan Jaminan Keselamatan, Pengurusan Keselamatan & Amalan Terbaik, Koordinasi Penyelidikan, dan Kumpulan Perunding Siber. Beliau merupakan salah seorang perintis di dalam usaha keselamatan siber di NISER (Pusat Tindak balas Kecemasan dan Keselamatan ICT Kebangsaan). Beliau memiliki Ijazah Kedoktoran Sains Komputer dari University of Bradford, United Kingdom, Sarjana Muda Kejuruteraan Elektrik dari Wichita State University, Kansas, Amerika Syarikat dan Diploma Lepasan Ijazah Analisis Sistem dari Universiti Teknologi MARA (UiTM).

Jailani 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).

Ketua, Jabatan Perundangan dan Kesetiausahaan / Setiausaha Syarikat
Sebagai Ketua Jabatan Undang-Undang dan Kesetiausahaan sejak Ogos 2007, Jailany bertanggungjawab ke atas semua hal berkenaan undang-undang dan kesetiausahaan syarikat dan menasihatkan pengurusan tentang undang-undang dan kesetiausahaan. Mempunyai latar belakang Perundangan dan Setiausaha Syarikat yang Berlesen, Jailany adalah pemegang Ijazah Undang-Undang (Kepujian) dari Universiti Malaya (UM).

Adli Bin Abd Wahid
Head, MyCERT Department

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 has been 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.

Ketua, Jabatan MyCERT
Ketua Pasukan Tindak balas Kecemasan Komputer sejak 2007, Adli juga mengetuai Pusat Bantuan Cyber999 serta Pusat Penyelidikan Malware CyberSecurity Malaysia. Beliau terlibat secara aktif di dalam pelbagai inisiatif keselamatan komputer global dan telah berucap di pelbagai forum keselamatan komputer di seluruh dunia. Adli merupakan Penerima (ISC)² Information Security Leadership Achievement (ISLA) Award di dalam kategori Pengamal Keselamatan IT pada 2009. Beliau adalah pemegang Sarjana Sains Komputer Sains di dalam pengkhususan Kejuruteraan Perisian.

Aswami Fadillah Bin Mohd Ariffin
Head, Digital Forensics Department

Aswami who is an honoree of the prestigious (ISC)² Information Security Leadership Achievement (ISLA) Award is one of the pioneers of CyberSecurity Malaysia. Aswami has been entrusted to lead the Digital Forensics Department since year 2006. He has handled more than 1000 cases including some of the high profile ones. He is a GIAC Certified Forensics Analyst (GCFA), Certified Wireless Security Professional (CWSP) and a Certified Ethical Hacker (CEH). Aswami holds a Degree in Electronics Engineering from the University of Liverpool, UK and a Master in Management from Universiti Malaya.

Ketua, Jabatan Forensik Digital
Aswami yang merupakan penerima anugerah berprestij (ISC)² Information Security Leadership Achievement (ISLA) adalah salah seorang perintis CyberSecurity Malaysia. Aswami diamanahkan untuk mengetuai Jabatan Forensik Digital sejak 2006. Beliau telah menangani lebih 1000 kes termasuk yang berprofil tinggi. Beliau adalah Penganalisis Forensik GIAC Bertauliah (GCFA), Ahli Profesional Bertauliah Keselamatan Tanpa Wayar, (CWSP) dan Penggodam Etika Bertauliah (CEH). Aswami memiliki Ijazah Kejuruteraan Elektrik dari University of Liverpool, United Kingdom dan Sarjana Pengurusan dari Universiti Malaya.

Mohd Anwer Bin Mohamed Yusoff
Head, Innovation & Commercialisation Deparment

The Head of Innovation & Commercialisation department since December 2008, Anwer has more than 20 years' experience in Enterprise Resource Planning, Supply Chain Management, Business Process Re-engineering, Malaysian telecommunications regulation, wireless broadband, and electronic commerce. He holds a Bachelor of Science in Aeronautical Engineering from Embry-Riddle Aeronautical University, Daytona Beach, Florida, US.

Ketua, Jabatan Innovasi dan Komersial
Menjadi Ketua Jabatan Inovasi & Pemerdagangan sejak Disember 2008, Anwer mempunyai lebih 20 tahun pengalaman di dalam Perancangan Sumber Perusahaan, Pengurusan Rangkaian Bekalan, *Business Process Re-engineering*, Peraturan Telekomunikasi Malaysia, Jalur Lebar Wayarles, dan Perdagangan Elektronik. Beliau memiliki Sarjana Muda Sains Kejuruteraan Aeronautik dari Embry-Riddle Aeronautical University, Daytona Beach, Florida, US.

Razman Azrai Bin Zainudin
Head, Corporate Planning & Strategy

Newly appointed as Head of Corporate Planning & Strategy, Razman has 15 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 and currently is a member of MOSTI KPI working 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 in Rhode Island, USA and MBA from Staffordshire University, United Kingdom.

Ketua, Perancangan Korporat & Strategi
Baru dilantik sebagai Ketua Perancangan Korporat & Strategi, Razman mempunyai 15 tahun pengalaman di dalam bidang ICT, menerajui perkhidmatan perundingan ICT untuk syarikat-syarikat penting di kawasan Asia Pasifik. Beliau pernah menjadi ahli Jawatankuasa Teknikal Hala Tuju Strategik ICT Nasional dan kini menjadi ahli jawatankuasa kerja MOSTI KPI. Razman juga adalah sekretariat untuk Jawatankuasa Pengurusan CyberSecurity Malaysia. Beliau adalah pemegang Sarjana Muda Sains Pengurusan Sains & Sistem Maklumat dari University in Rhode Island, Amerika Syarikat dan *MBA* dari Staffordshire University, United Kingdom.

Foreword by the CEO

As we look back and review 2009, it is pertinent to consider the viral growth of the internet over the past 20 years and the role cyber security plays in its rapid development. The internet and the cyber world are arguably the defining phenomena of the present age. Their influence is pervasive, touching every facet of our lives to the extent that many of us live as much in that alternative reality as we do in the *'real world'*.

Two decades ago at a time when Malaysians first heard of the word 'internet', there were only four million internet users worldwide. By 2000, this figure had multiplied to 360 million. Today, according to *internetworldstats.com*, more than 1.7 billion people in every inhabited corner of the world go online on a regular basis.

Such exponential growth would never have been possible without the assurance and confidence provided to users via cyber security. It is very much like a silent sentinel that watches and

Perutusan Ketua Pegawai Eksekutif

MENGIMBAU dan mengimbas tahun 2009, kita tidak dapat lari daripada memperkatakan pertumbuhan pantas Internet sepanjang 20 tahun kebelakangan ini dan peranan yang dimainkan keselamatan siber sejajar perkembangannya. Internet dan dunia siber ini adalah fenomena paling mengujakan abad ini. Pengaruhnya nyata membuak, menyentuh segenap ruang kehidupan kita sehingga sebahagian besar daripada kita hidup dalam realiti alternatif itu sepertimana kita melakukannya di dunia sebenar.

Ketika rakyat Malaysia pertama kali mendengar perkataan `internet' dua dekad lalu, pengguna internet di seluruh dunia hanya berjumlah empat juta orang. Menjelang tahun 2000, angka ini berganda kepada 360 juta. Hari ini, *internetworldstats.com* melaporkan lebih 1.7 bilion pengguna dari seluruh pelosok dunia menggunakan internet secara kerap.

Pertumbuhan pesat seperti itu mustahil dicapai tanpa jaminan dan keyakinan yang diberi kepada pengguna menerusi keselamatan siber. Ia boleh

protects us from threats seen and unseen as we go about our daily business. Cyber security is irrevocably linked to the future of the internet and its inherent cyber world.

Likewise in Malaysia, cyber security provides the platform for the growth of the internet and supports the development of information and communication technologies (ICT). It is an essential component of our online culture.

As a reflection of Malaysia's prominence in this field, we are currently the Chair for OIC-CERT (Organisation of Islamic Conference – Computer Emergency Response Team), a collaboration between the OIC member countries to share knowledge, expertise and cooperate on cyber security. I am proud to note that we are playing a leadership role in this area.

Domestically, I am pleased to state that the level of cyber security has seen significant improvement particularly in the last three years since we intensified our cyber security awareness campaign. It is gratifying that growing awareness of cyber threats has also translated into interest in mitigating the risk. For example, there is now much greater management commitment to ensure that cyber security is part of every CEO's list of priorities in both the public as well as private sectors.

Success on this score provides the impetus for us to intensify our awareness campaign on cyber security. In the coming years, we will continue targeting schoolchildren for our awareness campaign as they will eventually form the backbone of our nation, its economy and society. As they say, prevention is always better than cure.

diibaratkan penjaga senyap yang memerhati dan melindungi kita daripada ancaman, baik yang boleh dilihat mahu pun sebaliknya sepanjang kita menjalani urusan seharian. Keselamatan siber adalah jambatan penghubung masa depan internet dan dunia siber.

Seperti juga di Malaysia, keselamatan siber menyediakan landasan bagi perkembangan internet dan menyokong pembangunan teknologi maklumat dan komunikasi (ICT). Ia adalah komponen penting bagi budaya dalam talian kita.

Mengimbas ketrampilan Malaysia dalam bidang ini, ketika ini kita menduduki Kerusi OIC-CERT (Persidangan Pertubuhan Islam - Pasukan Tindakbalas Kecemasan Komputer) iaitu usahasama di kalangan negara anggota OIC untuk berkongsi pengetahuan, kepakaran dan bekerjasama membabitkan aspek keselamatan siber. Saya bangga menyatakan bahawa kami memainkan peranan utama dalam perkara ini.

Di peringkat domestik, sukacita saya nyatakan bahawa tahap keselamatan siber menampakkan peningkatan ketara, terutama dalam tempoh tiga tahun kebekalangan ini sejak kami merancakkan kempen kesedaran keselamatan siber. Kesedaran meninggi terhadap ancaman siber turut diterjemah menjadi keinginan untuk mengurangkan risikonya. Sebagai contoh, komitmen pihak pengurusan dalam memastikan keselamatan siber menjadi sebahagian daripada senarai keutamaan CEO sektor awam dan swasta ketika ini adalah jauh lebih tinggi.

Kejayaan dalam aspek ini memberi kami lonjakan untuk meningkatkan kempen kesedaran terhadap keselamatan siber. Dalam tahun-tahun mendatang, kami akan terus meletakkan pelajar sekolah sebagai sasaran kempen kesedaran kerana di akhirnya, mereka akan menjadi tunjang negara, baik ekonomi mahupun masyarakatnya. Seperti yang kerap dikatakan, mencegah adalah lebih baik daripada mengubati.

Yet, despite our best efforts at prevention, it is inevitable that there will be cyber crime. After all, crime is a natural by-product of any successful and profitable industry. Today, cyber crime has developed an underground economy for commercial and industrial espionage. This is a development that we are becoming increasingly vigilant over, being the nation's principal cyber security agency and leading cyber crimefighter.

That said, the situation in Malaysia remains manageable and within the threshold limits, notwithstanding the 68% increase of security incidents referred to Cyber999 Help Centre in 2009 compared to the previous year. The bulk of these incidents involved relatively minor infractions such as denial of service, malware attacks, online harassment and fraud.

In this regard, I take pleasure in mentioning the successful launch in July 2009 of our Cyber999 Help Centre, as well as the Cyber Security Malaysia Malware Research Centre in December the same year. These services and facilities serve to reinforce a robust and resilient cyber security framework necessary for the sustained growth of Malaysia's ICT industry, and in particular, the Multimedia Super Corridor (MSC Malaysia).

"Yet, despite our best efforts at prevention, it is inevitable that there will be cyber crime. After all, crime is a natural by-product of any successful and profitable industry. Today, cyber crime has developed an underground economy for commercial and industrial espionage."

In addition, I am pleased to state that there has been significant progress in the growth and development of local cyber security products and services over the past few years. Indeed, I am given to understand that the number of domestic players in this field multiplied three-fold in 2009. While many are small and medium-sized enterprises, several have gone public with listing on Bursa Malaysia.

It is heartening to note that many local cyber security companies are exporting their products and services overseas, especially to the predominantly consumer markets of the OIC member countries. The global market for cyber security is reportedly worth an estimated US$60 billion and is expected to post impressive growth rates in the coming years. Gaining market access and securing market share is the domestic industry's goal moving forward and forms one of the objectives of the 10th Malaysia Plan.

The emergence of digital security among Malaysian companies has also led to greater creativity and innovation in local content for cyber security. We are starting to see new and innovative biometrics solutions and access controls that are proudly 'Made

Sehebat mana sekalipun usaha kami dalam mencegah, jenayah siber memang tidak dapat dielak. Tambahan pula, jenayah adalah produk sampingan mana-mana industri yang menempa kejayaan dan keuntungan. Hari ini, jenayah siber telah membentuk ekonomi bawah tanah bagi pengintipan komersial dan industri. Ini adalah perkembangan yang kami awasi dengan penuh ketelitian, seiring fungsi kami sebagai agensi keselamatan siber utama negara dan peneraju anti jenayah siber.

Namun demikian, situasi di Malaysia kekal terurus dan berada di dalam batas kawalan walaupun berlaku peningkatan 68% dari segi insiden keselamatan yang dirujuk kepada Pusat Bantuan Cyber999 pada 2009 berbanding tahun sebelumnya. Sebahagian besar daripada aduan ini membabitkan pelanggaran undang-undang kecil seperti perkhidmatan terhalang, serangan malware, gangguan dalam talian dan penipuan.

Susulan itu, saya ingin menyentuh kejayaan Pusat Bantuan Cyber999 yang dilancarkan pada Julai 2009 dan Pusat Kajian Malware CyberSecurity Malaysia pada tahun sama. Perkhidmatan dan kemudahan ini bermatlamat membentuk kerangka keselamatan siber yang mantap dan berdaya tahan yang diperlukan bagi menjamin pertumbuhan mapan industri ICT Malaysia dan Koridor Raya Multimedia Malaysia (MSC Malaysia).

Sebagai tambahan, sukacita saya ingin maklumkan bahawa terdapat kemajuan yang signifikan dari segi pertumbuhan dan pembangunan produk serta perkhidmatan keselamatan siber tempatan sejak beberapa tahun lalu. Malah, saya difahamkan bilangan penggerak domestik dalam bidang ini bertambah tiga kali ganda pada 2009. Walaupun kebanyakannya adalah perusahaan bersaiz kecil dan sederhana, namun ada beberapa syarikat yang telah tersenarai di Bursa Malaysia.

Melihat akan banyaknya syarikat keselamatan siber tempatan yang mengeksport produk dan perkhidmatan mereka ke luar negara adalah sesuatu yang menggembirakan, terutama ke negara OIC yang mempunyai pasaran kepenggunaan tinggi. Nilai pasaran global bagi keselamatan siber dilaporkan dalam anggaran AS$60 bilion dan dijangka mencatat kadar pertumbuhan memberangsangkan pada tahun-tahun mendatang. Sasaran industri domestik ialah mendapatkan akses pasaran dan menjamin saham pasaran untuk terus ke hadapan dan membentuk satu daripada matlamat Rancangan Malaysia Ke-10.

Kemunculan keselamatan digital di kalangan syarikat Malaysia turut membawa kepada daya kreativiti dan inovasi lebih cemerlang dari segi kandungan tempatan bagi keselamatan siber. Kami mulai melihat penyelesaian biometrik dan kawalan akses baru serta inovatif yang dengan bangganya memaparkan `Buatan Malaysia'.

“Sehebat mana sekalipun usaha kami dalam mencegah, jenayah siber memang tidak dapat dielak. Tambahan pula, jenayah adalah produk sampingan mana-mana industri yang menempa kejayaan dan keuntungan. Hari ini, jenayah siber telah membentuk ekonomi bawah tanah bagi pengintipan komersial dan industri.”

in Malaysia'.

As an agency of the Government and a leader in the field, CyberSecurity Malaysia continues to play a backend role in supporting the industry. During the year under review, CyberSecurity Malaysia was also allocated some funds for the disbursement of financial assistance to stimulate the local industry under the Second Economic Stimulus Package (ESP2). In this regard, we played a critical role in bringing together established and emerging players in a consortium so they can pool their resources and efforts while learning from each other and tapping on one another's strengths.

Looking ahead, we will continue to focus on professional development of cyber security professionals to ensure we have a sufficient pool of talent to secure our cyber space as well as for the export of talent and services abroad.

We are confident of tapping into new growth areas by exploiting our collaborations at international level. Currently, we cooperate and collaborate with 71 countries including the member nations of OIC and the Asia Pacific Rim.

Our immediate goal is for Malaysia as a nation to be self-reliant in the area of cyber security.

Lt. Col. Husin Bin Jazri (Retired), CISSP, CBCP
Director and Chief Executive Officer
CyberSecurity Malaysia

Sebagai agensi Kerajaan dan peneraju dalam bidang ini, CyberSecurity Malaysia terus berperanan sebagai tulang belakang yang menyokong industri. Sepanjang tahun penilaian, CyberSecurity Malaysia turut memperuntukkan sejumlah dana bagi pengagihan bantuan kewangan ke arah merangsang industri tempatan menerusi Pakej Rangsangan Ekonomi Kedua (ESP2). Dalam perkara ini, kami memainkan peranan kritikal ke arah menyatukan penggerak terkemuka dan baru dalam konsortium supaya mereka dapat menggabungkan sumber dan usaha, selain saling mempelajari dan mencungkil kekuatan sesama sendiri pada masa sama.

Mencongak langkah ke depan, kami akan terus memberi perhatian terhadap pembangunan profesional pakar keselamatan siber bagi memastikan kami mempunyai bilangan tenaga mencukupi untuk melindungi ruang siber, selain mengeksport kepakaran dan perkhidmatan ke luar negara.

Kami yakin untuk menembusi kawasan pertumbuhan baru dengan meneroka usahasama di peringkat antarabangsa. Ketika ini, kami menjalankan usahasama dan kerjasama dengan 71 negara termasuk negara anggota Persidangan Pertubuhan Islam (OIC) dan Lingkaran Asia Pasifik.

Matlamat terdekat kami ialah untuk menjadikan Malaysia negara yang bergantung sepenuhnya kepada keupayaan sendiri dalam bidang keselamatan siber.

Lt. Col. Husin Bin Jazri (Bersara), CISSP, CBCP
Pengarah dan Ketua Pegawai Eksekutif
CyberSecurity Malaysia

Cyber Security Awareness For Everyone

(CyberSAFE)

www.cyberSAFE.my

Securing Our Cyberspace

Best Brand Internet Security 2008 & 2009

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

CyberSecurity MALAYSIA

An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

INFORMATION SECURITY PROFESSIONAL DEVELOPMENT

SANS

CSSLP

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP

SYSTEMS SECURITY CERTIFIED PRACTITIONER
SSCP

EC-Council

DRI MALAYSIA
the institute for continuity management

KRYTERION HOST LOCATION

IQT

Securing Our Cyberspace

Best Brand Internet Security 2008 & 2009

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

CyberSecurity MALAYSIA
An agency under MOSTI

1Malaysia

MOSTI
Ministry of Science, Technology and Innovation

Operations Review

CyberSecurity Malaysia experienced one of its most interesting and challenging years in 2009 with the sustained threat to cyber security coming on top of a tentative world economy still reeling from the effects of the global financial crisis. Nevertheless, we persevered in addressing the cyber security needs of our clients and the nation while continuing to implement the programmes and projects set out in the 9th Malaysia Plan. We were given a boost as a fund recipient under the Second Economic Stimulus Package (ESP2) in our efforts to sustain the ICT security industry's contribution to the national economy. ESP2 also provided the support for us to enhance the collaboration between industry and government in securing the Critical National Information Infrastructure (CNII). During the year under review, we were successful in expanding our client base while encouraging service innovation to meet the rising challenges and demand for cyber security,

Since the establishment of CyberSecurity Malaysia in 2001, our services are now categorised into five areas of expertise or core services:

1. **Cyber Emergency Services**
   i. MyCERT – Cyber999
   ii. Digital Forensics – CyberCSI

2. **Security Quality Management Services**
   i. Security Management & Best Practices
   ii. Security Assurance Services
      - Malaysia ICT Security Evaluation Facilities (MySEF)
      - Malaysia Vulnerability Assessment Center (MyVAC)

3. **Malaysia Common Criteria Certification Body (MyCB)**

4. **Cyber Security Policy Research**
   i. Strategic Policy Research
   ii. Cyber Media Research
   iii. Policy Implementation Coordination

5. **InfoSecurity Professional Development & Outreach**
   i. InfoSecurity Professional Development
   ii. Outreach

Tinjauan Operasi

Tahun 2009 menyaksikan CyberSecurity Malaysia mengharungi banyak cabaran dan pengalaman menarik susulan dari pelbagai ancaman terhadap keselamatan siber ketika ekonomi dunia beransur-ansur pulih daripada krisis kewangan global. Bagaimanapun, kami tetap berjaya melindungi kepentingan keselamatan siber yang diperlukan semua pelanggan dan negara, di samping terus melaksanakan pelbagai program dan projek yang dirancang menerusi Rancangan Malaysia Kesembilan (RMK-9). Kami mendapat suntikan semangat sebagai penerima dana menerusi Pakej Rangsangan Ekonomi Kedua (ESP2), seiring usaha mengekalkan sumbangan industri keselamatan ICT terhadap ekonomi negara. ESP2 turut memberi sokongan untuk kami meningkatkan kerjasama di antara industri dan kerajaan dalam menubuhkan Prasarana Maklumat Kritikal Negara (CNII). Mengimbas kembali pencapaian sepanjang tahun lalu, kami telah berjaya memperluaskan pangkalan pelanggan dan menggalakkan inovasi perkhidmatan dalam usaha menangani lonjakan cabaran dan keperluan terhadap keselamatan siber.

Sejak CyberSecurity Malaysia diwujudkan pada 2001, perkhidmatan kami dibahagikan kepada lima bahagian kepakaran atau asas:

1. **Perkhidmatan Kecemasan Siber**
   i. MyCERT – Cyber999
   ii. Forensik Digital – CyberCSI

2. **Perkhidmatan Pengurusan Kualiti Keselamatan**
   i. Pengurusan & Amalan Terbaik Keselamatan
   ii. Perkhidmatan Jaminan Keselamatan
      - Malaysia ICT Security Evaluation Facilities (MySEF)
      - Malaysia Vulnerability Assessment Center (MyVAC)

3. **Badan Pensijilan Kriteria Bersama Malaysia (MyCB)**

4. **Penyelidikan Dasar Keselamatan Siber**
   i. Penyelidikan Dasar Strategik
   ii. Penyelidikan Media Siber
   iii. Penyelarasan Pelaksanaan Dasar

5. **Pembangunan Profesional Keselamatan Maklumat dan Capaian.**
   i. Pembangunan Profesional Keselamatan Maklumat
   ii. Capaian

CYBER EMERGENCY SERVICES

1. MyCERT – Cyber 999™

MyCERT (Malaysia Computer Emergency Response Team) has dealt with an increasing number of computer security incidents since its establishment in 1997. This rise in incidents has corresponded with the tremendous growth of internet usage in the country since the mid-1990s. Today, the most prevalent incidents include the denial of service, malware attacks, fraud and online harassment. Besides its primary role to maintain computer and cyber security, MyCERT also provides advisory services to domestic internet users as well as other international computer security incident response teams (CSIRTs).

For the year under review, MyCERT's Cyber999 service handled a total of 3,564 security incidents, representing a year-on-year increase of 68%. Added to this figure are another 43,287 incidents related to malware hosting, remote file inclusion (RFI) attacks and infection attempts that occurred in the research network operated by the Malware Research Centre. It is heartening to note that MyCERT registered an incident resolution rate of 98% or almost 46,000 incidents.

In dealing with these incidents, MyCERT handled 1,889,165 unique IP addresses affected by cyber threats, the most common of which were system intrusion followed by online fraud. More information on the incidents can be viewed at: http://www.mycert.org.my/en/services/statistic/mycert/2009/main/detail/625/index.html

As part of its mandate, MyCERT issued 61 security advisories related to various vulnerabilities in applications and security events in 2009. The list of advisories can be viewed at: http://www.mycert.org.my/en/services/advisories/mycert/2009/main/index.html

PERKHIDMATAN KECEMASAN SIBER

1. MyCERT – Cyber 999™

Semenjak penubuhannya pada 1997, MyCERT (Pasukan Tindak balas Kecemasan Komputer Malaysia) berdepan dengan peningkatan insiden yang membabitkan keselamatan komputer. Keadaan itu selari dengan peningkatan penggunaan internet yang memberangsangkan di negara ini sejak pertengahan 1990-an. Hari ini, antara masalah paling kerap dihadapi termasuk penidakan perkhidmatan, serangan *malware*, penipuan dan gangguan dalam talian. Selain peranan utamanya untuk mengekalkan keselamatan komputer dan alam siber, MyCERT turut menyediakan perkhidmatan nasihat kepada pengguna internet domestik dan Pasukan Tindak balas Insiden Kecemasan Keselamatan Komputer Antarabangsa (CSIRTs) yang lain.

Bagi tahun di bawah penilaian, perkhidmatan Pusat Bantuan Cyber999 MYCERT telah mengendalikan sejumlah 3,564 insiden keselamatan, iaitu peningkatan 68% berbanding tahun sebelumnya. Fakta ini ditambah dengan 43,287 insiden berkaitan perumahan malware (malware hosting), serangan remote file inclusion (RFI) dan percubaan serang jangkitan (infection attempts) yang berlaku dalam kajian rangkaian yang dikendalikan Pusat Kajian *Malware*. Seperkara membanggakan ialah kadar penyelesaian yang didaftar MyCERT telah mencecah 98 % atau kira-kira 46,000 insiden.

Dalam usaha menangani insiden-insiden ini, sehingga kini MyCERT mengendalikan 1,889,165 alamat IP unik yang mengalami ancaman siber, di mana insiden yang paling kerap berlaku ialah pencerobohan sistem, diikuti penipuan dalam talian. Maklumat lanjut mengenai insiden boleh dilihat di: http://www.mycert.org.my/en/services/statistic/mycert/2009/main/detail/625/index.html

Sebagai sebahagian daripada mandatnya, MyCERT turut mengeluarkan 61 peringatan keselamatan berkaitan pelbagai kelonggaran dalam aplikasi dan acara keselamatan pada 2009. Senarai peringatan boleh dilihat di: http://www.mycert.org.my/en/services/advisories/mycert/2009/main/index.html

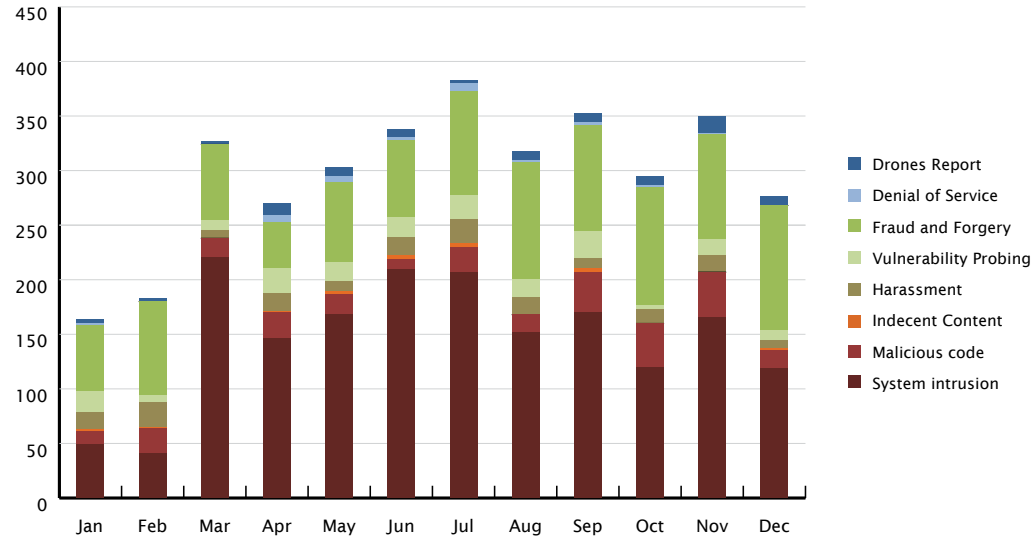


Figure 1: Incidents handled by MyCERT in 2009
Rajah 1: Insiden dikendalikan MyCERT pada 2009

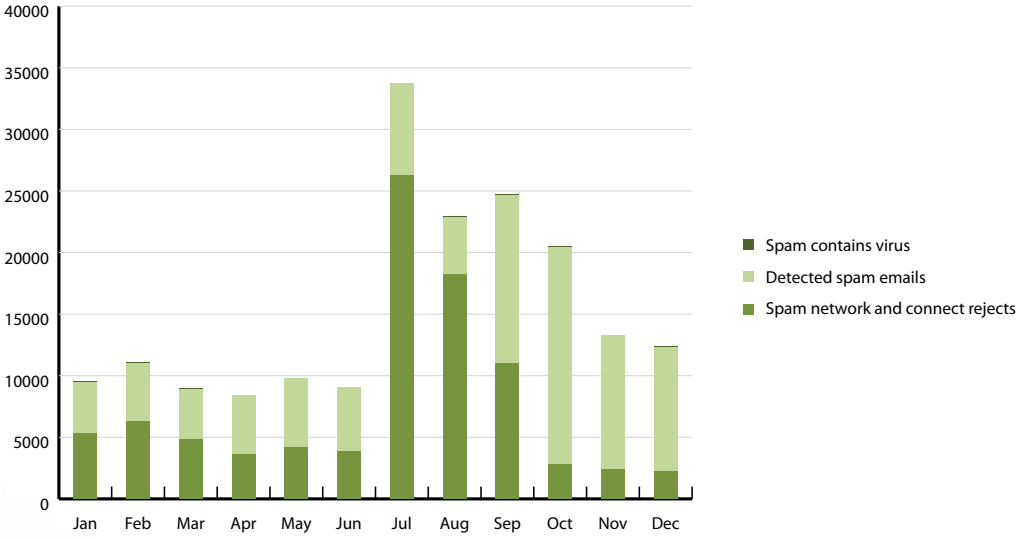


Figure 2: Spam handled by MyCERT in 2009
Rajah 2: Spam dikendalikan MyCERT pada 2009

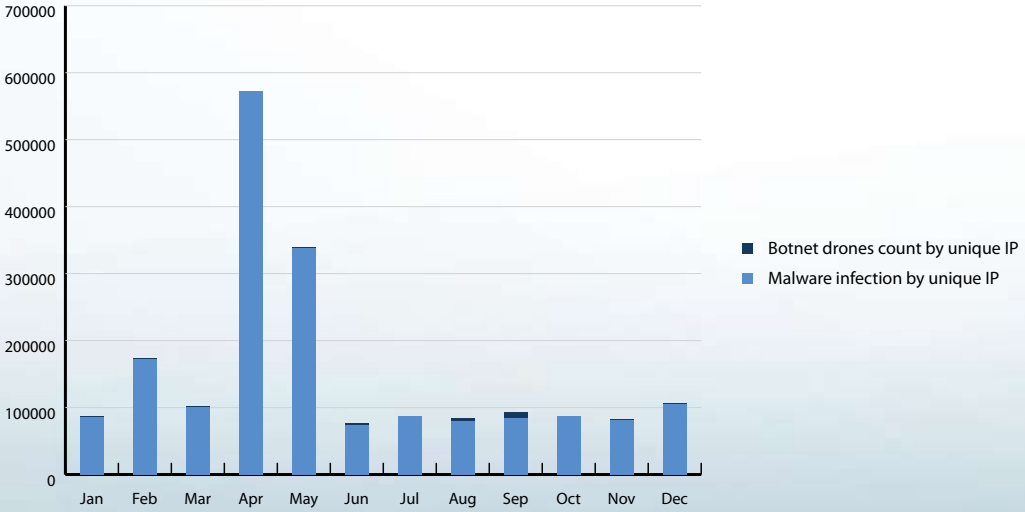


Figure 3: Infected computers handled by MyCERT in 2009
Rajah 3: Komputer terjejas dikendalikan MyCERT pada 2009

The most prominent of these security events was the 'Conficker' (also known as 'Downadup' and 'Kido') malware which exploited a relatively known vulnerability in the Microsoft Windows operating system. Apart from issuing a security advisory and press release, MyCERT also worked closely with .my Domain Registry, the Conficker Working Group and local Internet Service Providers (ISPs) to detect and warn owners of computers infected by Conficker.

1.1 Knowledge Sharing

Besides handling computer related incidents, MyCERT is also a point of reference for various organisations and participates in knowledge sharing and exchange program through various activities including conferences, training and seminars in both the domestic and international arenas.

In response to requests for assistance and guidance by the international community, MyCERT provided training to the Egypt Computer Emergency Response Team (EG-CERT) and the Oman National CERT (O-CERT) on handling computer security incidents.

In 2009, MyCERT also conducted hands-on training at the following events:

- Honeynet Hands-on Workshop at the OIC-CERT Conference 2009 (Honeynet Hands-on), Malaysia;
- Web Application Security Workshop at the FIRST Technical Colloquium KL 2009;
- Web Security Training (Web Security), Malaysia; and
- Web Intrusion: Practical Analysis with OSS Tools at the MSC Malaysia OSS Conference 2009.

As active participants in various international initiatives related to cyber security, MyCERT staff shared their expertise and experience at international conferences including:

- OIC-CERT Conference 2009, Malaysia;
- Asia Forum of IT, Thailand;
- Honeynet Project Annual Conference, Malaysia;
- APCERT AGM & Conference, Taiwan;
- APECTEL 39, Singapore;
- Anti-phishing Working Group CECOS III, Spain;
- Security Awareness Seminar - Institution of Engineering and Technology, Brunei;
- FIRST Annual Conference, Japan;
- ASEAN Law Enforcement Workshop, Indonesia; and
- FIRST-TC (Technical Colloquium) KL 2009, Malaysia.

MyCERT was involved in two cyber security exercises in 2009 - the ASEAN CERT Incident Drill (ACID) and the National Cyber Drill (X-Maya 2). CyberSecurity Malaysia coordinated and developed the drill scenarios for X-Maya 2, which was organised by the National Security Council (NSC). A total of 18 agencies from 10 CNII sectors took part in X-Maya 2 and engaged in incident handling activities such as malware analysis and application hardening.

1.2 Important Milestones

CyberSecurity Malaysia registered two significant milestones in 2009. They were the launch of Cyber999 on July 7, 2009 and launch of the CyberSecurity Malaysia Malware Research Centre on December 1, 2009, both by the Minister of Science, Technology and Innovation (MOSTI), Datuk Seri Dr Maximus Ongkili.

Cyber999 is the brand name of MyCERT's service to deal with cyber threats while the centre – referred to as 'HoneyNet' or 'LebahNet' – provides CyberSecurity Malaysia with a base to spearhead the nation's research and development to meet the threat of malware activities.

Malware yang paling ketara berkaitan aspek keselamatan ini ialah 'Conficker' (turut dikenali sebagai 'Downadup' dan 'Kido') di mana ia mengeksploitasi kelonggaran yang diketahui secara relatif wujud dalam sistem operasi Microsoft Windows. Selain daripada mengeluarkan peringatan keselamatan dan kenyataan media, MyCERT turut bekerja rapat dengan .my Domain Registry, Kumpulan Kerja Conficker dan Penyedia Perkhidmatan Internet (ISP) tempatan bagi mengesan dan memberi amaran kepada pemilik komputer yang diserang Conficker.

1.1 Perkongsian Pengetahuan

Selain menangani insiden berkaitan komputer, MyCERT juga adalah sumber rujukan bagi pelbagai organisasi dan mengambil bahagian dalam perkongsian serta pertukaran pengetahuan menerusi pelbagai aktiviti termasuk persidangan, latihan dan seminar di arena domestik dan antarabangsa.

Sebagai respon terhadap permintaan masyarakat antarabangsa untuk bantuan dan bimbingan, MyCERT menyediakan latihan kepada Pasukan Tindakbalas Kecemasan Komputer Egypt (EG-CERT) dan Oman National CERT (O-CERT) dalam menangani insiden keselamatan komputer.

Pada 2009, MyCERT turut mengadakan latihan langsung seperti berikut:
- Bengkel Langsung Honeynet pada Persidangan OIC-CERT 2009 (Honeynet Hands-on), Malaysia;
- Bengkel Keselamatan Aplikasi Web pada Kolokium Teknikal FIRST KL 2009;
- Latihan Keselamatan Web (Web Security), Malaysia; dan
- Pencerobohan Web: Analisis Praktikal Menggunaan Perkakasan OSS pada Persidangan MSC Malaysia 2009.

Sebagai peserta aktif di pelbagai inisiatif antarabangsa berkaitan keselamatan siber, kakitangan MyCERT berkongsi kepakaran dan pengalaman pada persidangan antarabangsa, antaranya:
- Persidangan OIC-CERT 2009, Malaysia;
- Forum IT Asia, Thailand;
- Persidangan Tahunan Projek Honeynet, Malaysia;
- AGM dan Persidangan APCERT, Taiwan;
- APECTEL 39, Singapura
- Kumpulan Kerja Anti-phishing CECOS III, Sepanyol;
- Seminar Kesedaran Keselamatan - Institut Kejuruteraan dan Teknologi, Brunei;
- Persidangan Tahunan FIRST, Jepun
- Bengkel Penguatkuasaan Undang-Undang ASEAN, Indonesia; dan
- FIRST-TC (Kolokium Teknikal) KL 2009, Malaysia.

MyCERT terbabit dengan dua dril keselamatan siber pada 2009 - Dril Insiden ASEAN CERT (ACID) dan Latih Amal Krisis Siber Kebangsaan (X-Maya 2). CyberSecurity Malaysia menyelaras dan membangunkan senario dril bagi X-Maya 2 anjuran Majlis Keselamatan Negara (NSC). Sebanyak 18 agensi daripada 10 sektor CNII telah mengambil bahagian dalam X-Maya 2 dan menyertai aktiviti menangani insiden seperti analisis malware dan pembekuan aplikasi (application hardening).

1.2 Pencapaian Penting

CyberSecurity Malaysia melakar dua pencapaian signifikan pada tahun 2009. Ia membabitkan pelancaran Cyber999 pada 7 Julai, 2009 dan pelancaran Pusat Kajian Malware CyberSecurity Malaysia pada 1 Disember, 2009, kedua-duanya telah disempurnakan perasmiannya oleh Menteri Sains, Teknologi dan Inovasi (MOSTI), Datuk Seri Dr Maximus Johnity Ongkili.

Pusat Bantuan Cyber999 ialah jenama perkhidmatan MyCERT bagi menangani ancaman siber manakala pusat berkenaan - dirujuk sebagai 'HoneyNet' atau 'LebahNet' – menyediakan asas bagi CyberSecurity Malaysia untuk meneraju kajian dan pembangunan negara dalam mengatasi ancaman aktiviti *malware*.

MyCERT also builds alliances with local and international organisations to extend cooperation and collaboration in understanding and handling computer security incidents, which are rarely isolated events. In 2009, MyCERT exchanged Memoranda of Understanding (MoUs) on the sharing of expertise and experience with the Egypt National CERT, the Taiwan Honeynet Project and Universiti Kuala Lumpur. These were in addition to existing partnerships with local internet service providers, the Asia Pacific Computer Emergency Response Teams (APCERT), Organisation of the Islamic Conference – Computer Emergency Response Teams (OIC-CERT), MY Domain Registry, Bank Negara Malaysia, the Ministry of Domestic Trade, Co-operatives and Consumerism, Royal Malaysian Police and other enforcement agencies.

1.3 Certification and Awards

In 2009, six MyCERT personnel achieved certification from the prestigious SANS (SysAdmin, Audit, Network, Security) Institute for SANS GPEN (Penetration Testing), SANS GCIH (Incident Handling) and the ISMS Lead Auditor. MyCERT was also recognised internationally when one of its employees received the ISC2 Information Security Leadership Achievement (ISLA) 2009 from the International Information Systems Security Certification Consortium, Inc. (ISC)²®.

MyCERT looks forward to the challenges and interesting engagements in 2010 and beyond. With the support of other services offered by CyberSecurity Malaysia, MyCERT will continue to position itself at the forefront in safeguarding the nation from cyber security threats.

2. Digital Forensics - CyberCSI

CyberSecurity Malaysia provides CyberCSI services to all law enforcement agencies (LEAs) and regulatory bodies (RBs) through its Digital Forensics Department (DFD) to deal with the rising number of cyber crimes involving different and increasingly sophisticated technologies. DFD is currently preparing to introduce a fully-fledged Digital Forensic Services with Standard Operating Procedure (SOP) in accordance to ASCLD/LAB-International (an ISO 17025 and American Society of Crime Lab Directors Standard dedicated to promoting excellence in forensic science through leadership and innovation).

For the year under review, DFD successfully analysed a total of 374 cases referred by LEAs and RBs such as the Royal Malaysian Police, Royal Malaysian Customs Department, Malaysian Communications and Multimedia Commission (MCMC), Companies Commission of Malaysia (CCM), Securities Commission (SC), the Ministry of Domestic Trade, Co-operatives and Consumerism, Malaysian Anti-Corruption Commission (MACC), the Ministry of Defence (MoD) and others.

Cumulatively between 2002 and 2009, DFD has assisted the LEAs and RBs on 1,186 cases with a broad case background. The number of cases in 2009, which included 50 onsite investigations, represents an increase of 26% over the previous year and reflects a trend that is expected to prevail in the years to come. Against this scenario, our digital forensics services are critical to the nation's cyber security and have already been included as a National Key Result Area (NKRA).

On all accounts, 2009 was a successful year for DFD with expert testimonies by our analysts leading to the closure of many cases brought on by the LEAs and RBs. CyberSecurity Malaysia is steadfastly committed to them in fighting cyber crimes in line with the DFD's vision in the Ninth Malaysia Plan (9MP) "To be a National Centre of Reference and Excellence in Digital Forensics with ASCLD/LAB-International Accreditation". We will continue to enhance our capabilities and capacities in digital forensics not only for the benefit of the nation, but also the global community.

MyCERT turut membentuk perikatan dengan organisasi tempatan dan antarabangsa dalam menawarkan kerjasama dan usahasama ke arah memahami dan menangani insiden keselamatan komputer yang kerap berlaku. Pada 2009, MyCERT bertukar Memorandum Persefahaman (MoU) bagi perkongsian kepakaran dan pengalaman dengan CERT Kebangsaan Egypt, Projek Honeynet Taiwan dan Universiti Kuala Lumpur. Ini adalah tambahan kepada kerjasama sedia ada dengan pengendali perkhidmatan tempatan, Pasukan Tindak balas Kecemasan Komputer Asia Pasifik (APCERT), Pasukan Tindak balas Kecemasan Komputer - Persidangan Pertubuhan Islam (OIC-CERT), MY Domain Registry, Bank Negara Malaysia, Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan, Polis Diraja Malaysia dan agensi penguatkuasaan lain.

1.3 Perakuan dan Anugerah

Pada 2009, enam kakitangan MyCERT telah mendapat perakuan daripada Institut SANS (SysAdmin, Audit, Network, Security) bagi SANS GPEN (Ujian Penembusan), SANS GCIH (Menangani Insiden) dan Auditor Pendahulu ISMS. MyCERT turut diiktiraf di peringkat antarabangsa apabila seorang daripada kakitangannya telah menerima anugerah menerusi Pencapaian Kepimpinan Keselamatan Maklumat (ISLA) ISC^2 2009 daripada International Information Systems Security Certification Consortium, Inc., (ISC)$^{2®}$.

MyCERT akan terus menyahut cabaran dan tuntutan tahun 2010 dan seterusnya. Dengan sokongan perkhidmatan lain yang ditawarkan CyberSecurity Malaysia, MyCERT akan terus mengukuhkan kedudukannya sebagai peneraju dalam melindungi negara daripada ancaman keselamatan siber.

2. Forensik Digital - CyberCSI

CyberSecurity Malaysia menawarkan perkhidmatan CyberCSI kepada semua agensi penguakuasa undang-undang (LEAs) dan badan kawal selia (RB) menerusi Jabatan Forensik Digital (DFD) dalam menangani peningkatan jenayah siber membabitkan teknologi berbeza dan semakin canggih. Ketika ini, DFD bersiap sedia untuk memperkenalkan Perkhidmatan Forensik Digital menyeluruh dengan Prosedur Operasi Standard (SOP) seperti ditetapkan oleh ASCLD/LAB-International (Standard Pengarah Makmal Jenayah mengikut Standard Masyarakat Amerika yang memiliki ISO 17025, khusus bagi mempromosi kecemerlangan sains forensik menerusi kepimpinan dan inovasi)

Bagi tahun penilaian, DFD berjaya menganalisis sejumlah 374 kes yang dirujuk oleh LEA dan RB seperti Polis Diraja Malaysia, Jabatan Kastam Diraja Malaysia, Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM), Suruhanjaya Syarikat Malaysia (SSM), Suruhanjaya Sekuriti (SC), Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan. Suruhanjaya Pencegahan Rasuah Malaysia (SPRM), Kementerian Pertahanan (MoD) dan lain-lain.

Secara kumulatif antara tahun 2002 hingga 2009, DFD telah membantu LEA dan RB dalam menangani sejumlah 1,186 kes berasaskan pelbagai rangkuman latar belakang. Bilangan kes dalam tahun 2009, termasuk 50 penyiasatan *onsite*, mewakili peningkatan 26% mengatasi tahun sebelumnya dan ini menggambarkan aliran yang dijangka berterusan dalam tahun-tahun akan datang. Berlatarkan senario ini, perkhidmatan forensik digital kami amat kritikal terhadap keselamatan siber negara dan disenaraikan sebagai Bidang Keberhasilan Utama Negara (NKRA).

Keseluruhannya, tahun 2009 merupakan tahun cemerlang bagi DFD dengan keterangan pakar oleh pengalnalisis kami membawa kepada penyelesaian banyak kes yang diketengahkan oleh LEA dan RB. CyberSecurity Malaysia amat komited dalam memerangi jenayah siber, sejajar visi DFD menerusi Rancangan Malaysia Kesembilan (RMK-9) "Untuk Menjadi Pusat Rujukan dan Kecemerlangan Kebangsaan bagi Forensik Digital berserta Akreditasi Antarabangsa-ASCLD/LAB". Kami akan terus meningkatkan keupayaan dan kemampuan di bidang forensik digital, bukan saja demi kepentingan negara tetapi merangkumi masyarakat global keseluruhannya.

As part of its knowledge sharing initiatives, DFD participated in several seminars and forums organised by various parties from the government, private sector and non-profit organisations. DFD also conducted training on digital forensics for LEAs and RBs including training to become Certified Fraud Examiners (CFE) under Bank Negara Malaysia. Our involvement and speaking engagements at local and international seminars, forums and workshops in 2009 include:

- Talk on Digital Forensics at International Symposium and Cybercrime Response, Seoul, South Korea;
- Talk on Digital Forensics at the OIC CERT Seminar, Kuala Lumpur;
- Ministry of Domestic Trade, Co-operatives and Consumerism (Perlis) Digital Forensics Workshop, Perlis;
- Cyber Security Talk at Institution of Engineers, Putrajaya;
- Talk on Prevention in Financial Crime & Bribery Forum, Kuala Lumpur;
- Talk on Digital Forensics at International Symposium of Forensic Science & Health of Environment, Kuala Lumpur; and
- Talk on Digital Forensics for Legal Department of the Inland Revenue Board of Malaysia, Kuala Lumpur.

DFD also conducted a highly-successful knowledge sharing session at Cyber Security Malaysia || SecureAsia@Kuala Lumpur on July 6 & 7, 2009. Attended by our Special Interest Group (SIG) mainly from the LEA and RBs, the event focused on addressing issues related to investigations involving digital evidence and adopting resolutions on moving forward. This SIG forum also included two digital forensic experts from Microsoft Asia and CEDAR Audio representatives who were invited as speakers. DFD presented several topics at the event such as ***'Quality Management in Digital Forensics Laboratory', 'Digital Media Investigation: The New Perspective'*** and '***Lawful Interception: The Time Is Now!'.***

Sebagai sebahagian daripada insiatif perkongsian pengetahuannya, DFD menyertai beberapa seminar dan forum anjuran pelbagai pihak meliputi sektor kerajaan, sektor swasta dan badan bukan kerajaan. DFD turut mengendalikan latihan forensik digital bagi LEA dan RB termasuk latihan untuk menjadi Pemeriksa Penipuan Bertauliah (CFE) di bawah Bank Negara Malaysia. Pembabitan kami dalam siri syarahan, seminar, forum dan bengkel tempatan serta antarabangsa sepanjang 2009 termasuk:

- Syarahan Forensik Digital di Simposium Antarabangsa Tindak balas Jenayah Siber, Seoul, Korea Selatan;
- Syarahan Forensik Digital di Seminar OIC-CERT, Kuala Lumpur;
- Bengkel Forensik Digital Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (Perlis), Perlis;
- Syarahan Keselamatan Siber di Institut Jurutera, Putrajaya;
- Syarahan Mengenai Pencegahan Jenayah Kewangan dan Forum Pemberian Rasuah, Kuala Lumpur;
- Syarahan Forensik Digital di Simposium Antarabangsa Forensik Digital dan Persekitaran Kesihatan, Kuala Lumpur; dan
- Syarahan Forensik Digital bagi Jabatan Perundangan Lembaga Hasil Dalam Negeri Malaysia, Kuala Lumpur.

DFD turut mengadakan sesi perkongsian pengetahuan yang mencapai kejayaan memberangsangkan menerusi CyberSecurity Malaysia || SecureAsia@Kuala Lumpur pada 6 & 7 Julai, 2009. Dihadiri oleh Kumpulan Kepentingan Khas (SIG) dengan sebahagian besarnya LEA dan RB, fokus acara itu ialah memberi penekanan terhadap isu berkaitan penyiasatan membabitkan bukti digital dan mencari penyelesaian untuk manfaat masa depan. Forum SIG turut membabitkan dua pakar forensik digital dari Microsoft Asia dan wakil CEDAR Audio yang dijemput memberi syarahan. DFD membentangkan beberapa topik seperti ***'Pengurusan Kualiti di Makmal Forensik Digital, 'Penyiasatan Media Digital: Perspektif Baru'*** dan ***'Pintasan Sah: Sekarang Masanya!"***

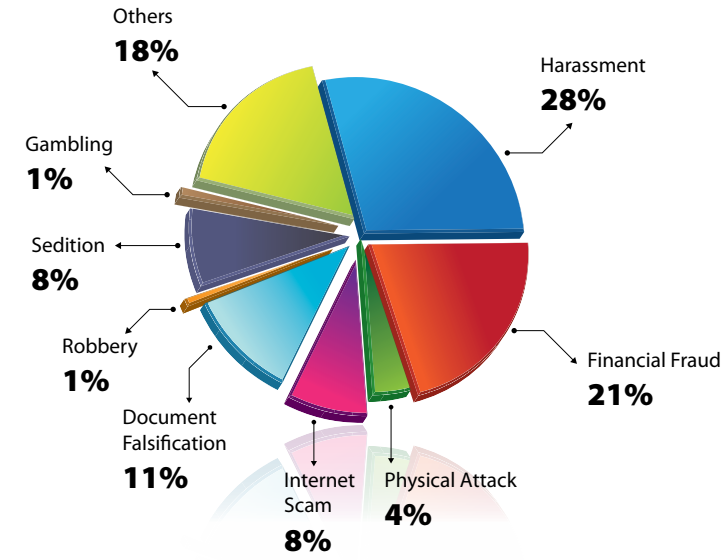


Figure 1: Case Background
Rajah 1: Latar belakang Kes

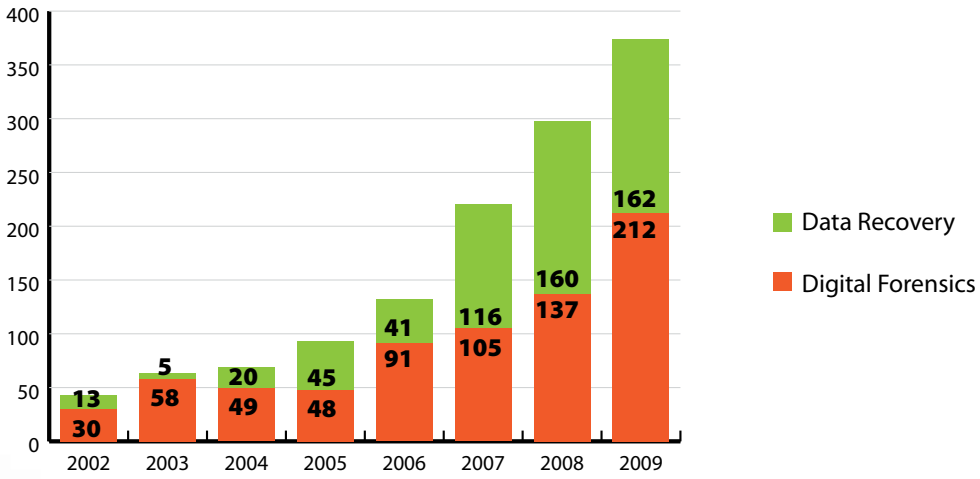


Figure 2: Yearly DF Case Statistics
Rajah 2: Statistik Tahunan Kes DF

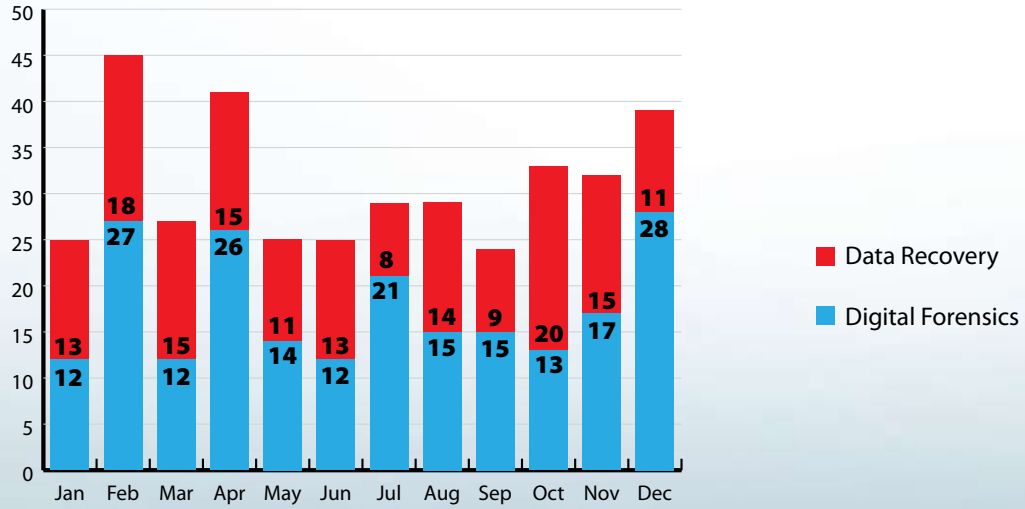


Figure 3: Monthly DF Cases Statistics
Rajah 2: Statistik Bulanan Kes DF

Research and Development is a critical aspect of digital forensics and an important purview of the DFD. Through our R&D efforts, we produced and distributed the second version of the Digital Forensics Live CD and Pocket Guide for Digital Forensics First Responders to LEAs and RBs. These products offer a guide and other useful information on digital forensics investigation.

We signed MoUs with local institutions of higher learning (IHLs) to create awareness and improve digital forensics capabilities through R&D programs. This included an MoU Management and Science University (MSU) to introduce a bachelor's degree in computer forensics. We also formed smart partnerships with local universities and colleges such as Universiti Teknologi MARA (UiTM), Universiti Utara Malaysia (UUM), Universiti Teknologi Malaysia (UTM), Universiti Kebangsaan Malaysia (UKM), Universiti Islam Antarabangsa (UIA) and Universiti Teknologi Petronas (UTP) for course module development, part-time lecturing, student internship programs and to supervise research programs at the post-graduate level. These initiatives are aimed at generating graduates with digital forensics expertise. We are heartened to note that they have resulted in increased student enrolment in this discipline.

The year 2009 marked another successful year for the DFD and is set to provide the springboard for future achievements under the 10th Malaysian Plan (10MP). We will continue to improve our service delivery by augmenting our skills and knowledge in digital forensics in the ever-escalating war against cyber crime.

SECURITY QUALITY MANAGEMENT SERVICES

1. Security Management and Best Practices (SMBP)

CyberSecurity Malaysia is at the forefront of efforts to promote, encourage and support the implementation of Security Management and Best Practices (SMBP) in information security among both public and private organisations in the country. CyberSecurity Malaysia has leveraged on SMBP to enhance its Information Security Management System (ISMS) and attain ISO/IEC 27001 certification after passing the annual surveillance audit. It is now well-placed to drive other organisations towards ISMS certification to secure the operating environment. In particular, CyberSecurity Malaysia is working to extend SMBP to CNII agencies in line with the directive by the Chief Secretary to the Government for critical organisations to be certified within three years.

To ensure the readiness of the organisation to provide critical services to stakeholders, the SMBP Department has consistently enhanced its Business Continuity programmes. It also played a significant role in the second annual Cyber Drill - codenamed X-MAYA2 - 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.

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 "Guideline on Identification, Collection/Acquisition and Preservation of Digital Evidence" presented at the SC27 Working Group meeting in Beijing in Maly 2009. Its subsequent approval represented a significant achievement and recognition of CyberSecurity Malaysia in ISO standards development. CyberSecurity Malaysia is currently working on the draft document which is expected to be published as an ISO/IEC 27037 document in 2011.

Penyelidikan dan Pembangunan (R&D) adalah antara aspek kritikal Forensik Digital, selain menjadi lingkungan penting DFD. Menerusi usaha R&D, kami menghasilkan dan mengagihkan versi kedua CD `Live' Forensik Digital dan Panduan bagi Responden Terawal Forensik Digital kepada LEA dan RB. Produk ini menawarkan panduan dan maklumat berguna berkaitan penyiasatan forensik digital.

Kami menandatangani MoU dengan institusi pengajian tinggi (IPT) bagi mewujudkan kesedaran dan memperbaiki kemampuan forensik digital menerusi program R&D. Ini termasuk MoU Universiti Pengurusan dan Sains (MSU) bagi memperkenalkan kursus Ijazah Sarjana Jurusan Forensik Komputer. Kami juga mengadakan kerjasama pintar dengan universiti dan kolej tempatan seperti Universiti Teknologi MARA (UiTM), Universiti Utara Malaysia (UUM), Universiti Teknologi Malaysia (UTM), Universiti Kebangsaan Malaysia (UKM), Universiti Islam Antarabangsa (UIA) dan Universiti Teknologi Petronas (UTP) bagi pembangunan modul kursus, syarahan separuh masa, program penempatan pelajar amali dan menyelia program kajian di peringkat lepasan ijazah. Inisiatif ini bermatlamat menambah bilangan graduan yang memiliki kepakaran forensik digital. Kami berbangga untuk memaklumkan tindakan itu mendorong kepada pertambahan penyertaan pelajar dalam bidang berkenaan.

Tahun 2009 merupakan satu lagi tempoh penuh kejayaan bagi DFD dan bersedia menjadi batu loncatan terhadap lebih banyak kejayaan masa depan di bawah Rancangan Malaysia ke-10 (RMK-10). Kami akan terus meningkatkan perkhidmatan dengan memperluaskan kepakaran dan pengetahuan di bidang forensik digital dalam memerangi jenayah siber yang semakin berleluasa.

PERKHIDMATAN PENGURUSAN KUALITI KESELAMATAN

1. Pengurusan & Amalan Terbaik Keselamatan (SMBP)

CyberSecurity Malaysia berada di barisan hadapan dalam mempromosi, menggalak dan menyokong pelaksanaan Pengurusan & Amalan Terbaik Keselamatan (SMBP) bagi keselamatan maklumat organisasi sektor awam dan swasta. CyberSecurity Malaysia menggerakkan SMBP supaya meningkatkan Sistem Pengurusan Keselamatan Maklumat (ISMS) dan meraih perakuan ISO/IEC 27001 selepas lulus audit pengawasan tahunan. Ia kini berada di landasan yang betul bagi membimbing organisasi lain ke arah mendapat perakuan ISMS dalam memelihara persekitaran operasi. Secara khususnya, CyberSecurity Malaysia sedang berusaha memperluaskan SMBP kepada agensi CNII sejajar dengan arahan Ketua Setiausaha Negara supaya organisasi kritikal perlu mendapat perakuan ISMS dalam tempoh tiga tahun.

Bagi memastikan kesediaan organisasi dalam menawarkan perkhidmatan kritikal kepada pelanggan, Jabatan SMBP meningkatkan program Kesinambungan Perniagaan secara konsisten. Ia turut memainkan peranan penting dalam Latih Amal Siber tahun kedua yang dikenali sebagai X-MAYA2, iaitu latihan stimulasi dan terselaras bagi menilai kesediaan keselamatan kecemasan siber CNII Malaysia dalam menentang serangan siber.

Sebagai sebahagian daripada tanggungjawabnya, jabatan ini turut membangunkan garis panduan dan amalan baik secara konsisten bagi kegunaan dalaman organisasi dan pengguna internet. Garis panduan ini menawarkan bimbingan dalam menangani peningkatan cabaran isu keselamatan dihadapi oleh masyarakat siber.

CyberSecurity Malaysia juga menyumbang kepada pembangunan piawaian keselamatan maklumat dan pengurusan berterusan perniagaan bagi badan tempatan dan antarabangsa. Organisasi ini menghasilkan secara bersama projek ISO "Garis panduan mengenai Pengenalan, Pengumpulan/ Pemerolehan dan Pemeliharaan Bukti Digital" yang dibentang pada mesyuarat Kumpulan Kerja SC27 di Beijing pada May 2009. Kelulusan yang diterimanya melambangkan pencapaian signifikan dan pengiktirafan ke atas CyberSecurity Malaysia mengikut pembangunan piawaian ISO. CyberSecurity Malaysia kini sedang merangka draf dokumen yang dijangka diterbitkan sebagai dokumen ISO/IEC 27037 pada 2011.

2. Security Assurance Department (SA)

In today's computing environment, trust is a predominant issue. A system is trusted when it behaves as expected. However, absolute security condition is something that is very difficult to achieve. The practical goal is to achieve a certain level of assurance that the system is trustworthy. The Security Assurance Department (SA) is entrusted to provide the security assurance services via two units - the Malaysia ICT Security Evaluation Facility (MySEF) and the National Vulnerability Assessment Centre (MyVAC)

- Malaysia ICT Security Evaluation Facility (MySEF)

The Malaysia ICT Security Evaluation Facility (MySEF) conducts independent evaluation of the security of ICT products aimed at establishing a level of confidence and assurance among users and consumers. By benchmarking against the Common Criteria (CC) (MS-ISO/IEC 15408) and the Common Evaluation Methodology (CEM) (MS-ISO/IEC 18405), MySEF helps to ensure the correct implementation and application of the service functionality of the products. The evaluation process encompasses such factors as the product design, development environment, delivery process, guidance documentation, testing procedures and also potential vulnerabilities.

During the year under review, MySEF applied for the Common Criteria evaluation facility licence from the MyCB (MyCC Certification Body) and is on track to obtain a full licence upon the completion of two evaluation projects. In December 2009, MySEF successfully passed the MS-ISO/IEC 17025 - The General Requirements for the Competence of Testing and Calibration Laboratories compliance audit by Standards Malaysia, which forms part of the licence requirements.

MySEF was also mandated to evaluate 30 local products under the Second Economic Stimulus Package (ESP2) programme in 2009. Via ESP2, MySEF was able to provide financial assistance to local ICT companies with the objective of increasing the number of homegrown products certified with the Common Criteria.

- National Vulnerability Assessment Centre (MyVAC)

The main mandate of the National Vulnerability Assessment Centre (MyVAC) is to continually assess the security posture of the Critical National Information Infrastructure (CNII) sectors with the aim of deterring and mitigating cyber threats. MyVAC conducts a Vulnerability Assessment and Penetration Testing (VAPT) on-site as well as off-site to identify potential vulnerabilities and at the same time, enhance the knowledge and skills in the areas of networking, wireless technologies, server operating systems, web applications and databases within these sectors. To date, MyVAC is equipped with two test laboratories: the Mobile and Network Security Test Lab and the Supervisory Control and Data Acquisition (SCADA) Security Test lab. Among the agencies that leveraged on MyVAC's services are the Ministry of Science, Technology and Innovation (MOSTI), the Royal Malaysian Police, the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), Universiti Sains Islam Malaysia (USIM), Universiti Putra Malaysia (UPM) and Universiti Pertahanan Nasional Malaysia (UPNM).

Under the Second Economic Stimulus Package (ESP2), MyVAC provided financial assistance for its Vulnerablility Assessment Service (VAS) to 30 CNII sectors. These included the Ministry of Science, Technology and Innovation (MOSTI), Office of the Chief Government Security Officer (CGSO), Immigration Department, National Registration Department, Ministry of Health (MoH), Inland Revenue Department, Road Transport Department, Westports Malaysia and Malaysia Airport Technologies Sdn Bhd.

A collaborative effort with the CGSO, this ESP2 VAS project also involved the assistance of 15 local security consultants: BDO Consulting, KPMG Malaysia, Diaspora, Intranium, Intellimicro Malaysia, Millenium Radius, Tri-IT, Extol MSC, PWC, SCAN Associates, iTania, Janasys, iProtocol, Time Engineering and Firmus Security.

In 2009, MyVAC was also involved in several events such as a dialogue session on CNII sectors organised by CGSO.

2. Jabatan Jaminan Keselamatan (SA)

Dalam persekitaran perkomputeran hari ini, kepercayaan adalah isu paling utama. Sesuatu sistem dipercayai sekiranya ia berfungsi seperti yang diharapkan. Bagaimanapun, keadaan keselamatan mutlak adalah sesuatu yang amat sukar dicapai. Sasaran praktikal ialah mencapai satu tahap jaminan bahawa sistem berkenaan boleh dipercayai. Jabatan Jaminan Keselamatan (SA) diberi kepercayaan menyediakan perkhidmatan jaminan keselamatan menerusi dua unit - Kemudahan Penilaian Keselamatan ICT Malaysia (MySEF) dan Pusat Penilaian Kelemahan Malaysia (MyVAC).

- Kemudahan Penilaian Keselamatan ICT Malaysia (MySEF)

Kemudahan Penilaian Keselamatan ICT Malaysia (MySEF) mengendalikan penilaian bebas berhubungan keselamatan produk ICT, bertujuan membentuk tahap keyakinan dan jaminan di kalangan pengguna. Dengan menetapkan Kriteria Umum (CC) (MS-ISO/IEC 15408) dan Metodologi Penilaian Umum (CEM) (MS-ISO/IEC 18405) sebagai penanda aras, MySEF membantu dalam memastikan pelaksanaan dan aplikasi yang betul supaya semua produk berfungsi seperti sepatutnya. Proses penilaian merangkumi faktor seperti reka bentuk produk, persekitaran pembangunan, proses penyampaian, pendokumentasian bimbingan, prosedur ujian dan kemungkinan kerentanan.

Sepanjang tahun kajian, MySEF memohon penilaian kemudahan bagi Kriteria Umum dari MyCB (Badan Perakuan MyCC) dan berada di landasan betul untuk mendapatkan lesen penuh, susulan siapnya dua projek penilaian. Pada Disember 2009, MySEF berjaya memperolehi MS-ISO/IEC 17025 - audit pematuhan Keperluan Umum bagi Kecekapan Menguji dan Makmal Pelarasan oleh Standards Malaysia yang membentuk sebahagian daripada keperluan lesen.

MySEF juga diberi kepercayaan menilai 30 produk tempatan di bawah program Pakej Rangsangan Ekonomi Kedua (ESP2) pada 2009. Menerusi ESP2, MySEF turut menyediakan bantuan kewangan kepada syarikat ICT tempatan, dengan objektif meningkatkan bilangan produk tempatan yang mendapat perakuan Kriteria Umum.

- Pusat Penilaian Kelemahan Malaysia (MyVAC)

Mandat utama Pusat Penilaian Kelemahan Malaysia (MyVAC) ialah menilai secara berterusan kerangka keselamatan sektor Prasarana Maklumat Kritikal Kebangsaan (CNII), dengan sasaran menangkis dan mengurangkan ancaman siber. MyVAC menjalankan Ujian Penilaian dan Penembusan Kerentanan (VAPT) di lokasi sebenar dan di luar lokasi bagi mengenal pasti kerentanan yang mungkin dihadapi dan pada masa sama, meningkatkan pengetahuan dan kepakaran jaringan, teknologi tanpa wayar, sistem operasi pelayan, aplikasi web dan pangkalan data di kalangan sektor ini. Ketika ini, MyVAC dilengkapi dua makmal ujian: Makmal Ujian Keselamatan Bergerak dan Perangkaian serta Makmal Ujian Keselamatan Kawalan Penyeliaan dan Perolehan Data (SCADA). Antara agensi yang mendapat manfaat perkhidmatan MyVAC ialah Kementerian Sains, Teknologi dan Inovasi (MOSTI), Polis Diraja Malaysia (PDRM), Unit Pemodenan Pentadbiran dan Perancangan Pengurusan (MAMPU), Universiti Sains Islam Malaysia (USIM), Universiti Putra Malaysia (UPM) dan Universiti Pertahanan Nasional Malaysia (UPNM).

Menerusi Pakej Rangsangan Ekonomi Kedua (ESP2), MyVAC menyediakan bantuan kewangan bagi Pusat Penilaian Kerentanan (VAS) kepada 30 sektor CNII. Ini termasuk Kementerian Sains, Teknologi dan Inovasi (MOSTI), Pejabat Pegawai Keselamatan Ketua Kerajaan (CGSO), Jabatan Imigresen, Jabatan Pendaftaran Negara, Kementerian Kesihatan (MoH), Lembaga Hasil Dalam Negeri, Jabatan Pengangkutan Jalan, Westports Malaysia dan Malaysia Airport Technologies Sdn Bhd.

Usahasama dengan CGSO, projek VAS ESP2 turut membabitkan bantuan 15 perunding keselamatan tempatan: BDO Consulting, KPMG Malaysia, Diaspora, Intranium, Intellimicro Malaysia , Millenium Radius, Tri-IT, Extol MSC, PWC, SCAN Associates, iTania, Janasys, iProtocol, Time Engineering dan Firmus Security.

Pada tahun 2009, MyVAC turut terbabit dalam beberapa majlis seperti sesi dialog mengenai sektor CNII anjuran CGSO.

MALAYSIA COMMON CRITERIA CERTIFICATION BODY (MyCB)

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 Information Technology – Security Techniques – Evaluation Criteria for IT Security. MyCB's formation as a certification body under CyberSecurity Malaysia was subsequent to 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 2009, MyCB focused its activities on promoting the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme to developers, consumers, government agencies, private organisations and others. The promotion is driven by advertising in the form of brochures, banners and print advertisement in the Malaysia SME Business Directory as well as talks and workshops in many parts of the country. For instance, MyCB gave a talk during the CyberSecurity Malaysia || SecureAsia@ Kuala Lumpur conference, at a series of MyCC Financial Assistance workshops in Kuala Lumpur and Ipoh, at the PIKOM regional workshop in Kuching, and also during exhibitions such as the PIKOM Leadership Summit 2009 and Pahang MSC Malaysia Launch.

MyCB capitalised on these events to distribute survey forms to gauge the demand for independent security evaluation and certification of ICT products in Malaysia as well as the public and local developer's understanding of the MyCC scheme.

The response from 276 individuals underscored the value of the MyCC scheme. Some 97% acknowledged the importance of security evaluation and certification for ICT products while 95% perceived certified products as being more valuable than non-certified ones. A similar percentage expressed confidence in developers' claims on the functions of certified ICT products. A total of 96% proclaimed support for the Government's effort to raise confidence levels in local ICT security products by conducting independent security evaluation and certification.

Local developers also agreed that there is a growing consumer demand for independent security evaluation and certification. They supported the view that certification of their ICT products would enhance their image and increase their prospects of enlarging market share.

However, some 37% of the respondents were not aware that CyberSecurity Malaysia offers ICT product security evaluation and certification services under the MyCC Scheme. To address this issue, MyCB is set aggressively promote the scheme through such means as media and video advertisement.

During the year, MyCB personnel participated in several international forums and meetings, both to represent Malaysia and to gain exposure in this vital field. Among the events were the Asian Information Security Evaluation and Certification (AISEC) Forum in Tokyo, the Annual International Common Criteria Conference (ICCC) and Common Criteria Recognition Arrangement (CCRA) working groups meeting in Norway. At these events, MyCB updated the international community on the development and establishment of the MyCC Scheme and its various initiatives moving forward.

CyberSecurity Malaysia also submitted an application to change the nation's CCRA participatory status from Consuming to Authorising to the Chairman of Common Criteria Management Committee (CCMC) in December 2009. A Shadow certification assessment by CCRA has been scheduled in 2010 and this will be an important milestone for the organisation.

BADAN PENSIJILAN KRITERIA BERSAMA MALAYSIA (MyCB)

Badan Pensijilan Kriteria Bersama Malaysia (MyCB) diwujudkan pada tahun 2008 bertujuan memberi penilaian dan perakuan produk dan sistem ICT tempatan yang memenuhi piawaian ISO/IEC 15408 Teknologi Maklumat – Teknik Keselamatan – Kriteria Penilaian bagi Keselamatan IT. Pembentukan MyCB sebagai badan perakuan di bawah CyberSecurity Malaysia adalah sejajar dengan penerimaan Malaysia sebagai ahli Perjanjian Pengiktirafan Kriteria Bersama (CCRA), piawaian antarabangsa bagi meraih pengiktirafan dan jaminan dari segi keselamatan ICT.

Pada tahun 2009, MyCB menumpukan aktiviti terhadap mempromosi Skim Penilaian dan Pensijilan Kriteria Bersama Malaysia (MyCC) kepada pemaju, pengguna, agensi kerajaan, organisasi swasta dan lain-lain. Promosi digerakkan dengan pengiklanan melalui brosur, pemidang dan iklan bercetak dalam Direktori Perniagaan PKS Malaysia selain syarahan dan bengkel di seluruh negara. Sebagai contoh, MyCB memberi syarahan pada Persidangan Cyber Security Malaysia || SecureAsia@Kuala Lumpur, beberapa siri bengkel Bantuan Kewangan MyCC di Kuala Lumpur dan Ipoh, bengkel wilayah PIKOM di Kuching, dan juga pameran seperti Sidang Kemuncak Kepimpinan PIKOM 2009 dan Pelancaran MSC Malaysia Pahang.

MyCB mengambil peluang melalui acara ini dengan mengedarkan borang kaji selidik bagi mengukur permintaan ke atas penilaian dan perakuan keselamatan bebas terhadap produk ICT di Malaysia, di samping melihat kefahaman pemaju awam dan tempatan mengenai Skim MyCC.

Maklumbalas daripada 276 individu menekankan nilai Skim MyCC. Kira-kira 97% menyedari kepentingan penilaian dan perakuan produk ICT manakala 95% menyifatkan produk diperakukan lebih bernilai berbanding yang tidak memiliki perakuan. Peratusan sama melahirkan keyakinan terhadap dakwaan pemaju mengenai fungsi produk ICT yang diperakukan. Sejumlah 96% menyatakan sokongan terhadap usaha Kerajaan meningkatkan tahap keyakinan produk ICT tempatan dengan mengadakan penilaian dan perakuan keselamatan bebas.

Pemaju tempatan turut mengakui wujud peningkatan permintaan daripada pengguna bagi penilaian dan perakuan keselamatan bebas. Mereka bersetuju dengan pendapat bahawa perakuan produk ICT akan meningkatkan imej masing-masing dan membuka peluang ke arah perluasan pasaran.

Bagaimanapun, kira-kira 37% responden tidak mengetahui CyberSecurity Malaysia menawarkan perkhidmatan penilaian dan perakuan produk ICT menerusi Skim MyCC. Bagi menangani isu ini, MyCB akan mempromosi skim berkenaan secara agresif menerusi pelbagai kaedah seperti iklan media dan video.

Tahun ini juga, kakitangan MyCB mengambil bahagian di dalam beberapa forum dan mesyuarat antarabangsa, kedua-duanya bagi mewakili Malaysia dan mendapat pendedahan di bidang penting ini. Antara yang disertai ialah Forum Penilaian dan Perakuan Keselamatan Maklumat Asia (AISEC) di Tokyo, Persidangan Tahunan Kriteria Umum Antarabangsa (ICCC) dan mesyuarat kumpulan kerja Perjanjian Pengiktirafan Kriteria Bersama (CCRA) di Norway. Di pertemuan itu, MyCB mengemaskini perkembangan pembangunan dan pengwujudan Skim MyCC dan pelbagai inisiatif disediakan sebagai persediaan untuk terus melangkah ke depan.

CyberSecurity Malaysia turut menghantar permohonan menukar status penyertaan CCRA negara daripada status menggunakan *(Consuming)* kepada penguatkuasa *(Authorising).* Permohonan ini dibuat kepada Pengerusi Jawatankuasa Pengurusan Kriteria Bersama (CCMC) pada Disember 2009. Penilaian perakuan awal oleh CCRA dijadualkan pada 2010 dan ia akan menjadi peristiwa penting bagi organisasi ini.

CYBER SECURITY POLICY RESEARCH

1. Strategic Policy Research Department (SPR)

The Strategic Policy Research Department (SPR) is responsible for all matters pertaining to strategic research and emerging cyber security issues. SPR is tasked with exploring new initiatives that have strategic impacts towards enhancing the nation's self reliance in cyberspace. In addition, the department is also responsible for identifying strategic collaboration with key organisations to enhance CyberSecurity Malaysia's position in global cyber security communities.

A major role of SPR is to prepare proposals that involve national policy matters for the consideration of relevant stakeholders such as the Ministry of Science, Technology and Innovation (MOSTI), the National Security Council (NSC), the National Cyber Security Coordination Committee (NC3) and the National Cyber Security Advisory Committee (NaCSAC) before being forwarded to the Cabinet. The proposals tabled and adopted in 2009 include 'Information Security Management Systems (ISMS)' and the 'Buy Malaysian First Policy for ICT Security Products' for critical sectors within the CNII. The department also submits monthly reports to MOSTI as one of the initiatives to enhance the awareness of stakeholder on the activities of CyberSecurity Malaysia and its contribution to the country. The department also provides advisories and feedbacks to various stakeholders, enabling them to make informed decisions pertaining to various strategic matters.

SPR spearheads the initiatives for the Organisation of The Islamic Conference – Computer Emergency Response Team OIC-CERT. CyberSecurity Malaysia is the co founder and presently the chair of this international collaboration and SPR is responsible for the formation and appointment of OIC-CERT to become an affiliated body to the OIC. SPR is now undertaking the promotion and membership drive for the OIC-CERT and leading the activities to meet the objectives of this collaboration.

Several strategic collaborations were established between CyberSecurity Malaysia and other OIC-CERT member countries under the OIC-CERT banner. Among the collaborative programs is to promote CyberSecurity Malaysia as a technical advisor in the establishment of CERT among OIC member nations.

On the home front, SPR led the initiative on 'A Study on the Laws of Malaysia to Accommodate the Legal Challenges in the Cyber Environment'. The outcome was tabled at the National IT Council chaired by the Prime Minister. The other initiative that is in progress is the development of the 'National Strategy for Cyber Security Acculturation and Capacity Building Program' aimed at securing the nation's cyberspace through acculturation and capacity building in cyber security.

2. Cyber Media Research Department (CMR)

Cyber Media Research Department (CMR) is responsible for provide ministerial papers and reports to the stakeholders pertaining to the development and issues in cyber security. To meet the stakeholders' expectations, CMR prepares papers such as the Memorandum to the Cabinet, Note to the Cabinet and official feedback to Parliamentary enquiries. One of the crucial papers is the monthly Note to the Cabinet on Cyber Incidences in Malaysia to continuously inform and update Cabinet Ministers on the gravity of cyber incidences in the country. In addition, CMR provides reports on potential cyber threats to MOSTI, the NSC and the Home Ministry.

CMR serves as the secretariat to a national committee overseeing the mitigation of cyber incidents in the country. CMR also manages the mailing list to facilitate communications among the committee members. To enhance this further, the department is spearheading the development of a portal that will provide a platform for an online forum to discuss issues at hand and facilitate information sharing.

PENYELIDIKAN DASAR KESELAMATAN SIBER

1. Jabatan Penyelidikan Dasar Strategik (SPR)

Jabatan Penyelidikan Dasar Strategik (SPR) bertanggungjawab bagi perkara berkaitan kajian strategik dan isu keselamatan siber semasa. SPR dipertanggungjawabkan untuk meneroka inisiatif baru yang mempunyai impak strategik terhadap meningkatkan kendiri negara di ruang siber. Sebagai tambahan, jabatan ini turut bertanggungjawab mengenal pasti usahasama strategik dengan organisasi utama ke arah melonjakkan kedudukan CyberSecurity Malaysia di kalangan masyarakat keselamatan siber global.

Fungsi utama SPR ialah menyediakan cadangan membabitkan dasar negara untuk pertimbangan pihak relevan seperti Kementerian Sains, Teknologi dan Inovasi (MOSTI), Majlis Keselamatan Negara (NSC), Jawatankuasa Penyelarasan Keselamatan Siber Kebangsaan (NC3) dan Jawatankuasa Penasihat Keselamatan Siber Kebangsaan (NaCSAC) sebelum diperpanjangkan ke Kabinet. Antara cadangan yang dibentang dan diterima pada 2009 termasuk `Sistem Pengurusan Keselamatan Maklumat (ISMS)' dan `Dasar Beli Barangan Produk Keselamatan ICT Malaysia Dahulu' bagi sektor kritikal di kalangan CNII. Jabatan turut menghantar laporan bulanan kepada MOSTI sebagai antara inisiatif meningkatkan kesedaran di kalangan pihak berkenaan terhadap aktiviti CyberSecurity Malaysia dan sumbangannya kepada negara. Jabatan turut menyediakan peringatan dan maklum balas kepada pelbagai pihak berkaitan yang membolehkan mereka membuat keputusan awal berhubung pelbagai permasalahan strategik.

SPR meneraju inisiatif Pasukan Tindak balas Kecemasan Komputer - Persidangan Pertubuhan Islam (OIC-CERT). CyberSecurity Malaysia adalah pengasas bersama dan ketika ini menjadi Pengerusi usahasama antarabangsa ini. SPR bertanggungjawab terhadap pembentukan dan pelantikan OIC-CERT sebagai badan bersekutu OIC. SPR sedang menggerakkan usaha promosi dan keahlian OIC-CERT dan mengetuai pelbagai aktiviti ke arah memenuhi objektif usahasama ini.

Beberapa usahasama strategik dibentuk di antara CyberSecurity Malaysia dan negara anggota OIC-CERT lain di bawah payung OIC-CERT. Antara program usahasama tersebut itu ialah mempromosi CyberSecurity Malaysia sebagai penasihat teknikal bagi penubuhan CERT di kalangan negara anggota OIC.

Di peringkat tempatan, SPR menerajui inisiatif 'Kajian Ke Atas Undang-Undang Malaysia Dalam Memenuhi Cabaran Perundangan bagi Persekitaran Siber'. Hasilnya dibentang pada Majlis IT Kebangsaan yang dipengerusikan Perdana Menteri. Inisiatif lain yang sedang dilakukan ialah `Strategi Kebangsaan Bagi Akulturasi Keselamatan Siber dan Program Pembinaan Keupayaan', bertujuan melindungi ruang siber negara menerusi akulturasi dan pembinaan keupayaan dari segi keselamatan siber.

2. Jabatan Penyelidikan Media Siber (CMR)

Jabatan Penyelidikan Media Siber (CMR) bertanggungjawab menyediakan kertas kementerian dan laporan kepada pihak berkaitan mengenai pembangunan dan isu-isu keselamatan siber. Dalam usaha memenuhi jangkaan pihak berkaitan, CMR menyediakan laporan seperti Memorandum kepada Kabinet, Nota kepada Kabinet dan maklumbalas rasmi kepada soalan Parlimen. Satu daripada laporan terpenting ialah Nota Bulanan kepada Kabinet Mengenai Insiden Siber di Malaysia bagi mengemaskini dan memaklumkan kepada Menteri Kabinet kedudukan insiden siber di negara ini. Sebagai tambahan, CMR menyediakan laporan kemungkinan ancaman siber kepada MOSTI, NSC dan Kementerian Dalam Negeri.

CMR berfungsi sebagai sekretariat kepada jawatankuasa kebangsaan yang mengendalikan pengurangan insiden siber di negara ini. CMR turut menguruskan senarai edaran bagi membantu komunikasi di kalangan ahli jawatankuasa. Bagi meningkatkan usaha ini, jabatan sedang membangunkan portal yang akan menyediakan platform bagi forum dalam talian untuk membincangkan isu semasa dan memudahkan perkongsian maklumat.

CMR conducts online research on existing and emerging cyber threats to develop and produce its reports. This is undertaken via a WebCrawler application jointly developed by CMR and the vendor. Trends and proposals are then collated, analysed and presented to the stakeholders. This ensures that stakeholders are better informed in the course of making decisions, formulating policies and developing guidelines for the country's information security initiatives.

In educating the public on cyber security issues, department staff regularly contribute articles for publication in various newspapers, magazine and related publications.

3. Policy Implementation Coordination (PIC)

The Policy Implementation Coordination Department (PIC) is dedicated towards implementing the National Cyber Security Policy (NCSP) and realising the government's vision of having a secured and safe cyber environment especially for the CNII sectors. CyberSecurity Malaysia has been given the mandate to oversee the implementation of the NCSP under the purview of MOSTI. Two committees were formed to facilitate the implementation of the NCSP and they are the National Cyber Security Coordination Committee (NC3) and the National Cyber Security Advisory Committee (NaCSAC). PIC is the co-secretariat together with MOSTI for both committees.

The NC3 is a national committee chaired by the Secretary General of MOSTI to oversee the implementation of the NCSP. New policies on framework or guidelines can be escalated to the NaCSAC, chaired by the Chief Secretary to the Government, for endorsement. As the secretariat, PIC provides members of the committees with sound advice on moving forward.

The NCSP's vision is that 'Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation'. To realise this vision, the nation's CNII sectors comprising Ministries, regulators and organisations must work together in a coordinated fashion under the guidance of the NC3 and NaCSAC.

Three NC3 meetings were held, on January 9, April 3 and July 2, 2009. This was followed by a National Cyber Security Advisory Committee (NaCSAC) meeting on July 17, 2009. NaCSAC accepted two cyber security proposals to be implemented under the NCSP initiatives. They are:

- The Information Security Management Systems (ISMS) certification for the CNII entities. The policy requires all CNII entities to adopt MS ISO/IEC 27001:2006 – ISMS (or its equivalent) and attain certification within three years;
- 'Buy Malaysia First' for ICT Products'. All CNII entities are to accord priority to local ICT products for installation within their critical systems. Preference is now given to ICT products with certification on the security functions. This effort will ensure that Malaysia can be self reliant in ICT security and contribute to the growth the nation's economy.

Aside from coordinating these committee meetings, PIC is also actively involved in several key initiatives aimed at protecting Malaysia's CNII entities, including:

- organising the 'Critical National Infrastructure Protection (CNIP) Conference' in collaboration with the Chief Government Security Office (CGSO) on July 6, 2009;
- conducting the 2009 annual CNII questionnaire survey and the first risk assessment exercise on selected CNII entities. This is done in collaboration with the CGSO, Ministry of Information, Communication & Culture (MICC) and National Security Council (NSC). On September 2009, a workshop was held to brief the selected CNII organisations and regulators on the annual survey and Risk Assessment exercise;
- participating in the national Cyber Drill 2009 (X-Maya 2) on December 9, 2009 as the secretariat for the National Cyber Coordination and Control Centre (NC4); and

Dalam membina dan menghasilkan laporan, CMR melakukan kajian dalam talian mengenai ancaman siber sedia ada dan berterusan. Tugas ini dilakukan menerusi aplikasi WebCrawler yang dibangunkan bersama oleh CMR dan vendor. Aliran dan cadangan kemudiannya digabung, dianalisis dan dibentang kepada pihak berkenaan. Ini bagi memastikan mereka memahami keadaan sebenar sebelum membuat keputusan, merangka dasar dan membangunkan garis panduan bagi inisiatif keselamatan maklumat negara.

Dalam mendidik masyarakat umum mengenai isu keselamatan siber, kakitangan jabatan sentiasa menghantar artikel bagi siaran di pelbagai media seperti akhbar, majalah dan penerbitan berkaitan.

3. Penyelarasan Pelaksanaan Dasar (PIC)

Penyelarasan Pelaksanaan Dasar (PIC) dikhususkan ke arah melaksanakan Dasar Keselamatan Siber Nasional (NCSP) dan menyedari visi kerajaan untuk memiliki persekitaran siber yang terjamin dan selamat, terutama bagi sektor CNII. CyberSecurity Malaysia telah diberi mandat untuk menyelia pelaksanaan NCSP di bawah skop MOSTI. Dua jawatankuasa dibentuk bagi membantu pelaksanaan NCSP, iaitu Jawatankuasa Penyelarasan Keselamatan Siber Kebangsaan (NC3) dan Jawatankuasa Penasihat Keselamatan Siber Kebangsaan (NaCSAC). PIC juga adalah sekretariat bersama dengan MOSTI bagi kedua-dua jawatankuasa.

NC3 adalah jawatankuasa kebangsaan yang dipengerusikan oleh Ketua Setiausaha MOSTI bagi menyelia perlaksanaan NCSP. Dasar baru mengenai kerangka atau garis panduan boleh dikemukakan kepada NaCSAC yang dipengerusikan Ketua Setiausaha Negara untuk pengesahan. Sebagai sekretariat, PIC menyediakan nasihat berguna kepada ahli jawatankuasa untuk terus melangkah ke hadapan.

Visi NCSP ialah 'Prasarana Maklumat Kritikal Kebangsaan Malaysia mesti sentiasa selamat, bingkas dan memiliki kebergantungan sendiri. Diperkukuhkan dengan budaya keselamatan, ia akan mengutamakan kestabilan, kesenangan sosial dan ruang kemakmuran'. Bagi menjayakan visi ini, sektor CNII negara merangkumi Kementerian, pengawal selia dan organisasi mesti bekerjasama secara teratur di bawah bimbingan NC3 dan NaCSAC.

Tiga mesyuarat NC3 diadakan iaitu pada 9 Januari, 3 April dan 2 Julai 2009. Ini disusuli dengan mesyuarat Jawatankuasa Penasihat Keselamatan Siber Kebangsaan (NaCSAC) pada 17 Julai , 2009. NaCSAC menerusi dua cadangan keselamatan siber untuk dilaksanakan menerusi inisiatif NCSP iaitu:

- Perakuan Sistem Pengurusan Keselamatan Maklumat (ISMS) bagi entiti CNII . Dasar ini memerlukan semua entiti CNII mengguna pakai MS ISO/IEC 27001:2006 – ISMS (atau setarafnya) dan mendapatkan perakuan dalam tempoh tiga tahun;
- 'Beli Barangan Malaysia Bagi Produk ICT'. Semua entiti CNII perlu memberi keutamaan kepada produk ICT tempatan bagi pemasangan dalam lingkungan sistem kritikal masing-masing. Keutamaan kini diberi kepada produk ICT yang mempunyai perakuan fungsi keselamatan. Usaha ini akan memastikan Malaysia memiliki kebergantungan sendiri dalam keselamatan ICT dan menyumbang kepada pertumbuhan ekonomi negara.

Selain daripada menyelaras mesyuarat jawatankuasa berkenaan, PIC juga terbabit secara aktif di dalam beberapa inisiatif utama yang bertujuan melindungi entiti CNII Malaysia, termasuk:

- menganjurkan 'Persidangan Perlindungan Prasarana Kritikal Kebangsaan (CNIP)' dengan kerjasama Pejabat Keselamatan Ketua Kerajaan (CGSO) pada 6 Julai, 2009;
- mengendalikan kaji selidik dan latihan penilaian risiko pertama tahunan 2009 ke atas entiti terpilih CNII. Ini dilakukan dengan kerjasama CGSO, Kementerian Penerangan, Komunikasi dan Kebudayaan (MICC) dan Majlis Keselamatan Negara (NSC). Pada September 2009, satu bengkel diadakan untuk memberi perangan kepada organisasi dan badan kawal selia CNII terpilih berhubung kaji selidik tahunan dan latihan penilaian risiko;
- menyertai Latih Amal Siber kebangsaan (X-Maya 2) pada 9 Disember, 2009 sebagai sekretariat bagi Penyelarasan Keselamatan Siber Nasional (NC4); dan

- participating and presenting papers at key international conferences and seminars on critical information infrastructure protection, such as:
  - the 5th Meridian Conference, Oct 28-30, 2009, organised by the Department of Homeland Security, USA;
  - ITU Cybersecurity Forum in Hyderabad, Sept 23 -25, 2009; and
  - The 2nd APEC Seminar on Protection of Cyberspace from Terrorist Use and Attacks (November 18 – 19, 2009), organised by the Ministry of Foreign Affairs and Trade, Republic of Korea and APEC Counter Terrorism Task Force (CTTF) in Seoul, Republic of Korea. This seminar was held mainly to discuss the various issues pertaining to the protection of cyberspace from terrorist use and attacks.

INFOSECURITY PROFESSIONAL DEVELOPMENT AND OUTREACH

1. Infosecurity Professional Development

InfoSecurity Professional Development (ISPD), formerly known as the Training Department, spearheads CyberSecurity Malaysia's efforts to share knowledge and experience with industry experts to provide relevant training to other organisations.

ISPD has introduced additional courses in 2009 to fulfill its commitment to generate more Information Security professionals in the country and response to the rising trend in cyber threats. We initiated a Malaysian Information Security Professionals networking program to enhance knowledge sharing among professionals and recognition within the professional community.

As an organisation entrusted to ensure the security of cyberspace in Malaysia, our expertise and services are widely sought after to provide training and counsel 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.

In the year 2009 we have successfully collaborated with the following organisations:

a) Disaster Recovery Institute (DRI) Malaysia.
b) EC Council Academy (M) Sdn Bhd
c) ISC^2

We have also seen an increase in number of Information Security professionals from 608 in the year 2008 to 924 in the year 2009. These partnerships help us to organise workshops, road-shows and prepare for the certification.

2. Outreach

The tremendous growth of the internet over the past two decades has dramatically transformed the way we work, play and live. Today, the internet is driving the creation of new businesses and facilitating the operations of traditional ones. It is empowering communities and societies at large by providing access to information and avenues for networking.

As one of the first developing nations to embrace the power of the internet, Malaysia has experienced an exponential growth in the number of internet users. Encouraged by the Government and fuelled by the establishment of MSC Malaysia in 1997, internet penetration is now at 59% with 15 million users and climbing fast.

- menyertai dan membentang kertas kerja pada persidangan utama dan seminar antarabangsa mengenai perlindungan Prasarana maklumat kritikal, seperti:
  - Persidangan Meridian ke-5, 28-30 Okt, 2009, anjuran Jabatan Keselamatan Negara, Amerika Syarikat;
  - Forum ITU Cybersecurity di Hyderabad, 23 -25 Sept, 2009; dan
  - Seminar Perlindungan Ruang Siber Daripada Kegunaan dan Serangan Pengganas APEC ke-2 (18 – 19 November, 2009), anjuran Kementerian Luar dan Perdagangan, Republik Korea dan Pasukan Petugas Menangani Keganasan (CTTF) APEC di Seoul, Republik Korea. Seminar ini diadakan bagi membincangkan pelbagai isu membabitkan perlindungan ruang siber daripada kegunaan dan serangan pengganas.

PEMBANGUNAN PROFESIONAL KESELAMATAN MAKLUMAT DAN CAPAIAN

1. Pembangunan Profesional Keselamatan Maklumat

Pembangunan Profesional Keselamatan Maklumat (ISPD), dulu dikenali sebagai Jabatan Latihan, menerajui usaha-usaha CyberSecurity Malaysia untuk berkongsi ilmu dan pengalaman dengan pakar-pakar industry untuk memberi latihan-latihan relevan kepada organisasi-organisasi lain.

ISPD telah memperkenalkan kursus-kursus tambahan pada 2009 untuk memenuhi komitmen untuk menghasilkan lebih ramai ahli professional di bidang Keselamatan Maklumat di Malaysia dan tindak balas ke atas trend ancaman siber yang kian meningkat. Kami mengasaskan program rangkaian Profesional Keselamatan Maklumat Malaysia untuk menggalakkan perkongsian ilmu di antara ahli-ahli professional dan pengiktirafan di dalam komuniti profesional tersebut

Sebagai sebuah organisasi yang diamanahkan untuk memastikan keselamatan alam siber di Malaysia, kepakaran dan perkhidmatan kami amat dicari untuk menyediakan latihan dan nasihat bagi pembangunan Pasukan Tindak balas Kecemasan Komputer (CERT), Sistem Pengurusan Keselamatan Maklumat (ISMS), Pengurusan Kesinambungan Perniagaan (BCM), teknologi Wayarles, pengujian Penetrasi, SCADA dan Forensik Digital.

Pada 2009, kami telah berjaya bekerjasama dengan organisasi-organisasi berikut:

a) Disaster Recovery Institute (DRI) Malaysia.
b) EC Council Academy (M) Sdn Bhd
c) ISC²

Kami juga telah melihat kenaikan jumlah ahli-ahli profesional Keselamatan Maklumat daripada 608 pada 2008 kepada 924 pada 2009. Perkongsian ini membantu kami untuk menganjurkan bengkel-bengkel, road-shows dan menediakan pensijilan

2. Capaian (Outreach)

Pertumbuhan hebat internet sejak dua dekad lalu telah mengubah cara kita bekerja, bermain dan menjalani kehidupan secara dramatik. Kini, internet menjadi daya penggerak pertumbuhan perniagaan baru dan memudahkan operasi perniagaan-perniagaan yang lama. Ia mengupayakan komuniti dan masyarakat umumnya dengan memberi akses kepada maklumat dan ruang untuk membina rangkaian.

Sebagai salah satu negara membangun pertama yang mendakap kuasa Internet, Malaysia telah mengalami kadar pertumbuhan eksponen di dalam jumlah pengguna internet. Dengan galakkan Kerajaan dan dirangsang pula oleh penubuhan MSC Malaysia pada 1997, penetrasi internet kini adalah pada kadar 59% dan meningkat dengan cepat.

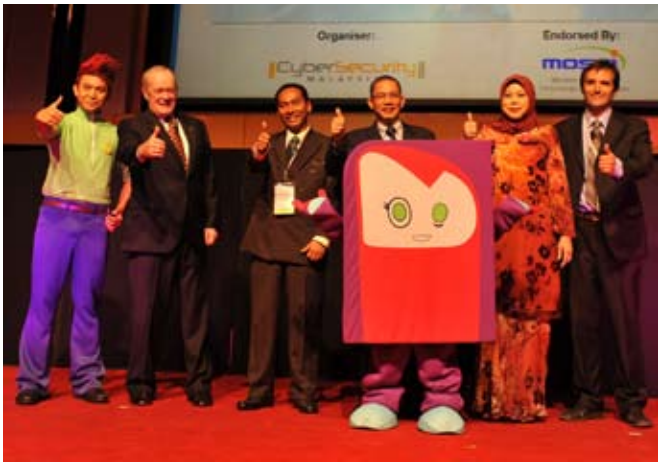
According to statistics from the Malaysian Communications and Multimedia Commission (MCMC), some 20% of Malaysian households are equipped with broadband while the growth of Mobile Wireless Broadband users almost tripled in 2009 to 3.8 million. Meanwhile, our mobile penetration rate is well over 100%.

From these numbers, it is becoming increasingly clear that more users are accessing the internet through 3G mobile connection, at cybercafés and WIFI hotspots. It is also interesting to note that one out of every four internet users is below the age of 19, which means 25% of our internet users are schoolchildren.

With easy access to internet connectivity, our children have the opportunity of going online outside our homes without supervision. This is particularly common in urban areas where even children in primary schools have mobile phones with internet access capability. This is certainly a matter of serious concern that requires careful consideration.

While the internet opens up borders and provides a wealth of information, it also allows unscrupulous internet predators to commit crimes which had previously been restricted to the real world. These borderless crimes are usually targeted at the gullible and the innocent among our children. Most of the time, they are too naïve and too trusting towards what they read and who they meet online.

Our only realistic means of protecting them from undesirable elements and influences on the internet is to provide them with the necessary education and knowledge as to the dangers and issues of internet behavior.



This is where CyberSecurity Malaysia, as the national specialist centre in cyber security, plays a role through its CyberSAFE program.

CyberSAFE, short for Cyber Security Awareness For Everyone, is CyberSecurity Malaysia's initiative to educate and enhance the awareness of the general public on the technological and social issues facing internet users, particularly on the dangers of getting online. The Outreach Department has been entrusted to roll out the CyberSAFE program to its targeted audience: -children, youths, parents as well as other adults and organisations.

The Department's main activities for 2009 include the following:

- **Launch of CybersSAFE Portal – August 9, 2009**
  CyberSecurity Malaysia's new internet safety awareness portal with more dedicated content for target groups was launched by Haji Fadillah Hj Yusof, Deputy Minister of MOSTI. Present during the launch were Datuk Lee Kim Shin, Assistant Minister for Infrastructure Development and Communication, representatives of Members of Parliament and the State Assembly, representatives from the Department of Education Miri, and teachers and secondary students from around Miri.

- **CyberSAFE Awareness Talks**
  Our full-day or half-day talks on internet safety have reached pupils, teacher and parents from more than 150 schools nationwide.

Mengikut statistik Suruhanjaya Komunikasi dan Multimedia (SKMM), lebih kurang 20% isi rumah di Malaysia telah pun dilengkapkan dengan jalur lebar sementara pertumbuhan pengguna jalur lebar telefon mudah alih meningkat hamper tiga kali ganda pada 2009 kepada 3.8 juta. Manakala penetrasi telefon mudah alih meningkat lebih 100%.

Daripada perangkaan tersebut, ianya menunjukkan bahawa lebih ramai pengguna menggunakan internet melalui telefon mudah alih 3G, di kafe-kafe siber dan pusat-pusat WIFI. Menariknya, satu daripada empat pengguna internet adalah di bawah umur 19 tahun, bermakna 25% pengguna internet kita adalah murid-murid sekolah.

Dengan akses mudah kepada internet, anak-anak kita memiliki kesempatan untuk berada dalam talian di luar rumah tanpa pengawasan. Ini adalah perkara biasa terutamanya di kawasan bandar di mana ada murid-murid sekolah rendah juga mempunyai telefon mudah alih yang mempunyai keupayaan akses internet. Ini tentunya perkara yang membimbangkan dan memerlukan pertimbangan yang teliti.

Walaupun internet membuka sempadan dan menyediakan lebih banyak maklumat, ia juga membolehkan pemangsa internet yang tidak bermoral untuk melakukan jenayah yang sebelumnya dihadkan di dunia nyata. Jenayah-jenayah tanpa batasan ini biasanya disasarkan kepada mereka yang mudah terpedaya dan kanak-kanak yang tidak bersalah. Pada kebiasaannya, mereka terlalu naif dan terlalu percaya kepada apa yang mereka baca, dan siapa mereka bertemu dalam talian.

Cara realistik untuk kita melindungi mereka daripada unsur-unsur dan pengaruh yang tidak diingini di internet adalah dengan menyediakan mereka dengan pendidikan dan pengetahuan yang diperlukan tentang bahaya dan isu-isu tingkah laku internet.

Di sinilah CyberSecurity Malaysia, sebagai pusat pakar keselamatan siber nasional, berperanan melalui program CyberSAFE.

CyberSAFE, adalah kata pendek untuk Cyber (Siber) Security (Keselamatan) Awareness (Kesedaran) For (Untuk) Everyone (Semua), ianya adalah sebuah inisiatif CyberSecurity Malaysia untuk mendidik dan meningkatkan kesedaran orang ramai tentang isu sosial dan teknologi yang didepani pengguna internet, terutamanya bahaya berada dalam talian. Jabatan Capaian (Outreach Department) telah diamanahkan untuk mengembangkan program CyberSAFE kepada kumpulan sasar - kanak-kanak, remaja, ibu-bapa dan juga orang dewasa dan organisasi.

Aktiviti-aktiviti utama Jabatan pada 2009 termasuk:

- **Pelancaran Portal CybersSAFE - 9 Ogos 2009**
  Portal kesedaran keselamatan internet CyberSecurity Malaysia yang baru dengan lebih pengisian untuk kumpulan sasar telah dilancarkan oleh YB Haji Fadillah Hj Yusof, Timbalan Menteri MOSTI. Hadir sama di pelancaran tersebut termasuklah Datuk Lee Kim Shin, Penolong Menteri Pembangunan Prasarana dan Komunikasi, wakil-wakil Ahli-ahli Parlimen dan Dewan Undangan Negeri, wakil-wakil Jabatan Pelajaran Miri dan guru-guru dan murid-murid sekolah menengah sekitar Miri.

- **Syarahan Kesedaran CyberSAFE**
  Syarahan sepenuh atau separuh hari mengenai keselamatan internet telah mencapai murid-murid, guru-guru dan ibu-bapa di lebih 150 sekolah di seluruh negara.

- **CyberSAFE Ambassadors Program – December 2009**
  CyberSAFE Ambassadors are selected from among students, teachers, and parents to champion CyberSAFE. They are provided with the necessary knowledge and resources to spread the CyberSAFE message.

- **Internet Safety Awareness Seminar – Internet & Family Values and Launch of Nic & Pxl – July 8, 2009**
  This was a full-day seminar attended by more than 300 secondary schoolchildren with parallel sessions for educators and parents.

Internationally, we have also been invited to present at international events such as the following:

- ITU/MIC Strategic Dialogue on Safer Internet Environment for Children on June 2-3, 2009 in Tokyo, Japan;

- Safer Internet Forum in Luxembourg on October 22-23, 2009; and

- Awareness Seminar in Brunei hosted by Authority for Info-communications Technology Industry of Brunei Darussalam (AITI).

Overall, our activities for 2009 have created the right momentum for us to move our Internet Safety Awareness agenda to even greater heights in 2010.

- **Program Duta CyberSAFE - Disember 2009**
  Duta CyberSAFE dilantik di antara murid-murid, guru-guru dan ibu-bapa untuk menguar-uarkan CyberSAFE. Mereka dilengkapi dengan ilmu dan sumber yang diperlukan untuk menghebahkan mesej CyberSAFE.

- **Seminar Kesedaran Keselamatan Internet - Nilai Kekeluargaan & Internet dan Pelancaran Nic & Pxl - 8 Julai 2009**
  Seminar satu hari ini dihadiri oleh lebih 300 murid-murid sekolah menengah dengan sesi selari untuk pendidik dan ibu-bapa.

Di peringkat antarabangsa, kami juga telah menerima undangan untuk member penerangan di acara-acara antarabangsa seperti di bawah:

- Dialog Strategik ITU/MIC tentang Persekitaran Lebih Selamat untuk Kanak-Kanak 2-3 Jun, 2009 di Tokyo, Jepun;

- Forum Internet Lebih Selamat di Luxembourg pada 22-23 Oktober 2009; dan

- Seminar Kesedaran di Brunei anjuran Authority for Info-communications Technology Industry of Brunei Darussalam (AITI).

Secara keseluruhannya, aktiviti-aktiviti kami pada tahun 2009 telah menghasilkan momentum yang tepat untuk kami menggerakkan agenda Kesedaran Keselamatan Internet ke arah yang lebih gemilang pada 2010.

Strategic Partnership 2009 Kerjasama Strategik

Partnership with APCERT
Kerjasama dengan APCERT

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

Partnership with OIC-CERT
Kerjasama dengan 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
Kerjasama dengan lain-lain Negara CERT

- 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
Kerjasama dengan Institusi Antarabangsa

- 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 ISESCO
- 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
Kerjasama Strategik Peringkat Nasional

- .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

Corporate Governance

STATEMENT OF CORPORATE GOVERNANCE

The Board of Director 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 conduct its business.

All selected members of the Board must obtained the prior approval from the Minister of Domestic Trade, Co-operatives and Consumerism (MDTCC).

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 18 to 24 of the Annual Report.

Tadbir Urus Korporat

PENYATA TADBIR URUS KORPORAT

Lembaga Pengarah CyberSecurity Malaysia dengan sukacitanya melaporkan bahawa pada tahun kewangan yang ditinjau, CyberSecurity Malaysia terus melaksanakan amalan tadbir urus korporat yang memuaskan dalam mengurus dan menerajui hala tuju perkembangan CyberSecurity Malaysia, iaitu dengan menerima pakai isi kandungan dan semangat prinsip sepertimana yang diperlukan oleh Kod Malaysia mengenai Tadbir Urus Korporat ("Kod").

TANGGUNGJAWAB LEMBAGA PENGARAH

Lembaga Pengarah merangka dan menyemak pelan strategik CyberSecurity Malaysia setiap tahun bagi menyelaras hala tuju operasi serta aktiviti CyberSecurity Malaysia supaya selaras dengan tujuan penubuhannya oleh Kerajaan Malaysia.

Lembaga Pengarah menimbang secara mendalam dan jika difikirkan sesuai, meluluskan untuk pelaksanaan perkara-perkara utama yang memberi kesan kepada CyberSecurity Malaysia termasuk perkara-perkara berkenaan pelan tindakan dan belanjawan tahunan, perbelanjaan utama, pembelian dan penjualan aset, dasar sumber manusia dan prestasi pengurusan. Lembaga Pengarah turut menyemak pelan tindakan yang dilaksanakan oleh Pengurusan untuk mencapai sasaran perniagaan dan operasi.

Lembaga Pengarah juga mengawasi operasi dan perniagaan CyberSecurity Malaysia dengan meminta pengurusan menghantar laporan operasi dan kewangan secara berkala dengan kerap, selain menetapkan piawaian minimum serta menggubal dasar berkenaan pengurusan risiko operasi dan bidang-bidang utama lain dalam aktiviti yang dijalankan oleh CyberSecurity Malaysia.

Tugas-tugas lain Lembaga Pengarah termasuk mengawasi secara kerap operasi dan prestasi CyberSecurity Malaysia serta memastikan supaya Prasarana, kawalan dalaman dan process pengurusan risiko sudah tersedia ada.

KOMPOSISI LEMBAGA PENGARAH

Lembaga Pengarah terdiri daripada para individu yang sangat berkaliber, mempunyai kemahiran, kepimpinan serta berpengalaman luas dalam bidang kepakaran masing-masing yang membolehkan mereka menyediakan sokongan kukuh terhadap pelaksanaan tugas and tanggungjawab mereka. Mereka menjalankan peranan dengan melaksanakan pertimbangan secara bebas dan menyertai secara bermatlamat, dalam perbincangan Lembaga Pengarah sambil pada masa yang sama, menjaga kepentingan pemegang kepentingan, pekerja, pelanggan serta komuniti di mana CyberSecurity Malaysia menjalankan operasinya.

Semua ahli Lembaga Pengarah yang dipilih perlu mendapat kelulusan daripada Menteri Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (KPDNKK) terlebih dahulu.

Sekurang-kurangnya setengah daripada jumlah komposisi Ahli-ahli Lembaga Pengarah hendaklah terdiri daripada sektor kerajaan dan dilantik oleh Menteri Sains, Teknologi dan Inovasi. Ahli-ahli selebihnya di ambil daripada sektor perdagangan atau sektor lain yang berkaitan yang dipilih oleh Ahli-ahli CyberSecurity Malaysia di Mesyuarat Agungnya. Kini terdapat lapan (8) orang ahli Lembaga Pengarah CyberSecurity Malaysia.

Lembaga Pengarah dibantu sepenuhnya dan secara berkesan dalam pengurusan harian CyberSecurity Malaysia oleh Ketua Pegawai Eksekutif serta pasukan pengurusan beliau.

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 2009, six (6) Board Meetings and two (2) meetings by way of circular resolutions were held.

APPOINTMENT, RETIREMENT BY ROTATION 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. However, other Members of the Board are to retire by rotation upon the expiry of their terms of directorship. One-third of the Members of the Board for the time being shall retire each year by rotation, or if the number is not a multiple of three (3) then the nearest to one third shall retire. The Member's of the Board is to retire in every year shall be those who have been longest in office since their last election, but if there are two (2) or more persons who became a Member of the Board on the same day, those to retire shall (unless they otherwise agree among themselves) be determined by lot.

YBhg. Dato' Madinah binti Mohamad, Director of CyberSecurity Malaysia is not subject to retirement since she is representing MOSTI. Lt. Col. 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. YBhg Datuk Abang Abdul Wahap bin Abg Julai and YBhg Datuk Dr Abdul Raman bin Saad tendered their retirement by rotation pursuant to Articles 49 and 51of 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 Fourth Annual General Meeting 2010.

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.

MESYUARAT LEMBAGA PENGARAH DAN BEKALAN MAKLUMAT KEPADA LEMBAGA PENGARAH

Mesyuarat Lembaga Pengarah diadakan secara kerap, di mana laporan mengenai kemajuan perniagaan, operasi serta minit mesyuarat Jawatankuasa Lembaga Pengarah CyberSecurity Malaysia dibentangkan untuk disemak oleh Ahli-ahli Lembaga Pengarah. Di mesyuarat Lembaga Pengarah ini, Ahli-ahli Lembaga Pengarah turut menilai cadangan perniagaan dan operasi serta cadangan korporat yang memerlukan kelulusan Lembaga Pengarah.

Agenda bagi setiap mesyuarat Lembaga Pengarah, bersama dengan laporan pengurusan, kertas cadangan serta dokumen sokongan yang komprehensif diberikan kepada semua Pengarah untuk penelitian mereka supaya Pengarah berkenaan mempunyai masa yang mencukupi untuk menyemak perkara-perkara yang akan dibincangkan di mesyuarat Lembaga Pengarah dan untuk memudahkan Lembaga Pengarah membuat keputusan.

Pada akhir tahun kewangan 2009, CyberSecurity Malaysia telah mengadakan enam (6) Mesyuarat Lembaga Pengarah dan dua (2) mesyuarat melalui resolusi pekeliling.

PELANTIKAN, PERSARAAN MENGIKUT GILIRAN DAN PEMILIHAN SEMULA AHLI-AHLI LEMBAGA PENGARAH

Ahli-ahli Lembaga Pengarah yang mewakili Kementerian Sains, Teknologi dan Inovasi ("MOSTI") tidak tertakluk kepada persaraan. Walau bagaimanapun, Ahli-ahli lain dalam Lembaga Pengarah perlu bersara mengikut giliran selepas tamat tempoh memegang jawatan mereka. Satu pertiga daripada Ahli-ahli Lembaga Pengarah buat masa ini akan bersara setiap tahun mengikut giliran atau jika bilangan tersebut bukan dalam gandaan tiga (3), angka yang terdekat kepada satu pertiga akan bersara. Ahli-ahli Lembaga Pengarah yang bersara setiap tahun adalah ahli yang paling lama memegang jawatan sejak pemilihan sebelumnya, tetapi sekiranya terdapat dua (2) ahli Lembaga Pengarah atau lebih yang telah menjadi Ahli Lembaga Pengarah pada hari yang sama sebelumnya, persaraan akan (kecuali mereka sebaliknya bersetuju di kalangan mereka) ditentukan melalui pemilihan.

YBhg. Dato' Madinah binti Mohamad Lembaga Pengarah CyberSecurity Malaysia tidak tertakluk kepada persaraan kerana beliau mewakili MOSTI. Lt. Col. Husin Hj Jazri (Bersara), sebagai Ketua Pegawai Eksekutif pula tertakluk kepada persaraan menurut tempoh perkhidmatan beliau dengan CyberSecurity Malaysia dan terma serta syarat yang berkaitan dengannya. YBhg. Datuk Abang Abdul Wahap bin Abg Julai dan YBhg. Datuk Dr Abdul Raman bin Saad telah menghantar surat persaraan mereka mengikut giliran berhubung Tataurusan 49 dan 51 dalam Tataurusan Pertubuhan CyberSecurity Malaysia. Mereka menawarkan diri untuk dipilih sebagai Pengarah dan akan dipertimbangkan untuk kelulusan para Ahli CyberSecurity Malaysia di Mesyuarat Agung Tahunan Keempat yang akan berlangsung pada tahun 2010.

PENDIDIKAN BERTERUSAN PARA PENGARAH

Para Pengarah digalakkan supaya menghadiri ceramah, program latihan dan seminar untuk mengemaskini diri mereka dengan perkembangan terbaru berkaitan industri di mana CyberSecurity Malaysia beroperasi.

MESYUARAT AGUNG TAHUNAN

Mesyuarat Agung Tahunan merupakan forum utama untuk berdialog dan berinteraksi degan Ahli-ahli CyberSecurity Malaysia yang terdiri daripada MOSTI dan Kementerian Kewangan (Diperbadankan) (MOF (Inc.)). Ahli-ahli diberikan peluang untuk mengemukakan soalan mengenai perkara dalam agenda mesyuarat agung tahunan yang diadakan. Notis mesyuarat dan laporan tahunan dihantar kepada Ahli-ahli CyberSecurity Malaysia sekurang-kurangnya 21 hari sebelum tarikh mesyuarat Tataurusan Pertubuhan 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.

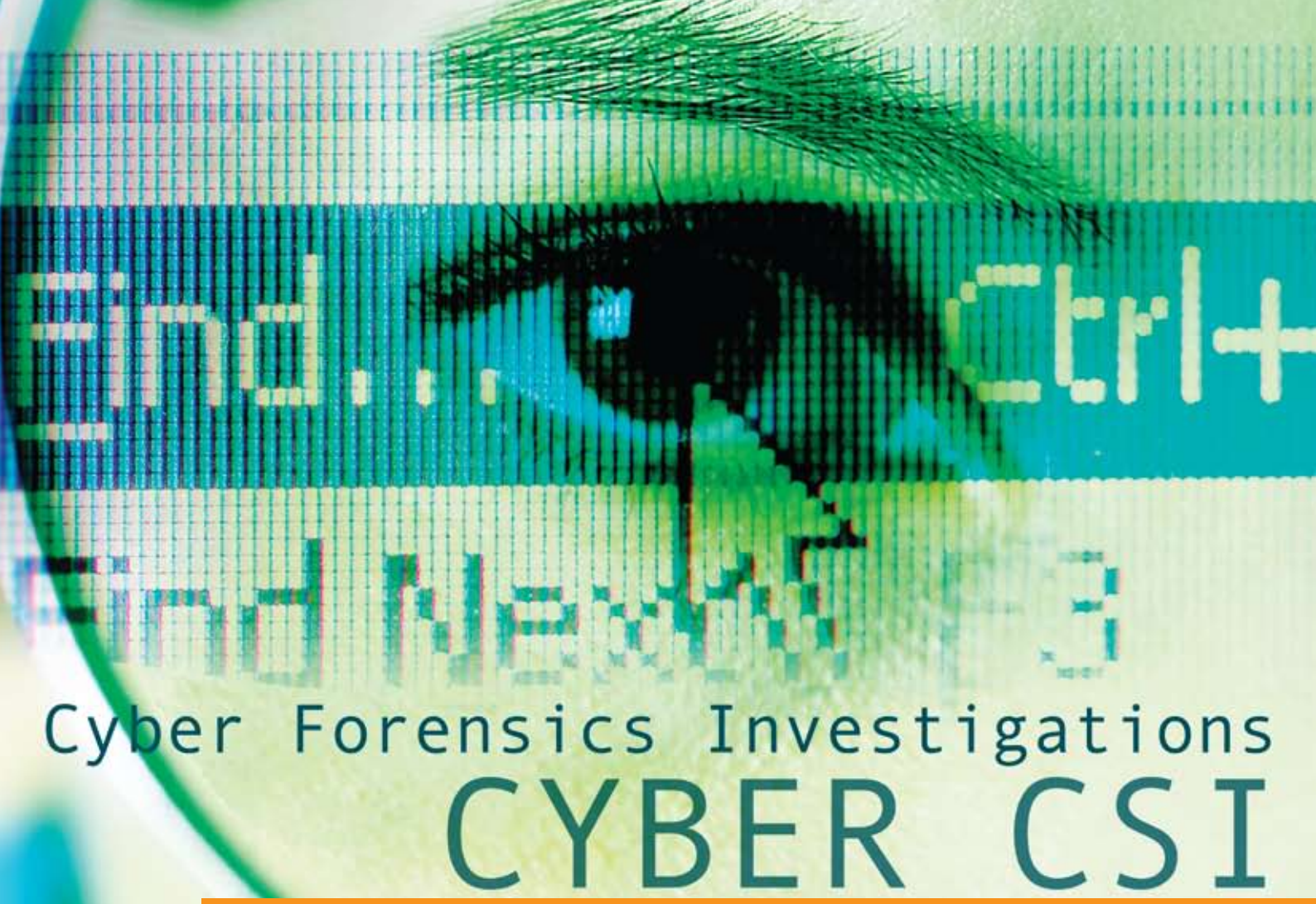
KAWALAN DALAMAN DAN PENGURUSAN RISIKO

Lembaga Pengarah bertanggungjawab terhadap sistem kawalan dalaman CyberSecurity Malaysia dan juga keberkesanannya. Walau bagaimanapun, sistem sedemikian direka untuk mengurus risiko CyberSecurity Malaysia dalam had profil risiko yang boelh diterima, bukannya menghapus risiko kegagalan mencapai dasar dan objektif perniagaan CyberSecurity Malaysia. Walau bagaimanapun, penetapan dan pengekalan sebuah sistem kawalan dalaman mampu menyediakan jaminan berpatutan tentang keberkesanan dan kecekapan operasi dan pematuhan kepada undang-undang dan peraturan serta prosedur dan garis panduan dalaman.

Melalui Pengurusan, Lembaga Pengarah, telah menjalankan satu process berterusan untuk mengenalpasti, menilai dan mengurus risiko operasi dan kewangan utama yang berhadapan dengan CyberSecurity Malaysia. Ia dilaksanakan dengan menyemak kawalan dan pengurusan risiko sedia ada, melaksana dan menerapkan budaya dan fungsi pengurusan risiko ke dalam CyberSecurity Malaysia.

Program kawalan dan pengurusan risiko dalaman yang ditetapkan oleh Lembaga Pengarah termasuk dasar dan prosedur mengenai risiko dan kawalan dengan mengenalpasti serta menilai risiko yang dihadapi dan merangka operasi dan pemantauan kawalan dalaman yang sesuai bagi mengawas serta mengawal semua risiko ini.

Lembaga Pengarah berpendapat bahawa sistem kawalan dalaman yang tersedia pada tahun yang ditinjau dan sehingga tarikh penerbitan laporan tahunan dan penyata kewangan ini adalah mencukupi untuk menjaga kepentingan para pemegang kepentingan, pelanggan, penguatkuasa peraturan dan kakitangan serta aset CyberSecurity Malaysia.



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 operations can be undertaken such as hard disk data analysis, retrieval of deleted file, intrusion tracking and discovery.

Securing Our Cyberspace

Activities Throughout 2009
Aktiviti Sepanjang Tahun 2009

Activities Throughout 2009

JANUARY 2009

Seminar and First Quarterly Meeting of the Organisation of the Islamic Conference- Computer Emergency Response Team (OIC-CERT) Member Countries
CyberSecurity Malaysia ushered in 2009 by organizing the OIC-CERT Seminar 2009. This two-day seminar was attended by 303 participants, of which 267 were local and 36 from overseas, mainly from the OIC member countries such as Brunei, Indonesia, Pakistan, Bangladesh, Saudi Arabia, Iran, Oman, Jordan, Syria, Turkey, Tunisia, Maghribi, Nigeria, Egypt and Libya. In conjunction with OIC-CERT Seminar 2009, the Annual General Meeting of OIC-CERT was also held. 16 OIC countries and representatives from the OIC Secretariat of Jeddah, Saudi Arabia and from IDB Area Office, Kuala Lumpur attended the meeting At the meeting, Malaysia, via CyberSecurity Malaysia was appointed as OIC-CERT Chair for two consecutive terms, 2009 2011.

Other activities:

- National Cyber Security Coordination Committee (NC3) Meeting 1/2009
- The Information Technology Chief and two (2) officers from the Digital Forensic Department of the French International Criminal Police Organisation (INTERPOL) paid a visit to CyberSecurity Malaysia.
- A Corporate Social Responsibility (CSR) program organized by CyberSecurity Malaysia was held at Kampung Simpang Arang, Gelang Patah, Johor. At the ceremony, CyberSecurity Malaysia contributed five (5) computers for the usage of orang asli students.
- Corporate Social Responsibility Project MOSTI - INFOSTI@MOSTI: Train The Trainer. CyberSecurity Malaysia conducted a training session for prospective trainers who will be training the community in Sabah.
- CyberSecurity Malaysia attended the High Technology Crime Investigation Association (HTCIA) International (HTCIA) Summit in Hong Kong.

FEBRUARY 2009

Carnival and Launch of INFOSTI@MOSTI Centre
Through our involvement as a committee member and council secretariat, CyberSecurity Malaysia was instrumental in making the carnival and launch of INFOSTI@MOSTI a success. It was held at Kota Marudu, Sabah and officiated by YB Datuk Seri Maximus Johnity Ongkili, Minister of Science, Technology and Innovation. Similar ceremony was held at Kota Semariang Batu, Petrajaya, Kuching and officiated by YB Tuan Haji Fadillah Yusof, Deputy Minister of Science, Technology and Innovation. This initiative was one of MOSTI's CSR programs to narrow the digital gap of rural residents and help them to be knowledgeable and savvy in IT. In conjunction with the carnival, CyberSecurity Malaysia organized a one-day "Train the Trainer" session at Kampung Semariang Batu, Kuching, Sarawak. CyberSecurity Malaysia also organized INFOSEC.my in Sarawak. The half a day session was officiated by YB Tuan Haji Fadillah bin Haji Yusuf. A total of 250 students and teachers from 23 secondary schools around Kuching attended this program. The students were given exposure to issues related to internet security and how to overcome them.

Other activities:

- Blue Ocean Strategy Seminar - attended by 31 participants from the management team of CyberSecurity Malaysia.
- Participated in the Meeting of the Economic Research Institute for ASEAN and East ASIA (ERIA). CyberSecurity Malaysia is one of the project group members of ERIA. The Project ERIA focuses on the utilization of common benchmarks among East Asian countries for information security.
- A training session on Network Security Monitoring (NSM) was organized by CyberSecurity Malaysia. Participants comprised staff from CyberSecurity Malaysia, Telekom Malaysia Berhad, TIME dotcom Berhad, .my DOMAIN REGISTRY (previously known as MYNIC Berhad) and JARING Communications Sdn. Bhd.
- Involved in the launch of Public Sector Trustmark Meeting by the Ministry of International Trade and Industry (MITI).

MARCH 2009

Forum On Managing The Impact Of The Economic Crisis On the ICT Industry
CyberSecurity Malaysia co-organized the forum together with the Ministry of Science, Technology and Innovation (MOSTI). The forum was officiated by YB Datuk Seri Dr Maximus Johnity Ongkili, the Minister.

Working Visits to CyberSecurity Malaysia
CyberSecurity Malaysia received several visits from various Organisations. Amongst the Ministries, agencies and institutions of higher learning that visited CyberSecurity Malaysia were:

- **2 March 2009** Students from Bachelor of IT, UiTM Perlis;
- **5 March 2009** Students from the Faculty of Science & Technology; Universiti Sains Islam Malaysia (USIM);
- **10 March 2009** Students from Diploma In Computer Science, UiTM Johor;
- **19 March 2009** - Web Site Task Force for the Ministry of Energy, Water and Communications;
- **23 March 2009** – Participant in a Cyber Crime Investigation Course Series 1/2009, Royal Police Laboratory;
- **24 March 2009** – Ministry of Science, Innovation and Technology;
- **24 March 2009** – Participant in Introductory Course for Cyber Ad Control, Ministry of Health, Malaysia (Enforcement Division)

Other activities:

- Attended the Annual General Meeting and Asia Pacific Computer Emergency Response Team (APCERT) Summit 2009.
- Google-Fu Training: Power Search Techniques Edition was conducted for the Ministry of Energy, Water and Communications and Securities Commission

APRIL 2009

National Cyber Security Policy Action Plan Workshop (NCSP) and Meeting of the National Cyber Security Administration Committee (NC3) bil. 1/2009
The National Cyber Security Policy Action Plan Workshop (NCSP) and a Meeting for the Administration Committee of National Cyber Security (NC3) bil. 1/2009 was held at Putrajaya International Convention Centre (PICC) on 2 April 2009. A total of 32 participants comprising Senior Officers from Government Departments and Agencies attended this workshop.

39th APEC Telecommunication And Information Working Group (APECTEL)
CyberSecurity Malaysia was part of the Malaysian delegation headed by Ministry of Energy, Water and Communications to the 39th APEC Telecommunication and Information Working Group (APECTEL), held at Suntec Convention Centre, Singapore. During the event, CyberSecurity Malaysia organized Security and Prosperity Steering Group session (SPSG) on 17 April 2009. This session exposed CyberSecurity Malaysia to the various cyber security-related initiatives and strategic issues which are taking place at international levels. In addition, CyberSecurity Malaysia presented a report on APCERT Drill 2008, where it represented APCERT in the relevant session.

Google-Fu Course and Program with Media in Sabah
The program was one of CyberSecurity Malaysia's initiatives to introduce and disseminate information about its services to the community in Sabah. The program involved media briefing by CyberSecurity Malaysia to promote cyber security services to Kota Kinabalu residents. CyberSecurity Malaysia in collaboration with the District Education Office of Kota Kinabalu, also conducted Google-Fu Course at SRK Tanjung Aru I. It was attended by 34 participants, comprised of teachers from around the district. The second Google-Fu Course was conducted at Kolej Yayasan Sabah, Kota Kinabalu about 10 days later.

Other activities:

- Avid System Training: Professional Video Editing And Media Cybernetics Image-Pro Plus for Digital Forensics
- Working Visit to CyberSecurity Malaysia
  - **8 April 2009** Students from Kolej Komuniti Hulu Selangor;
  - **13 April 2009** Lecturers and Webmasters from Institut Perguruan Malaysia, Kuala Lumpur;
  - **15 April 2009** Visit by the Prime Minister's Department of Brunei. This visit was headed by YBhg. Sa Bali bin Abas, Permanent Secretary at the Prime Minister's Office (acting as Chief Secretary of Malaysia) along with other delegation from Bru-CERT. The objective of the visit was to enhance diplomatic relations and engage support from the highest authorities in Brunei Darussalam in combating cyber threats.
  - **22 April 2009** International Participant (MTCP) organized by INTAN, Bukit Kiara

Activities Throughout 2009

MAY 2009

Collaboration among OIC Member Countries for the Computer Emergency Response Team
The proposal by the Organisation of The Islamic Conference (OIC), during the OIC-CERT Annual General Meeting, whereby OIC-CERT serves as the `***Affiliated Institution of the OIC'*** was agreed by the Preparatory Meeting of Senior Officers to the Foreign Ministers' Council, 36th Session on 4 6 May 2009. CyberSecurity Malaysia as OIC-CERT Chairman attended the meeting as an observer. During the Plenary Conference, YB. Datuk Anifah Aman, Minister of Foreign Affairs, announced of his full support to Malaysia's proposal to create cooperation among OIC member countries in the field of science and technology. The excerpt from his speech to promote OIC-CERT are as follows ***"...Malaysia has also been actively involved in the establishment of the Computer Emergency Response Team amongst the OIC Member Countries (OIC- CERT). This initiative is intended to promote voluntary collaboration amongst CERTs of OIC Member States and a cooperative effort to enhance Member States' CERT's capabilities. Through collaboration and cooperation, it is hoped that Member States could develop their own CERTs, free from any external influence."***

Other activities:

- Digital Forensics Training for Malaysian Anti-Corruption Commission
- CyberSecurity Malaysia presented a country report on cyber security status and programmes in Malaysia at 3rd Counter-eCrime Operations Summit (CECOS III) held in Spain.
- Strategic Discussion among CyberSecurity Malaysia, Universiti Teknologi Petronas and Women Entrepreneurs Association (FEW)
- Exhibition in conjunction with Kaamatan Festival, Kota Marudu District Level
- Working visit to CyberSecurity Malaysia from Malaysia Airlines; and also from Malaysian Society for Cryptology Research

JUNE 2009

Workshop for Workgroups Analysing Weaknesses and Loopholes in Malaysian Law in Preparation for a Cyber Environment
Held at Langkawi, Kedah, the purpose of the workshop was to deliberate the draft report of the Third Phase of the Analysis of Weaknesses and Loopholes in Malaysian Law in Preparation for a Cyber Environment that is about to conclude. This workshop also served as a platform for 13 Ministries and enforcement agencies to provide feedback, in terms of operational and enforcement aspects, regarding the timeliness and appropriateness of the proposals presented by appointed consultant Tetuan Zul Rafique & Partners. In its capacity as Chairman and workshop secretariat, CyberSecurity Malaysia was responsible for presenting the results of this workshop's discussion to the Technical Committee Meeting scheduled for 20 July 2009 and subsequently, to the Cabinet.

Information Dissemination Workshop for ICT Weaknesses Evaluation Service
CyberSecurity Malaysia obtained permission to carry out a service project to evaluate ICT weaknesses under the aegis of the Second Economic Stimulus Package. Among the project main activities was the introduction and promotion of the service to evaluate ICT weaknesses among the target group i.e. Critical National Information Infrastructure CNII which includes public and private sectors. CyberSecurity Malaysia involved as the organizer, supported by the Ministry of Science, Technology and Innovation (MOSTI), and it carried out an information dissemination workshop. 26 representatives from 10 Ministries, government agencies and private companies attended this workshop.

Information dissemination workshop for evaluation and international certification services for ICT products for small and medium enterprises (SMEs)
CyberSecurity Malaysia also obtained approval to carry out this project specifically for ICT products for Small and Medium Enterprises (SMEs) under the Second Economic Stimulus Package. This information workshop was organized at the Palace of the Golden Horses Hotel and 35 representatives from SMEs took part.

Other activities:

- Audio Digital Forensics Training
- Business Continuity Management (BCM) Project
- Standards Development for Business Continuity Management (BCM) at National Level
- Development of Guidelines and Best Practices

JULY 2009

Cyber Security Malaysia II SecureAsia@Kuala Lumpur 2009 - *"Critical Infrastructure Protection in Current Global Financial Crisis"*
The Cyber Security Malaysia II SecureAsia@Kuala Lumpur 2009 Conference and Exhibition was held at the Kuala Lumpur Convention Centre from 6 to 8 July, 2009 – with the theme ***"Critical Infrastructure Protection in Current Global Financial Crisis".***

The conference received the cooperation of all parties, especially the Ministry of Science, Technology and Innovation (MOSTI), the Office of the Chief Government Security Officer (CGSO), International Information System Security Certification Consortium (ISC2) and Firmus Security Sdn Bhd as well as co-sponsorship from the private sector such as Symantec Corporation and IBM.

The objective of this national-level conference was to raise the awareness and share information on cyber security. Several memorandum of understanding (MoU) were signed between CyberSecurity Malaysia and local agencies while several agencies and local information security professionals were conferred awards for the contributions to information security in Malaysia.

A total of 402 participants attended the conference of which 22% were foreign participants from Singapore, Australia, India, South Korea and 13 other countries. A total of 17 topics on information security papers were tabled by various speakers from Malaysia as well as Canada, the US, Singapore, Hong Kong, Thailand, Japan and Australia.

At the conference, CyberSecurity Malaysia also launched its Cyber999 Help Centre, which is the initiative under 9th Malaysia Plan (RMK9). With this service, internet users including individuals and agencies can receive technical assistance related to cyber security incidents from CyberSecurity Malaysia. For the first time ever, CyberSecurity Malaysia organised the Malaysia Cyber Security Awards 2009 during which seven (7) local organisations received awards.

At the Information Security Leadership Awards (ISLA) award ceremony organised by ISC2, three CyberSecurity Malaysia representatives – Lt. Col. Husin Jazri (Retired), En. Aswami Fadillah Mphd. Ariffin and En. Adli Abdul Wahid – received awards from ISC2 in recognition of their contribution to information security.

CyberSecurity Malaysia also launched its corporate song entitled ***'CyberWorld For You'***, which was conceptualised to enhance the basic knowledge of the cyber world among the younger generation.

The Cyber Security Malaysia II SecureAsia@Kuala Lumpur 2009 Conference and Exhibition also organized four satellite seminars:

i. ***Digital Forensics Seminar***, attended by 63 participants from national law enforcement agencies;
ii. ***Critical National Infrastructure Protection (CNIP) Seminar***, attended by 177 participants from 10 Critical National Information Infrastructure sectors;
iii. ***Infor-Security Symposium Seminar***, attended by 215 participants who represented local and international banking institutions; and
iv. ***Internet Safety Awareness Seminar***, attended by 420 participants comprising secondary students from the Klang Valley, teachers, parents and other individuals.

In conclusion, Cyber Security Malaysia II SecureAsia@Kuala Lumpur 2009 Conference and Exhibition was a testimony to Malaysia's ability to host international conferences while also offering the opportunity to promote services made available by CyberSecurity Malaysia.

National Cyber Security Advisory Committee Meeting (NaCSAC) (1/2009)
The first NaCSAC Meeting was held on 17 July, 2009 and was chaired by YBhg Tan Sri Mohd. Sidek Hassan, Chief Secretary to the Government at the National Secretariat, Prime Minister's Office. The meeting was attended by members from 20 Ministries and agencies related to CNII.

Other activities:

- Critical National Infrastructure Protection Conference
- National Cyber Security (NC3) Coordination Committee Meeting (3/2009)
- National Cyber Security Advisory Committee Meeting (NaCSAC) (1/2009)
- 5th ICT Security Forum in Damsyik, Syria
- Security Management & Best Practices Technical Committee Meeting
- Information Security Management System (ISMS)
- Training on Introduction to Forensic Video Analysis
- Training on Smart Card Common Criteria

Activities Throughout 2009

AUGUST 2009

Internet Security Awareness Seminar and Official Launch of CyberSAFE
CyberSecurity Malaysia launched its CyberSAFE portal at the Marriott Resort & Spa, Miri, Sarawak on 9 August, 2009 by YB. Tuan Hj. Fadillah Yusof, Deputy Minister of Science, Technology and Innovation, in conjunction with the Internet Security Awareness Seminar which carried the theme "***Let's Make the Internet a Safer Place".*** The CyberSAFE Portal was developed to support the internet security awareness programme under the slogan Cyber Security Awareness for Everyone. The portal can be viewed at **http://www.cybersafe.my**. Users can learn and determine the best ways to surf the internet for work or social networking. An awareness seminar was also held in conjunction with the official launch of CyberSAFE with a total of 195 secondary school students from Miri took part in the program.

- **Other activities:**
- Awareness Programme on Internet Security – CyberSAFE
- Workshop on Cyber War
- Industry Dialogue - Info Security Malaysia: Moving Forward
- Seminar on Symptoms of Sexual Freedom among Urban Youths, Series 2
- Working Visit from Vietnam CERT (VINCERT)
- Technical Training on Cyber Security Incidents sponsored by the National Telecommunication Regulatory Authority, Egypt

SEPTEMBER 2009

Cyber Security Forum, sponsored by the International Telecommunication Union (ITU) for the Asia-Pacific Region
CyberSecurity Malaysia was invited by ITU to present a working paper entitled ***'Malaysia National Cyber Security Policy – Towards an Integrated Approach for Cyber Security and Critical Information Infrastructure Protection'*** at the cyber security forum, jointly sponsored by ITU and the Ministry of Communication and Information Technology India. CyberSecurity Malaysia sent two representatives to the forum, which was held in Hyderabad, India.

Other activities:

- Common Criteria Executive Sub-Committee (CCES) and Common Criteria Management Committee (CCMC) Meetings
- ISO/IEC 27001:2005 Certification preparatoractivities include Online Assessment, Compliance Checklist and Object Evidence.
- Risk Assessment Workshop, Annual Questionnaire and Awareness of Information Security Management System
- Charity Function and Official Opening of the Al-Jazari Multimedia Centre in Bait Al Amin, Perak
- Talk to Enhance Awareness on Cyber Security to Teachers
- Advanced Technical Training: Advance in Software Vulnerability Assessment and Exploit Development Workshop
- Mock Court Training (as expert witnesses) for Digital Forensics Analysts

OCTOBER 2009

Meridian Conference 2009 – Critical Information Infrastructure Protection (CIIP): A Joint Responsibility
The Meridian Conference 2009 with the themed ***"Critical Information Infrastructure Protection: A Joint Responsibility"*** was held for the 5th time at the Fairfax, Embassy Row in Washington. CyberSecurity Malaysia presented a working paper on National Cyber Security Policy during the first day of the conference. Malaysia was also elected as the Point of Contact for The International Critical Information Infrastructure Protection Directory, an intermediary body and coordinator of CIIP activities for the G8 nations.

Computer emergency response expertise training – with the Oman Computer Emergency Responses Team
CyberSecurity Malaysia was invited by e-COP Pte Ltd, a Singapore-based information technology safety company to organise an expertise training exercise on computer safety. Seven personnel from the Computer Emergency Response Team from Oman (OmanCERT) participated in this programme coordinated by MyCERT. The objective was to train OmanCERT personnel in preparation for their involvement in the Forum of Incident Response and Security Teams (FIRST).

Other activities:

- Participated in the 5th Joint London Action Plan (LAP) workshop in Lisbon, Portugal organised by Autoridade Nacional de Comunicacoes (ANACOM). Malaysia and Japan were the two Asian participants presented working papers at the workshop.
- Presented two working papers at the Cyber Threats and Safety colloquium organised by the Universiti Darul Iman (UDM) at the FELDA Residence in Kuala Terengganu.
- Invited to give a talk on – Overview on Internet Gambling – at the Online Gambling workshop in Genting Highlands sponsored by the Ministry of Finance.
- Shared information and experience via two presentation papers – Introduction to Digital Forensics, Introduction to Computer Forensics and Introduction to Computer and Storage Media at the introductory workshop on forensic digital methodology organised by Pulau Pinang Division of the Ministry of Domestic Trade, Cooperative and Consumerism (KPDNKK)
- Educational excursion: the bright sparks programme from the Bait Al-Amin centre and Universiti Teknologi Petronas (UTP) undergraduates
- National innovation conference and exhibition (NICE)

NOVEMBER 2009

The Safety And Protection of Critical Targets – East Zone - Dialogue 2009
The Office of the Government Chief Security Officer, Prime Minister's Department, and CyberSecurity Malaysia jointly organised the dialogue on the Safety and Protection of Critical Targets East Zone 2009 at the Hyatt Regency Hotel in Kuantan, Pahang.

Other activities:

- Received and briefed visitors from:
  - Commercial Crime Investigation Studies Unit of the Royal Police Force Of Malaysia (PDRM) And The Royal Police Force Of Thailand
  - YBhg. Dato' Sabariah Hassan – Executive Secretary (Management) Ministry Of Science, Technology And Innovation (MOSTI)
  - YBhg. Datin Paduka Prof Dr Khatijah Mohd Yusoff, Deputy Secretary General (Science), Ministry of Science, Technology And Innovation (MOSTI).
  - Presented two working papers- Facial Photographic Comparison Based on Facial Structure and Feature Analysis and Analysis of Handwritten Signature in Printed Document Using Adobe Photoshop- at the International Forensic Science And Environmental Health Symposium 2009.
  - Conducted Digital Forensics briefing to the Human Resource Department of the Inland Revenue Board (LHDN). Another briefing was also held for the Ministry of Domestic Trade, Cooperative and Consumerism (KPDNKK) in Perlis.
  - Conducted the second training session for personnel from the Computer Emergency Response Team from Oman (OmanCERT). CyberSecurity Malaysia was invited by e-COP Pte Ltd, a Singapore-based information technology safety company, to train OmanCERT personnel in preparation for their participation in the Forum of Incident Response and Security Teams (FIRST).
  - Participated in the APEC Seminar on Protection of Cyberspace From Terrorist Use And Attacks – Seoul, Republic of Korea
  - Signed a Memorandum Of Understanding with the Korean Institute of Criminology (KIC)
  - Participated in a few exhibition:-
    - Borneo International Trade Fair 2009
    - 2009 Corn Festival, Kota Marudu, Sabah

Activities Throughout 2009

DECEMBER 2009

World Computer Security Day – WCSD MALAYSIA 2009
The World Computer Security Day (WCSD) 2009 was extra special as it was observed for the first time in Malaysia from 30 November – 2 December 2009. With the themed of ***"Computer Security is Everyone's Responsibility"***, the celebration was officiated by YB. Dato' Seri Dr Maximus Johnity Ongkili, Minister of Science, Technology and Innovation. Various programmes on cyber security were held and it was attended by 254 guests from various sectors such as IT professionals, media and students.

A total of four Memorandum of Understanding –Mo, were signed during the WCSD celebration, mainly between CyberSecurity Malaysia and Disaster Recovery Institute (DRI) Malaysia Sdn Bhd, RHB Bank, Taiwan HonetNet and Universiti Kuala Lumpur. With these MoU's CyberSecurity Malaysia will cooperate and work together with these parties in the research, learning and teaching of various aspects of cyber security.

The celebrations received wide media coverage as well as online networks such as Facebook and Twitter. Generally, the entire celebration programme revolved around the core activities of:

- **The 1st ASEAN Cyber Volunteers Development Course** – the committee for the ASEAN Youth Cooperation (CAYC) in collaboration with CyberSecurity Malaysia organised a cyber safety course at The Royale Chulan, Kuala Lumpur on 1 December 2009 with 35 participants from ASEAN nations.
- **InfoSecurity Professional Networking Forum** – This forum was held on 30 November with the themed of ***"Changing the Cyber Landscape, Converging Towards Innovation".***
- **Launching of the CyberSecurity Malaysia Malware Research Centre** – YB Datuk Seri Dr Maximus Johnity Ongkili, Minister of Science, Technology and Innovation launched the CyberSecurity Malaysia Malware Research Centre on 1 December 2009. This centre was established to create public awareness on the threats of malware and focus on the capacity development to research and counter malware elements. The research centre is part of CyberSecurity Malaysia's initiative towards the development of its capacity to address and manage these risks and its potentially detrimental effects.
- **INFOSECURITY.my & First Technical Colloquium** – CyberSecurity Malaysia is a member of the Forum of Incident Response Security Team (FIRST), which is based at the Carnegie Mellon University in America. The national agency was entrusted with the task to organise the INFOSECURITY,my and First Technical Colloquium Seminar 2009 (FIRST-TC) in conjunction with WCSD. This seminar was the highlight of the WCSD celebrations and also part of the primary activities in the international cyber security calendar of events. A total of 164 local and foreign participants attended the seminar which focused on current cyber threats and risks, and global initiatives to counter such elements and challenges.

Other activities:

- Safety and Protection of Critical Targets Dialogue – Northern Sector 2009
- Digital Forensics Briefing to The Institute of Engineers Malaysia
- Presented ***"The Digital Forensics World – A Malaysian Perspective"*** at a forum on the Prevention of Financial Crimes and Bribery organised by the Malaysian Anti-Corruption Board in Kuala Lumpur.
- Visit from the Communications and Information Department of Indonesia

National Cyber Crisis Practical Training(X-MAYA2)
The National Security Council (MKN) and CyberSecurity Malaysia jointly organized this annual drill programme on the 9 – 10 December 2009 at the CyberSecurity Malaysia premise for organisations in the Critical National Information Infrastructure (CNII). Officiated by YB Tuan Haji Fadillah Yusof, Deputy Minister of Science, Technology and Innovation, the cyber drill was participated by 28 organisations. X-MAYA 2 exercise was aimed to test the national cyber crisis plan while strengthening the coordination and networking between the relevant government agencies. During the session, the structure and function of the National Cyber Coordination and Control Centre (NC4) was represented by MAMPU, PRDM, MINDEFF, SKMM and CyberSecurity Malaysia. This exercise successfully met its objectives to consolidate the national cyber crisis plan towards strengthening the country's capacity and capabilities to weather crisis situations.

Aktiviti 2009

JANUARI 2009

Seminar dan Mesyuarat Suku Pertama Negara Anggota Persidangan Pertubuhan Islam-Pasukan Tindakbalas Kecemasan Komputer (OIC-CERT)
CyberSecurity Malaysia menyambut kedatangan 2009 dengan menganjurkan Seminar OIC-CERT 2009. Seminar dua hari ini dihadiri 303 peserta iaitu 267 peserta tempatan manakala 36 dari luar negara, kebanyakannya dari negara anggota seperti Brunei, Indonesia, Pakistan, Bangladesh, Arab Saudi, Iran, Oman, Jordan, Syria, Turki, Tunisia, Maghribi, Nigeria, Mesir dan Libya. Sempena Seminar OIC-CERT 2009, Mesyuarat Agung Tahunan OIC-CERT turut diadakan. Sebanyak 16 negara OIC dan wakil Sekretariat OIC di Jeddah, Arab Saudi dan Pejabat Wilayah IDB, Kuala Lumpur menghadiri mesyuarat tersebut. Pada mesyuarat itu, Malaysia dilantik menyandang Kerusi OIC-CERT menerusi CyberSecurity Malaysia untuk dua penggal berturut-turut 2009-2011.

Aktiviti lain:

- Mesyuarat Jawatankuasa Penyelaras Keselamatan Siber Kebangsaan (NC3) 1/2009
- Lawatan Ketua Teknologi Maklumat dan dua (2) pegawai dari Jabatan Forensik Digital Persatuan Polis Jenayah Antarabangsa (INTERPOL) Perancis ke CyberSecurity Malaysia.
- Program Tanggungjawab Sosial Korporat (CSR) anjuran CyberSecurity Malaysia diadakan di Kampung Simpang Arang, Gelang Patah, Johor. Di majlis itu, CyberSecurity Malaysia menyumbangkan lima (5) bagi kegunaan pelajar Orang Asli.
- Program Tanggungjawab Sosial Korporat MOSTI - INFOSTI@MOSTI: Melatih Pelatih. CyberSecurity Malaysia mengadakan sesi latihan bagi bakal pelatih yang akan membimbing masyarakat di Sabah.
- CyberSecurity Malaysia menghadiri Sidang Kemuncak Persatuan Penyiasatan Jenayah Teknologi Tinggi Antarabangsa (HTCIA) di Hong Kong.

FEBRUARI 2009

Karnival dan Pelancaran Pusat INFOSTI@MOSTI
Menerusi pembabitan kami sebagai ahli jawatankuasa dan sekretariat majlis, CyberSecurity Malaysia berperanan besar dalam memastikan karnival dan pelancaran INFOSTI@MOSTI mencatat kejayaan. Ia diadakan di Kota Marudu, Sabah dan dirasmikan oleh YB Datuk Seri Maximus Johnity Ongkili, Menteri Sains, Teknologi dan Inovasi. Majlis sama turut diadakan di Kota Semariang Batu, Petrajaya, Kuching dan dirasmikan oleh YB Tuan Haji Fadillah Yusof, Timbalan Menteri Sains, Teknologi dan Inovasi. Inisiatif ini adalah satu daripada program CSR MOSTI ke arah merapatkan jurang digital di kalangan masyarakat luar bandar dan membantu mereka memiliki pengetahuan serta mahir dalam bidang IT. Serentak dengan karnival itu, CyberSecurity Malaysia menganjurkan sesi ***"Melatih Pelatih"*** selama sehari di Kampung Semariang Batu, Kuching, Sarawak. CyberSecurity Malaysia turut INFOSEC.my in Sarawak. Sesi separuh hari itu dirasmikan oleh YB Tuan Haji Fadillah bin Haji Yusuf. Seramai 250 pelajar dan guru daripada 23 sekolah menengah di sekitar Kuching menyertai program itu. Pelajar terbabit diberi pendedahan terhadap isu berkaitan keselamatan internet dan kaedah mengatasinya.

Aktiviti Lain:

- Seminar Strategy Blue Ocean - dihadiri 31 peserta daripada pasukan pengurusan CyberSecurity Malaysia.
- Menyertai Mesyuarat Institut Kajian Ekonomi Bagi ASEAN dan ASIA Timur (ERIA). CyberSecurity Malaysia adalah satu daripada ahli kumpulan projek ERIA. Projek ERIA bertumpu ke arah memanfaatkan penanda aras umum bagi keselamatan maklumat di kalangan negara Asia Timur.
- Sesi latihan mengenai Pemantauan Keselamatan Rangkaian (NSM) dianjurkan oleh CyberSecurity Malaysia. Peserta merangkumi kakitangan CyberSecurity Malaysia, Telekom Malaysia Berhad, TIME dotcom Berhad, .my DOMAIN REGISTRY (sebelum ini dikenali sebagai MYNIC Berhad) dan JARING Communications Sdn. Bhd.
- Terbabit dalam pelancaran Mesyuarat Trustmark Sektor Awam oleh Kementerian Perdagangan Antarabangsa dan Industri (MITI).

MAC 2009

- **Forum Mengurus Kesan Krisis Ekonomi Terhadap Industri ICT**
  CyberSecurity Malaysia menjadi penganjur bersama forum berkenaan dengan Kementerian Sains, Teknologi dan Inovasi, (MOSTI). Forum dirasmikan oleh Menterinya, YB Datuk Seri Dr Maximus Johnity Ongkili.
- **Lawatan Kerja ke CyberSecurity Malaysia**
  CyberSecurity Malaysia menerima kunjungan daripada pelbagai organisasi. Antara Kementerian, agensi dan institusi pengajian tinggi yang melawat CyberSecurity Malaysia adalah:
  - **2 Mac 2009** - Pelajar Ijazah Sarjana Muda IT, UiTM Perlis;
  - **5 Mac 2009** - Pelajar Fakulti Sains dan Teknologi; Universiti Sains Islam Malaysia (USIM);
  - **10 Mac 2009** - Pelajar Diploma Sains Komputer, UiTM Johor;
  - **19 Mac 2009** - Pasukan Petugas Khas Laman Web bagi Kementerian Tenaga, Air dan Komunikasi;
  - **23 Mac 2009** - Peserta Kursus Penyiasatan Jenayah Siber Siri 1/2009, Makmal Polis Diraja;
  - **24 Mac 2009** – Kementerian Sains, Teknologi dan Inovasi;
  - **24 Mac 2009** – Peserta Kursus Pengenalan Bagi Kawalan Iklan Siber, Kementerian Kesihatan Malaysia (Bahagian Penguatkuasaan)

Aktiviti lain:

- Menyertai Mesyuarat Agung Tahunan dan Sidang Kemuncak Pasukan Tindakbalas Kecemasan Komputer Asia Pasifik (APCERT) 2009.
- Latihan Google-Fu: Edisi Teknik Carian Kuasa dikendalikan untuk Kementerian Tenaga, Air dan Komunikasi serta Suruhanjaya Sekuriti

APRIL 2009

- **Bengkel Pelan Tindakan Dasar Keselamatan Siber Kebangsaan (NCSP) dan Mesyuarat Jawatankuasa Pengurusan Keselamatan Siber Keangsaan (NC3) bil. 1/2009**
  Bengkel Pelan Tindakan Dasar Keselamatan Siber Kebangsaan (NCSP) dan Mesyuarat Jawatankuasa Pengurusan Keselamatan Siber Keangsaan (NC3) bil. 1/2009 diadakan di Pusat Konvensyen Antarabangsan Putrajaya (PICC) pada 2 April 2009. Seramai 32 peserta merangkumi Pegawai Kanan dari Jabatan dan Agensi Kerajaan menghadiri bengkel terbabit.
- **Kumpulan Kerja Telekomunikasi dan Maklumat APEC ke-39 (APECTEL)**
  CyberSecurity Malaysia adalah sebahagian daripada delegasi Malaysia diketuai Kementerian Tenaga, Air dan Telekomunikasi ke Kumpulan Kerja Telekomunikasi dan Maklumat APEC ke-39 (APECTEL), yang diadakan di Suntec Convention Centre, Singapura. Pada majlis itu, CyberSecurity Malaysia mengendalikan sesi Kumpulan Pemandu Keselamatan dan Kemakmuran (SPSG) pada 17 April 2009. Sesi ini mendedahkan CyberSecurity Malaysia kepada pelbagai inisiatif berkaitan keselamatan siber dan isu strategik yang berlaku di peringkat antarabangsa. Sebagai tambahan, CyberSecurity Malaysia membentangkan laporan Latihan APCERT 2008, di mana ia mewakili APCERT bagi sesi berkaitan.
- **Kursus Google-Fu dan Program Bersama Media di Sabah**
  Program ini adalah antara inisiatif CyberSecurity Malaysia dalam memperkenalkan dan menyebarkan maklumat mengenai perkhidmatannya kepada masyarakat di Sabah. Program termasuk taklimat media oleh CyberSecurity Malaysia bagi mempromosi perkhidmatan keselamatan siber kepada penduduk Kota Kinabalu. CyberSecurity Malaysia dengan kerjasama Pejabat Pendidikan Daerah Kota Kinabalu turut mengendalikan Kursus Google-Fu di SRK Tanjung Aru I. Ia dihadiri 34 peserta, merangkumi guru-guru sekitar daerah itu. Kursus Google-Fu kedua dikendalikan di Kolej Yayasan Sabah, Kota Kinabalu kira-kira 10 hari kemudian.

Aktiviti lain:

- Latihan Sistem Avid: Suntingan Video Profesional dan Imej-Pro Media Sibernetik bagi Forensik Digital
- Lawatan ke CyberSecurity Malaysia:
  - **8 April 2009** - Pelajar Kolej Komuniti Hulu Selangor;
  - **13 April 2009** - Pensyarah dan Webmaster Institut Perguruan Malaysia, Kuala Lumpur;
  - **15 April 2009** - Lawatan Jabatan Perdana Menteri Brunei. Lawatan diketuai YBhg. Sa Bali bin Abas, Setiausaha Tetap di Jabatan Perdana Menteri (selaku Ketua Setiausaha Malaysia) seiring delegasi lain dari Bru-CERT. Objektif lawatan ialah meningkatkan hubungan diplomatik dan meraih sokongan daripada pihak berkuasa atasan Brunei Darussalam dalam melawan ancaman siber.
  - **22 April 2009** - Peserta Antarabangsa (MTCP) anjuran INTAN, Bukit Kiara

MEI 2009

Usahasama di kalangan Negara Anggota OIC bagi Pasukan Tindakbalas Kecemasan Komputer
Cadangan oleh Persidangan Pertubuhan Islam (OIC) ketika Mesyuarat Agung Tahunan OIC-CERT yang mana OIC-CERT bertindak sebagai ***`Institusi Bersekutu OIC'*** dipersetujui oleh Mesyuarat Persediaan Pegawai Kanan Kepada Majlis Menteri Luar Sesi ke-36 pada 4-6 Mei 2009. CyberSecurity Malaysia selaku Pengerusi OIC-CERT menghadiri mesyuarat sebagai pemerhati. Ketika Persidangan Pleno, Menteri Luar, YB. Datuk Seri Anifah Aman, mengumumkan sokongan penuhnya terhadap cadangan Malaysia untuk membentuk kerjasama di kalangan negara anggota OIC dalam bidang sains dan teknologi. Sedutan ucapannya dalam mempromosi OIC-CERT adalah seperti berikut: ***"... Malaysia terbabit secara aktif dalam penubuhan Pasukan Tindakbalas Kecemasan Komputer di kalangan Negara Anggota OIC (OIC-CERT). Inisiatif ini bertujuan menggalakkan usahasama sukarela di kalangan Negara Anggota OIC-CERT dan usaha murni ke arah meningkatkan kemampuan CERT Negara Anggota. Adalah diharapkan Negara Anggota dapat membangunkan CERT masing-masing yang bebas daripada pengaruh luar menerusi usahasama dan kerjasama ini".***

Aktiviti lain:

- Latihan Forensik Digital bagi Suruhanjaya Pencegahan Rasuah Malaysia (SPRM)
- CyberSecurity Malaysia membentangkan laporan negara berhubung status dan program keselamatan siber di Malaysia pada Sidang Kemuncak Operasi Menentang e-Jenayah ke-3 (CECOS III) di Sepanyol.
- Perbincangan Strategik di kalangan CyberSecurity Malaysia, Universiti Teknologi Petronas dan Persatuan Usahawan Wanita (FEW)
- Pameran sempena Pesta Kaamatan Peringkat Daerah Kota Marudu
- Lawatan kerja ke CyberSecurity Malaysia oleh Malaysia Airlines; dan Pertubuhan Kajian Kriptologi Malaysia

JUN 2009

- **Bengkel bagi Kumpulan Kerja Mengkaji Kelemahan dan Lompang Dalam Undang-Undang Malaysia Sebagai Persediaan ke arah Persekitaran Siber**
  Diadakan di Langkawi, Kedah, bengkel ini bertujuan memperincikan laporan draf Fasa Ketiga Analisa Kelemahan dan Lompang Dalam Undang-Undang Malaysia Sebagai Persediaan ke arah Persekitaran Siber yang hampir lengkap. Bengkel ini turut menjadi platform bagi 13 Kementerian dan agensi penguatkuasaan memberi maklum balas dari aspek operasi dan penguatkuasaan berhubung ketepatan masa dan kesesuaian cadangan yang dibentang oleh perunding dilantik, Tetuan Zul Rafique & Partners. Dalam kapasitinya sebagai Pengerusi dan Sekretariat bengkel, CyberSecurity Malaysia bertanggungjawab membentangkan hasil perbincangan bengkel ke Mesyuarat Jawatankuasa Teknikal yang dijadualkan pada 20 Julai 2009 dan disusuli kepada Kabinet.

- **Bengkel Penyebaran Maklumat Bagi Perkhidmatan Penilaian Kelemahan ICT**
  CyberSecurity Malaysia mendapat kebenaran untuk melaksanakan projek perkhidmatan bagi menilai kelemahan ICT di bawah naungan Pakej Rangsangan Ekonomi Kedua. Antara aktiviti utama projek tersebut ialah pengenalan dan promosi perkhidmatan bagi menilai kelemahan ICT di kalangan kumpulan sasar i.e Prasarana Maklumat Kritikal Kebangsaan (CNII) merangkumi sektor awam dan swasta. CyberSecurity Malaysia terbabit selaku penganjur dengan sokongan Kementerian Sains, Teknologi dan Inovasi (MOSTI), menganjurkan bengkel penyebaran maklumat. Bengkel dihadiri 26 wakil daripada 10 Kementerian, agensi kerajaan dan syarikat persendirian.

- **Bengkel penyebaran maklumat bagi penilaian dan persijilan antarabangsa produk ICT bagi Perusahaan Kecil dan Sederhana (PKS)**
  CyberSecurity Malaysia turut mendapat kelulusan melaksanakan projek ini khusus bagi produk ICT untuk Perusahaan Kecil dan Sederhana (PKS) di bawah Pakej Rangsangan Ekonomi Kedua. Bengkel maklumat ini diadakan di Hotel Palace of the Golden Horses dan disertai 35 wakil PKS.

Aktiviti lain:

- Latihan Forensik Audio Digital
- Projek Pengurusan Kesinambungan Perniagaan (BCM)
- Pembangunan Piawaian bagi Pengurusan Kesinambungan Perniagaan (BCM) peringkat kebangsaan
- Pembangunan Garis Panduan dan Amalan Baik

JULAI 2009

- **Cyber Security Malaysia II SecureAsia@Kuala Lumpur 2009 - *"Perlindungan Prasarana Kritikal Dalam Krisis Kewangan Global Semasa".***
  Persidangan dan Pameran Cyber Security Malaysia II SecureAsia@Kuala Lumpur 2009 diadakan di Pusat Konvensyen Kuala Lumpur pada 6 hingga 8 Julai, 2009 – bertemakan ***"Perlindungan Prasarana Kritikal Dalam Krisis Kewangan Global Semasa".***

  Persidangan tersebut menerima sokongan semua pihak, terutama Kementerian Sains, Teknologi dan Inovasi (MOSTI), Pejabat Pegawai Keselamatan Ketua Kerajaan (CGSO), Konsortium Persijilan Sistem Keselamatan Maklumat Antarabangsa (ISC2) dan Firmus Security Sdn Bhd, selain tajaan bersama sektor swasta seperti Symantec Corporation IBM.

  Objektif persidangan peringkat kebangsaan ini ialah meningkatkan kesedaran dan berkongsi maklumat mengenai keselamatan siber. Beberapa memorandum persefahaman (MoU) ditandatangani antara CyberSecurity Malaysia dan agensi tempatan manakala bebeapa agensi dan golongan profesional keselamatan maklumat tempatan menerima anugerah atas sumbangan terhadap keselamatan maklumat di Malaysia.

  Seramai 402 peserta menghadiri persidangan, dengan 22% daripadanya adalah peserta asing dari Singapura, Australia, India, Korea Selatan dan 13 negara lain. Sebanyak 17 topik berkaitan keselamatan maklumat dibentang oleh peserta dari Malaysia, Kanada, Amerika Syarikat, Singapura, Hong Kong, Thailand, Jepun dan Australia.

  Pada persidangan itu, CyberSecurity Malaysia turut melancarkan Pusat Bantuan Cyber999, iaitu inisiatif di bawah Rancangan Malaysia Ke-9 (RMK9). Dengan perkhidmatan ini, pengguna internet termasuk individu dan agensi boleh mendapatkan bantuan teknikal berhubung insiden keselamatan siber daripada CyberSecurity Malaysia. Buat julung kalinya, CyberSecurity Malaysia mengendalikan Anugerah Keselamatan Siber Malaysia 2009 yang menyaksikan tujuh (7) organisasi tempatan diberi penghargaan.

  Pada majlis Anugerah Kepemimpinan Keselamatan Maklumat (ISLA) anjuran ISC2, tiga wakil CyberSecurity Malaysia – Lt. Kol. Husin Jazri (Bersara)), En. Aswami Fadillah Mohd. Ariffin and En. Adli Abdul Wahid – menerima anugerah daripada ISC2 sebagai menghargai sumbangan mereka teradap keselamatan maklumat.

  CyberSecurity Malaysia turut melancarkan lagu korporat bertajuk ***'CyberWorld For You'*** yang dicipta bagi meningkatkan pengetahuan asas dunia siber di kalangan generasi muda.

  Persidangan dan Pameran Cyber Security Malaysia II SecureAsia@Kuala Lumpur 2009 turut mengendalikan empat seminar satelit:
  - ***Seminar Forensik Digital*** yang dihadiri 63 peserta daripada agensi penguatkuasa undang-undang kebangsaan;
  - ***Seminar Perlindungan Prasarana Maklumat Kritikal Kebangsaan (CNIP)***, dihadiri 177 peserta dari 10 sektor Prasarana Maklumat Kritikal Kebangsaan;
  - ***Seminar Simposium Info-Security***, dihadiri 215 peserta yang mewakili institusi perbankan tempatan dan antarabangsa; dan
  - ***Seminar Kesedaran Keselamatan Internet***, dihadiri 420 peserta merangkumi pelajar sekolah menengan dari Lembah Klang, guru, ibu dan dan individu.

  Sebagai kesimpulannya, Persidangan dan Pameran CyberSecurity Malaysia II SecureAsia@Kuala Lumpur 2009 adalah testimoni terhadap kemampuan Malaysia dalam menjadi tuan rumah persidangan antarabangsa dan pada masa sama, menawarkan peluang mempromosi perkhidmatan yang disediakan CyberSecurity Malaysia.

- **Mesyuarat Jawatankuasa Penasihat Keselamatan Siber Kebangsaan (NaCSAC) (1/2009)**
  Mesyuarat NaCSAC pertama diadakan pada 17 Julai, 2009 dan dipengerusikan Ketua Setiausaha Negara, YBhg Tan Sri Mohd. Sidek Hassan, di Sekretariat Kebangsaan, Jabatan Perdana Menteri. Mesyuarat dihadiri ahli daripada 20 Kementerian dan agensi berkaitan CNII.

Aktiviti lain:

- Persidangan Perlindungan Prasarana Kritikal Kebangsaan
- Mesyuarat Jawatankuasa Penyelaras Keselamatan Siber Kebangsaan (NC3) (3/2009)
- Mesyuarat Jawatankuasa Penasihat Keselamatan Siber Kebangsaan (NaCSAC) (1/2009)
- Forum Keselamatan ICT kelima di Damsyik, Syria
- Mesyuarat Jawatankuasa Teknikal Pengurusan Keselamatan dan Amalan Baik
- Sistem Pengurusan Keselamatan Maklumat (ISMS)
- Latihan Mengenai Pengenalan Kepada Analisis Video Forensik
- Latihan Kriteria Umum Kad Pintar

OGOS 2009

Seminar Kesedaran Keselamatan Internet dan Pelancaran Rasmi CyberSAFE
CyberSecurity Malaysia melancarkan portal CyberSAFE di Marriott Resort & Spa, Miri, Sarawak pada 9 Ogos, 2009 oleh Timbalan Menteri Sains, Teknologi dan Inovasi, YB. Tuan Hj. Fadillah Yusof, sempena Seminar Kesedaran Keselamatan Internet bertemakan ***`Let's Make the Internet a Safer Place'***. Portal CyberSAFE dibangunkan untuk menyokong program kesedaran keselamatan internet di bawah slogan Kesedaran Keselamatan Siber Untuk Semua. Portal berkenaan boleh dilayari di **http://www.cybersafe.my**. Pengguna boleh mempelajari dan menentukan cara terbaik melayari internet untuk kerja atau rangkaian sosial. Satu seminar kesedara turut diadakan sempena pelancaran rasmi CyberSAFE dengan 195 pelajar sekolah menengah dari Miri menyertai program.

Aktiviti lain:

- Program Kesedaran Mengenai Keselamatan Internet - CyberSAFE
- Bengkel Mengenai Perang Siber
- Dialog Industri - Info Security Malaysia: Bergerak Ke Hadapan
- Seminar Mengenai Simptom Kebebasan Seksual di kalangan Remaja Bandar, Siri 2
- Lawatan kerja CERT Vietnam CERT (VINCERT)
- Latihan Teknikal Mengenai Insiden Keselamatan Siber tajaan Lembaga Kawalselia Telekomunikasi Kebangsaan, Mesir

SEPTEMBER 2009

Forum Keselamatan Siber, ditaja oleh Kesatuan Telekomunikasi Antarabangsa (ITU) bagi Wilayah Asia-Pasifik
CyberSecurity Malaysia diundang oleh ITU untuk membentang kertas kerja bertajuk ***'Dasar Keselamatan Siber Kebangsaan Malaysia - Ke Arah Pendekatan Bersepadu bagi Keselamatan Siber dan Perlindungan Prasarana Maklumat Kritikal'*** pada forum keselamatan siber, anjuran bersama ITU dan Kementerian Komunikasi dan Teknologi Maklumat India. CyberSecurity Malaysia menghantar dua wakil ke forum berkenaan yang diadakan di Hyderabad, India.

Aktiviti lain:

- Mesyuarat Jawatankuasa Kecil Eksekutif Kriteria Umum (CCES) dan Jawatankuasa Pengurusan Kriteria Umum (CCMC)
- SO/IEC 27001:2005 Aktiviti Persediaan Persijilan termasuk Penilaian Dalam Talian, Senarai Pematuhan dan Bukti Objek.
- Bengkel Penilaian Risiko, Soal Jawab Tahunan dan Kesedaran Terhadap Sistem Pengurusan Keselamatan Maklumat
- Majlis Kebajian dan Pembukaan Rasmi Pusat Multimedia Al-Jazari di Bait Al Amin, Perak
- Ceramah bagi Meningkatkan Kesedaran Mengenai Keselamatan Siber kepada Guru-Guru
- Latihan Teknikal Lanjutan: Bengkel Penilaian Lanjutan Dalam Kegoyahan (Vulnerability) Perisian dan Pembangunan Eksploit
- Latihan Mahkamah Olok-Olok (sebagai saksi pakar) bagi Penganalisis Forensik Digital

OKTOBER 2009

- **Persidangan Meridian 2009 – Perlindungan Prasarana Maklumat Kritikal (CIIP): Tanggungjawab Bersama**
  Persidangan Meridian 2009 bertemakan ***"Perlindungan Prasarana Maklumat Kritikal: Tanggungjawab Bersama"*** diadakan buat kali kelima di Fairfax, Embassy Row, Washington. CyberSecurity Malaysia membentangkan kertas kerja mengenai Dasar Keselamatan Siber Kebangsaan di hari pertama persidangan. Malaysia turut dipilih sebagai Pusat Hubungan (Point of Contact) bagi Direktori Perlindungan Prasarana Maklumat Kritikal Antarabangsa, sebuah badan perantara dan penyelaras kegiatan CIIP bagi negara G8.
- **Latihan Kepakaran Tindakbalas Kecemasan Komputer bersama Pasukan Tindakbalas Kecemasan Komputer Oman**
  CyberSecurity Malaysia diundang oleh e-COP Pte Ltd, syarikat keselamatan teknologi maklumat berpangkalan di Singapura, untuk mengendalikan latihan kepakaran mengenai keselamatan komputer. Tujuh kakitangan Pasukan Tindakbalas Kecemasan Komputer dari Oman (OmanCERT) mengambil bahagian dalam program yang diselaras oleh MyCERT. Matlamatnya ialah melatih kakitangan OmanCERT membuat persediaan menyertai Forum Pasukan Tindakbalas Kejadian dan Keselamatan (FIRST).

Aktiviti lain:

- Menyertai Bengkel Pelan Tindakan Bersama London Ke-5 (LAP) di Lisbon, Portugal anjuran Autoridade Nacional de Comunicacoes (ANACOM). Malaysia dan Jepun merupakan dua negara Asia yang membentangkan kertas kerja di bengkel berkenaan.
- Membentangkan dua kerta kerja di Kolokium Ancaman dan Keselamatan Siber anjuran Universiti Darul Iman (UDM) di Kediaman FELDA, Kuala Terengganu.
- Diundang menyampaikan cermah – Pandangan Menyeluruh Mengenai Judi Internet – di Bengkel Judi Dalam Talian di Genting Highlands tajaan Kementerian Kewangan.
- Berkongsi maklumat dan kepakaran menerusi dua pembentangan – Pengenalan Kepada Forensik Digital, Pengenalan Kepada Forensik Komputer dan Pengenalan kepada Komputer dan Storan Media (Storage Media) di Bengkel Pengenalan Metodologi Forensik Digital anjuran Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (KPDBKK) cawangan Pulau Pinang
- Lawatan Pendidikan: Program `bright sparks' dari Pusat Bait Al-Amin dan mahasiswa Universiti Teknologi Petronas (UTP)
- Persidangan dan Pameran Inovasi Kebangsaan (NICE)

NOVEMBER 2009

Keselamatan dan Perlindungan Sasaran Kritikal - Zon Timur - Dialog 2009
Pejabat Ketua Keselamatan Kerajaan, Jabatan Perdana Menteri dan CyberSecurity Malaysia secara bersama menganjurkan dialog Keselamatan dan Perlindungan Sasaran Kritikal Zon Timur 2009 di Hyatt Regency Hotel, Kuantan, Pahang.

Aktiviti lain:

- Menerima kunjungan dan memberi taklimat kepada pelawat dari:
  - Unit Kajian Penyiasatan Jenayah Komersial Polis Diraja Malaysia (PDRM) dan Polis Diraja Thailand
  - YBhg. Dato' Sabariah Hassan – Setiausaha Eksekutif (Pengurusan) Kementerian Sains, Teknologi dan Inovasi (MOSTI)
  - YBhg. Datin Paduka Prof Dr Khatijah Mohd Yusoff, Timbalan Setiausaha Agung (Sains) Kementerian Sains, Teknologi dan Inovasi (MOSTI)
  - Membentangkan dua kertas kerja - Perbandingan Fotografik Wajah Berdasarkan Analisis Struktur Wajah dan Rupabentuk dan Analisis Tandatangan Bertulis dalam Dokuman Bercetak Menggunakan Adobe Photoshop di Simposium Sains Forensik dan Kesihatan Alam Sekitar Antarabangsa 2009.
  - Mengendalikan taklimat Forensik Digital kepada Jabatan Sumber Manusia Lembaga Hasil Dalam Negeri (LHDN). Satu lagi taklimat turut diadakan bagi Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (KPDNKK) di Perlis.
  - Mengendalikan sesi latihan kedua bagi kakitangan Pasukan Tindakbalas Kecemasan Komputer dari Oman (OmanCERT). CyberSecurity Malaysia diundang oleh e-COP Pte Ltd, syarikat keselamatan teknologi maklumat berpangkalan di Singapura, untuk melatih kakitangan OmanCERT dalam membuat persediaan menyertai Forum Pasukan Tindakbalas Kejadian dan Keselamatan (FIRST).
  - Menyertai Seminar APEC Mengenai Perlindungan Alam Siber Daripada Penggunaan dan Serangan Pengganas - Seoul, Korea Selatan
  - Menandatangani Memorandum Persefahaman dengan Institut Kriminologi Korea (KIC)
  - Menyertai beberapa pameran:-
    - Pameran Perdagangan Antarabangsa Borneo 2009
    - Pesta Jagung 2009, Kota Marudu, Sabah

DISEMBER 2009:

- **Hari Keselamatan Komputer Sedunia – WCSD MALAYSIA 2009**
  Hari Keselamatan Komputer Sedunia (WCSD) 2009 menjadi lebih istimewa apabila ia disambut buat pertama kalinya di Malaysia dari 30 November – 2 Disember 2009. Bertemakan ***"Keselamatan Komputer Adalah Tanggungjawab Semua"***, sambutannya dirasmikan oleh Menteri Sains, Teknologi dan Inovasi, YB. Dato' Seri Dr Maximus Johnity Ongkili. Pelbagai program berkaitan keselamatan siber diadakan dan dihadiri 254 tetamu daripada pelbagai sektor merangkumi golongan profesional IT, media dan pelajar.

  Sebanyak empat Memorandum Persefahaman – MoU ditandatangani sepanjang sambutan WCSD, sebahagian besarnya antara CyberSecurity Malaysia dan Institut Pemulihan Bencana (DRI) Malaysia Sdn Bhd, RHB Bank, Taiwan HonetNet dan Universiti Kuala Lumpur. Berlandasakan MoU tersebut, CyberSecurity Malaysia akan bekerjasama dengan pihak terbabit di bidang penyelidikan, pembelajaran dan pengajaran pelbagai aspek keselamatan siber.

  Sambutan berkenaan mendapat liputan meluas media, selain rangkaian laman sosial seperti Facebook dan Twitter. Secara amnya, keseluruhan program sambutan berlingkar sekitar aktiviti utama merangkumi:

  - **Kursus Pembangunan Sukarelawan Siber ASEAN pertama** – Jawatankuasa Kerjasama Belia ASEAN (CAYC) dengan usahasama CyberSecurity Malaysia menganjurkan kursus keselamatan siber di The Royale Chulan, Kuala Lumpur pada 1 Disember 2009 dengan 35 peserta dari negara ASEAN.
  - **Forum Rangkaian Profesional InfoSecurity** – Forum ini diadakan pada 30 November bertemakan ***"Mengubah Landskap Siber, Penumpuan Ke Arah Inovasi"***
  - **Pelancaran Pusat Kajian Malware CyberSecurity Malaysia** – Menteri Sains, Teknologi dan Inovasi, YB Datuk Seri Dr Maximus Johnity Ongkili, melancarkan Pusat Kajian Malware CyberSecurity Malaysia pada 1 Disember 2009. Pusat ini ditubuhkan bagi mewujudkan kesedaran awam terhadap ancaman malware dan tumpuan terhadap pembangunan kapasiti bagi mengkaji dan melawan unsur malware. Pusat kajian ini adalah antara inisiatif CyberSecurity Malaysia ke arah pembangunan keupayaannya dalam menangani serta menguruskan risiko dan kesan yang timbul daripadanya.
  - **INFOSECURITY.my & Kolokium Teknikal FIRST** - CyberSecurity Malaysia merupakan ahli Forum Pasukan Keselamatan dan Tindakbalas Kejadian (FIRST), yang berpangkalan di Carnegie Mellon University, Amerika Syarikat. Agensi kebangsaan itu dipertanggungjawabkan untuk merancang INFOSECURITY.my dan Seminar Kolokium Teknikal FIRST 2009 (FIRST-TC) bersempena dengan WCSD. Seminar ini adalah kemuncak sambutan WCSD dan juga sebahagian aktiviti utama dalam acara kalendar keselamatan siber antarabangsa. Sejumlah 164 peserta tempatan dan antarabangsa menghadiri seminar yang memberi tumpuan kepada ancaman dan risiko siber semasa, dan inisiatif global dalam menangani elemen dan cabaran sedemikian.

- **Latihan Praktikal Krisis Siber Nasional (X-MAYA2)**
  Majlis Keselamatan Negara (MKN) dan CyberSecurity Malaysia menjadi penganjur bersama program latihan tahunan ini pada 9 – 10 Disember 2009 di premis CyberSecurity Malaysia bagi persatuan di Insfrastruktur Maklumat Kritikal Kebangsaan (CNII). Dirasmikan oleh Timbalan Menteri Sains, Teknologi dan Inovasi, YB Tuan Haji Fadillah Yusof, latihan siber itu disertai 28 organisasi. Latihan X-MAYA 2 bertujuan menguji pelan krisis siber nasional sambil memperkukuhkan penyelarasan dan rangkaian di kalangan agensi kerajaan yang berkaitan. Pada sesi itu, struktur dan fungsi Pusat Penyelarasan dan Kawakan Siber Nasional (NC4) diwakili oleh MAMPU, PRDM, MINDEF, SKMM dan CyberSecurity Malaysia. Latihan ini berjaya memenuhi matlamat ke arah menyepadukan pelan krisis siber nasional ke arah memantapkan keupayaan negara dan kemampuan menangani situasi krisis.

Aktiviti lain:

- Dialog Keselamatan dan Perlindungan Sasaran Kritikal - Sektor Utara 2009
- Taklimat Forensik Digital kepada Institut Jurutera Malaysia
- Pembentangan ***"Dunia Digital Forensik - Dari Perspektif Malaysia"*** pada forum Pencegahan Jenayah Kewangan dan Rasuah anjuran Suruhanjaya Pencegahan Rasuah Malaysia di Kuala Lumpur.
- Lawatan Jabatan Komunikasi dan Maklumat Indonesia

Certified • Recognised • Assured

www.cybersecurity.my/mycc

Malaysian Common Criteria Evaluation & Certification Scheme
TM
mycc

Securing Our Cyberspace

Best Brand Internet Security 2008 & 2009

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

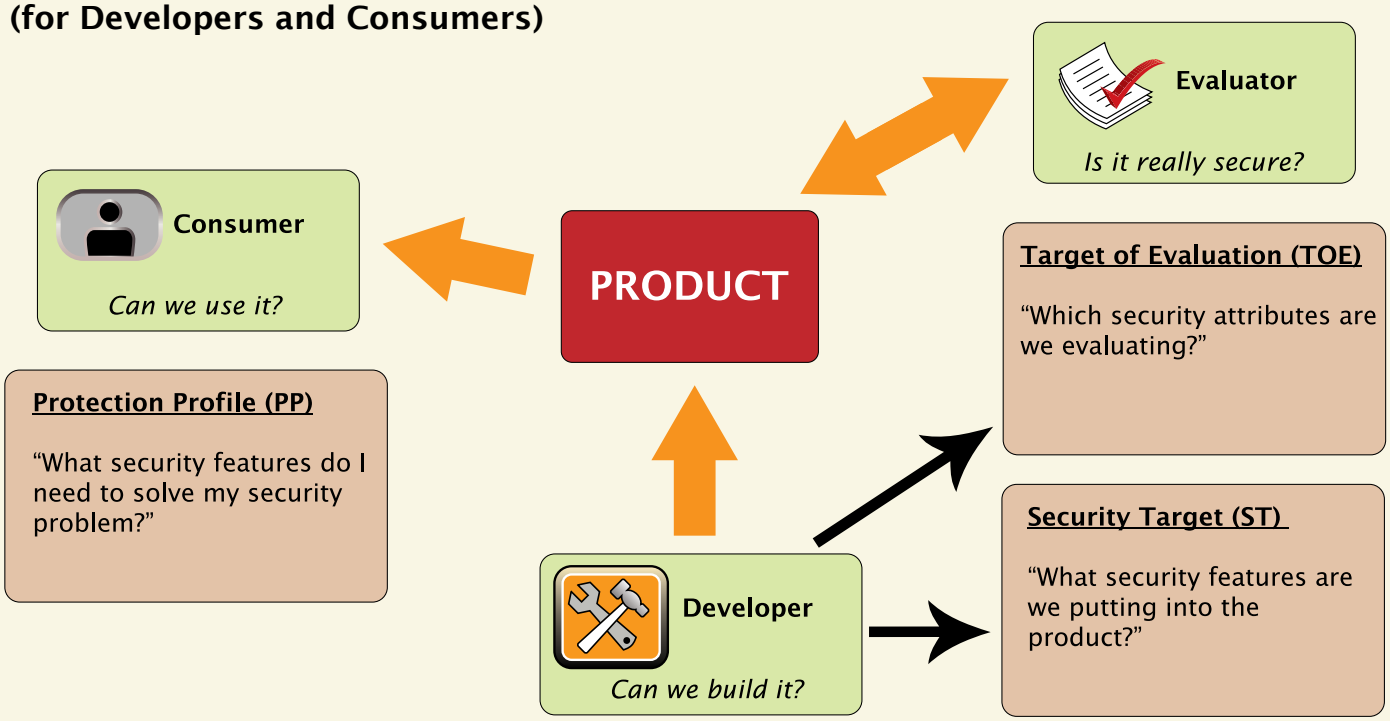
CyberSecurity MALAYSIA
An agency under MOSTI

1 Malaysia

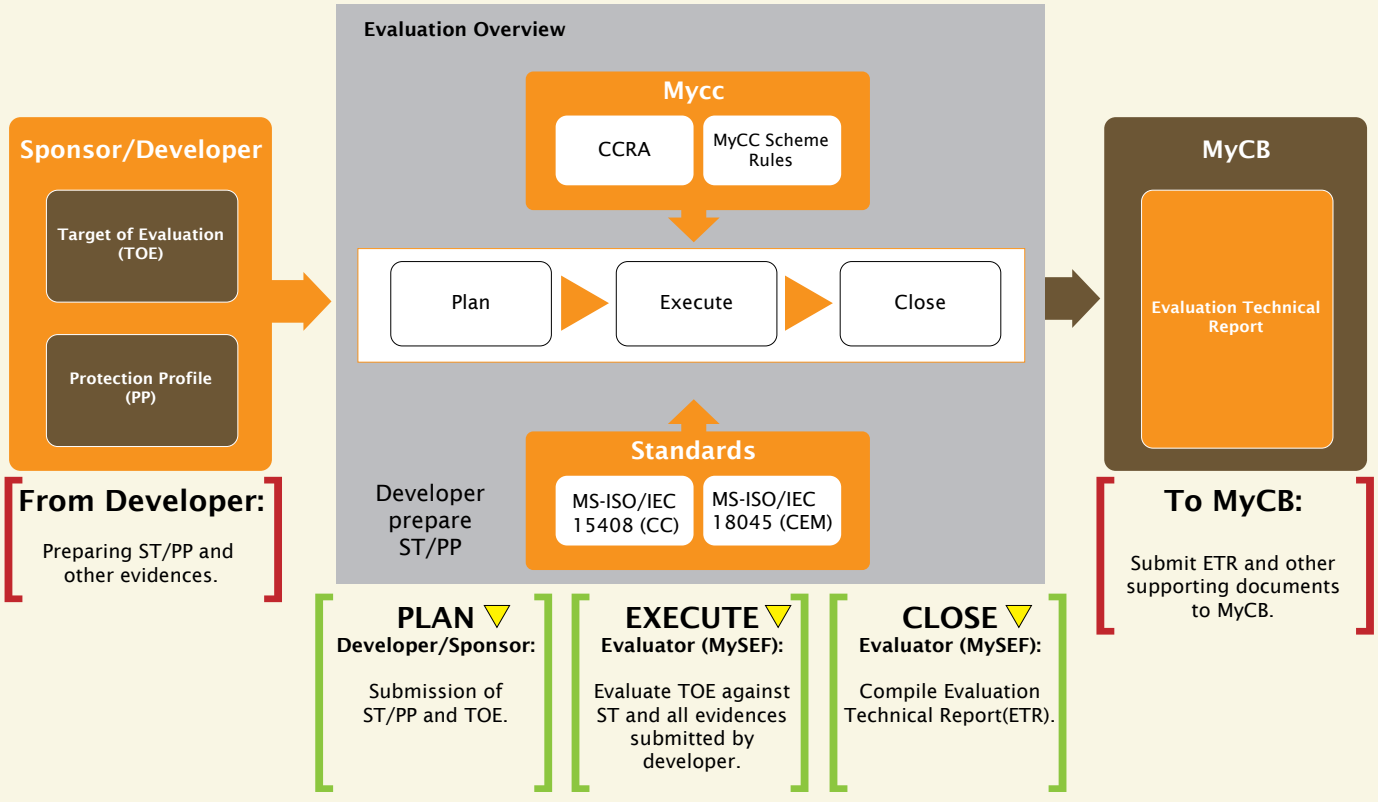
MOSTI
Ministry of Science, Technology and Innovation

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



Cybersecurity Malaysia

(Company Limited By Guarantee)

STATUTORY FINANCIAL STATEMENTS

For The Year Ended 31 December 2009

Corporate Information

Board of Directors

General Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired) - Chairman

Dato' Madinah binti Mohamad

Lt Col 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)

Directors' Report

The Directors have pleasure in submitting their report and the audited financial statements of the Company for the year ended 31 December 2009.

1. Principal Activity

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

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

	RM
Net surplus of income for the year	1,067,483

4. Reserves and Provisions

There were no material transfers to or from reserves or provisions during the year ended 31 December 2009.

5. Directors of the Company

The directors in office since the date of last directors' report are:-

General Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired)
(Chairman) (Appointed on 16 July 2009)

Lt. Col. Husin bin Jazri (Retired)

Puan Rubaiah binti Hashim

Encik Ir Md Shah Nuri Md Zain

Datuk Abang Abdul Wahap bin Abg Julai
(Appointed on 11 May 2009)

Datuk Dr. Abdul Raman bin Saad
(Appointed on 25 June 2009)

Dato' Madinah binti Mohamad
(Appointed on 16 July 2009)

Puan Rohani binti Mohamad
(Appointed on 28 January 2010)

Dato' Abdul Hanan bin Alang Endut
(Resigned on 30 June 2009)

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 income statement and balance sheet 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 2009 which secures the liabilities of any other person; and

(vi) there does not exist any contingent liability which has arisen since 31 December 2009.

(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 :-

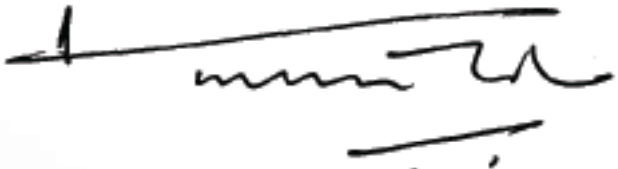
(a) the results of the Company's operations during the financial year were not substantially affected by any item, transaction or event of a material and unusual nature; and

(b) 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.

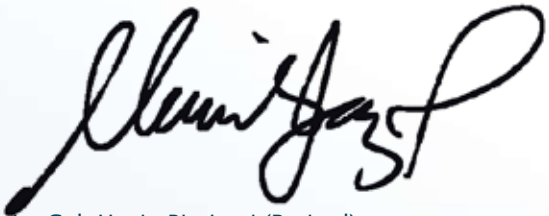
7. Auditors

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 Dato' Seri Panglima Mohd Azumi Bin Mohamed (Retired)



Lt. Col. Husin Bin Jazri (Retired)

Kuala Lumpur,

Date: 17 May 2010

Balance sheet as at 31 December 2009

	Note	2009 RM	2008 RM
ASSETS			
Non Current Assets			
Property, plant and equipment	6	27,607,629	8,361,253
Intangible assets	7	3,345,713	1,230,806
		30,953,342	**9,592,059**
Current Assets			
Trade receivables	8	660,945	122,975
Other receivables		1,115,492	466,137
Short term deposits with licensed banks	9	8,000,000	3,000,000
Cash and bank balances		16,205,211	6,426,961
		25,981,648	**10,016,073**
Total Assets		**56,934,990**	**19,608,132**
RESERVES AND LIABILITIES			
Reserves			
Accumulated reserves		1,577,784	510,301
Non Current Liabilities			
Government grants	10	53,656,081	18,102,564
Current Liabilities			
Other payables and accruals		1,345,298	995,267
Tax payable	11	355,827	-
		1,701,125	**995,267**
Total Reserves and Liabilities		**56,934,990**	**19,608,132**

The notes on pages 94 to 105 form part of these financial statements.

Income Statement
For The Year Ended 31 December 2009

	Note	2009 RM	2008 RM
Revenue	12	1,235,951	679,810
Cost of Services Rendered		(759,020)	(271,824)
		476,931	**407,986**
Income from Grants	13	34,141,928	24,399,940
Other Income	14	187,359	57,877
Administrative Expenses		(21,667,220)	(18,223,029)
Advertising and Marketing Expenses		(2,649,953)	(1,306,364)
General and Other Expenses		(9,065,735)	(5,512,188)
Surplus / (deficit) of Income Before Taxation	15	1,423,310	(175,778)
Taxation	11	(355,827)	-
Net Surplus / (Deficit) of Income for the Year		1,067,483	(175,778)

The notes on pages 94 to 105 form part of these financial statements.

Statement of Changes in Reserves
For The Year Ended 31 December

	Accumulated Reserves
	RM
As at 1 January 2008	686,079
Net deficit of income for the year	(175,778)
Balance at 31 December 2008	510,301
Net surplus of income for the year	1,067,483
Balance at 31 December 2009	**1,577,784**

The notes on pages 94 to 105 form part of these financial statements.

Cash Flow Statement
For The Year Ended 31 December

	2009 RM	2008 RM
Cash Flows From Operating Activities		
Surplus / (deficit) of income before tax	1,423,310	(175,778)
Adjustments for:		
Depreciation of property, plant and equipment	2,087,048	892,741
Amortisation of intangible assets	586,239	260,787
Interest income	176,909	50,956
Grant income recognised	(34,141,928)	(24,399,940)
	(29,868,422)	(23,371,234)
Changes in working capital :-		
Increase in trade receivables	(537,970)	(28,812)
Increase in other receivables	(498,921)	(108,813)
Increase in other payables	350,031	186,813
	(30,555,282)	(23,322,046)
Operating government grants received (Note 10b)	13,800,000	12,000,000
Interest received	(176,909)	(50,956)
Net cash used in operating activities	(16,932,191)	(11,373,002)
Cash Flows Form Investing Activities		
Purchase of property, plant and equipment	(21,483,858)	(4,813,355)
Purchase of intangible assets	(2,701,146)	(1,008,801)
Net cash used in investing activities	(24,185,004)	(5,822,156)
Cash Flows From Financing Activity		
Development government grants received (Note 10a)	55,895,445	17,516,900
Net Increase in Cash and Cash Equivalents During The Year	14,778,250	321,742
Cash and Cash Equivalents At Beginning Of The Year	9,426,961	9,105,219
Cash and Cash Equivalents At End Of Year	24,205,211	9,426,961
Cash and Cash Equivalents Comprise:-		
Fixed deposit	8,000,000	3,000,000
Cash and bank balances	16,205,211	6,426,961
	24,205,211	**9,426,961**

The notes on pages 94 to 105 form part of these financial statements.

Notes To The Financial Statements
- 31 December 2009

1. Principal Activities

The principal activities of the Company are the provision of cyber security services to the Malaysian public namely Cyber Emergency services, Security Quality Management services, Cyber Security Research and Policy services and InfoSecurity 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 17 May 2010 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 and principal place of operations 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.

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. Basis Of Preparation Of The Financial Statements

The financial statements of the Company are prepared under the historical cost convention and comply with Financial Reporting Standards (FRSs) and the Companies Act, 1965 in Malaysia.

The Company has not applied the new or revised Financial Reporting Standards ("FRSs") and Issues Committee ("IC") interpretations, amendments to FRSs and the Issues Committee ("IC") Interpretations and amendments to FRS classified as "Improvement to FRSs (2009)" which have been issued by the Malaysian Accounting Standards Board ("MASB") as described hereunder :-

New and Revised FRSs and Interpretations

		Effective for financial period beginning on or after
FRS 1	First-time Adoption of Financial Reporting Standards (Revised)	1 July 2010
FRS 3	Business Combinations (Revised)	1 July 2010
FRS 4	Insurance Contracts	1 January 2010
FRS 7	Financial Instruments : Disclosures	1 January 2010
FRS 8	Operating Segments	1 July 2009
FRS 101	Presentation of Financial Statements (Revised)	1 January 2010
FRS 123	Borrowing Costs (Revised)	1 January 2010
FRS 127	Consolidated and Separate Financial Statements (Revised)	1 July 2010
FRS 139	Financial Instruments : Recognition and Measurement	1 January 2010
IC Interpretation 9	Reassessment of Embedded Derivatives	1 January 2010
IC Interpretation 10	Interim Financial Reporting and Impairment	1 January 2010
IC Interpretation 11	FRS 2 - Group and Treasury Share Transactions	1 January 2010
IC Interpretation 12	Service Concession Arrangements	1 July 2010
IC Interpretation 13	Customer Loyalty Programmes	1 January 2010
IC Interpretation 14	FRS 119 - The Limit on a Defined Benefit Asset, Minimum Funding Requirements and their Interaction	1 January 2010
IC Interpretation 15	Agreements for the Construction of Real Estate	1 July 2010
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

Amendments to FRSs and Interpretations

		Effective for financial period beginning on or after
FRS 1	First-time Adoption of Financial Reporting Standards	1 January 2010
	Limited Exemption from Comparative FRS 7 Disclosures for First-time Adopters (Amendment to FRS 1)	1 January 2011
FRS 2	Share-based Payment - Vesting Conditions and Cancellations	1 January 2010
FRS 5	Non-current Assets Held for Sale and Discontinued Operations - Plan to sell the controlling interest in a subsidiary	1 July 2010
FRS 7	Financial Instruments : Disclosures	1 January 2010
	Improving Disclosures about Financial Instruments (Amendments to FRS 7)	1 January 2011
FRS 127	Consolidated and Separate Financial Statements : Cost of an Investment in a Subsidiary, Jointly Controlled Entity or Associate	1 January 2010
FRS 132	Financial Instruments : Presentation - Puttable Financial Instruments and Obligations Arising on Liquidation - Classification of Rights Issues - Component Part Classification for a Compound Financial Instrument	1 January 2010
FRS 138	Intangible Assets - Additional consequential amendments arising from revised FRS 3	1 July 2010
FRS 139	Financial Instruments : Recognition and Measurement	1 January 2010
IC Interpretation 9	Reassessment of Embedded Derivatives - Scope of IC Interpretation 9 and revised FRS 3	1 July 2010

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

		Effective for financial period beginning on or after
FRS 2	Share-based Payment : Scope of FRS 2 and revised FRS 3	1 July 2010
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	1 January 2010
FRS 7	Financial Instruments: Disclosures - Presentation of finance costs	1 January 2010
FRS 8	Operating Segments - Disclosure of information about segment assets	1 January
FRS 107	Statement of Cash Flows - Classification of expenditures on unrecognised assets	1 January 2010
FRS 108	Accounting Policies, Changes in Accounting Estimates or Errors - Status of implementation guidance	1 January 2010
FRS 110	Events After the Reporting Period - Dividends declared after the end of the reporting period	1 January 2010
FRS 116	Property, Plant and Equipment - Recoverable amount and sale of assets held for rental	1 January 2010
FRS 117	Leases - Classification of leases of land and buildings	1 January 2010
FRS 118	Revenue - Costs of originating a loan; and determining whether an entity is acting as a principal or as an agent	1 January 2010
FRS 119	Employee Benefits :- Curtailment and negative past service cost; - Plan administration costs; - Replacement of term 'fall due'; and - Guidance on contingent liabilities	1 January 2010
FRS 120	Accounting for Government Grants and Disclosure of Government Assistance : - Government loans with a below market rate of interest; and - Consistency of terminology with other FRSs	1 January 2010
FRS 123	Borrowing Costs - Components of borrowing costs	1 January 2010
FRS 127	Consolidated and Separate Financial Statements - Measurement of subsidiary held for sale in separate financial statements	1 January 2010
FRS 128	Investments in Associates : - Required disclosures when investments in associates are accounted for at fair value through profit or loss; and - Impairment of investment in associate	1 January 2010
FRS 129	Financial Reporting in Hyperinflationary Economies: - Description of measurement basis in financial statements; and - Consistency of terminology with other FRSs	1 January 2010
FRS 131	Interests in Joint Ventures - Required disclosures when interests in jointly controlled entities are accounted for at fair value through profit or loss	1 January 2010
FRS 134	Interim Financial Reporting - Earnings per share disclosures in interim financial reports	1 January 2010

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

		Effective for financial period beginning on or after
FRS 136	Impairment of Assets: - Disclosure of estimates used to determine recoverable amount; and - Unit of accounting for goodwill impairment test	1 January 2010
FRS 138	Intangible Assets : - Advertising and promotional activities; - Unit of production method of amortisation; and - Measuring the fair value of an intangible asset acquired in a business combination	1 January 2010
FRS 140	Investment Property : - Property under construction or development for future use as investment property; - Consistency of terminology with FRS 108; and - Investment property held under lease	1 January 2010

The Company will adopt the new, revised and amended FRSs and IC Interpretations, where applicable, when they become effective. Currently, they are expected not to have any significant impact on the financial statements of the Company upon their initial application.

The impact of applying FRS 7 and FRS 139 on the financial statements upon their first adoption is not disclosed by virtue of the exemptions provided in the respective FRSs.

5. Significant Accounting Policies

The following accounting policies, unless otherwise stated below, have been used consistently in dealing with items which are considered material in relation to the financial statements:

(a) Property, Plant and Equipment

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 income statement.

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

(b) 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.

(c) Impairment of Assets

The carrying values of assets (other than inventories and financial assets) are reviewed for impairment when there is an indication that the asset value might be impaired. Impairment is measured by comparing the carrying values of the assets with their recoverable amounts. The recoverable amount is the higher of net realisable value and value in use, which is measured by reference to discounted future cash flows. Recoverable amounts are estimated for individual assets or, if it is not possible, for the relevant cash-generating unit.

An impairment loss is charged to the income statement immediately. Subsequent increase in the recoverable amount of an asset is treated as a reversal of the previous impairment loss and is recognised to the extent of the carrying amount of the asset that would have been determined (net of amortisation and depreciation) had no impairment loss been recognised. The reversal is recognised in the income statement immediately.

(d) 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.

(e) 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.

(f) 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.

(g) 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.

(h) Income Recognition

Consultancy service charges, seminar and training fees and interest income are recognised on an accruals basis.

(i) Financial Instruments

Financial instruments carried on the balance sheet include cash and bank balances, receivables and payables. The particular recognition methods adopted are disclosed in the individual accounting policy statement associated with each item.

A financial asset is any asset that is cash; a contractual right to receive cash or another financial asset from another enterprise; a contractual right to exchange financial instrument with another enterprise under conditions that are potentially favourable; or an equity instrument of another enterprise.

A financial instrument issued by the Company is classified as a liability or equity in accordance with the substance of the contractual arrangement. Interest, gains and losses relating to a financial instrument classified as liability are reported as expense or income. Distributions to holders of financial instruments classified as equity are charged directly to equity. Financial instruments are offset when the Company has a legally enforceable right to set off the recognised amounts and intends either to settle on a net basis, or to realise the asset and settle the liability simultaneously.

(j) 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 income statement 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 and Economic Stimulus Package 2 projects (ESP2) are recognised in the income statement in the same period as the related expenses which they are intended to compensate.

Operating grants receivable from the Government of Malaysia are credited to the Government Grants Account - Operating Fund and recognised in the income statement 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 income statement over the life of the tangible/intangible assets acquired by the annual transfer of an amount equal to the depreciation/amortisation charge.

(k) 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.

(l) 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.

6. Property, Plant and Equipment

	Freehold Land	Renovation & Improvement	Furniture & Fittings	IT Equipment	Office Equipment	Motor Vehicles	Total
2009	RM	RM	RM	RM	RM	RM	RM
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 on 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
2008							
Cost:							
At 1 January		1,842,413	652,617	2,103,163	351,711	-	4,949,904
Additions		1,498,271	267,863	2,699,283	176,012	171,926	4,813,355
As at 31 December		3,340,684	920,480	4,802,446	527,723	171,926	9,763,259
Accumulated Depreciation:							
At 1 January		193,294	69,590	225,996.00	20,385.00	-	509,265
Charge for the year		305,109	83,692	448,490	45,420	10,030	892,741
As at 31 December		498,403	153,282	674,486	65,805	10,030	1,402,006
Net Book Value At 31 December 2008		2,842,281	767,198	4,127,960	461,918	161,896	8,361,253

7. Intangible Assets

	2009 RM	2008 RM
Cost :		
At 1 January	1,562,978	554,177
Addition	2,701,146	1,008,801
At 31 December	4,264,124	1,562,978
Accumulated amortisation		
At 1 January	332,172	71,385
Charge for the year	586,239	260,787
At 31 December	918,411	332,172
Carrying value at 31st December	3,345,713	1,230,806

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

8. Trade Receivables

	2009 RM	2008 RM
Trade receivables	660,945	122,975

The normal credit terms of trade receivables are 45 days (2008:45 days)

9. Short Term Deposits With Licensed Banks

The effective weighted average interest rate of the short term deposits during the year was 2.0% (2008: 2.7%) per annum.

The maturity period of the deposits range from 7 to 120 days (2008:1 to 365 days).

10. Government Grants

	Note	2009 RM	2008 RM
Development Fund	(a)	51,919,199	17,140,662
Operating Fund	(b)	1,736,882	961,902
		53,656,081	18,102,564
(a) Development Fund			
At 1 January		17,140,662	11,689,487
Add: - Grants received from the Government of Malaysia		55,895,445	17,516,900
		73,036,107	29,206,387
Less: Transfer to Income Statement			
- Depreciation for property, plant and equipment		(1,351,485)	(574,126)
- Amortisation for intangible assets		(360,490)	(187,500)
- Operational expenses		(19,404,933)	(11,304,099)
		(21,116,908)	(12,065,725)
As at 31 December		51,919,199	17,140,662

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		
At 1 January	961,902	1,296,117
Add: Grants received from the Government of Malaysia	13,800,000	12,000,000
	14,761,902	13,296,117
Less: Transfer to Income Statement		
- Depreciation for property, plant and equipment	(735,563)	(318,614)
- Amortisation for intangible assets	(225,749)	(73,287)
- Operational expenses	(12,063,708)	(11,942,314)
	(13,025,020)	(12,334,215)
As at 31 December	1,736,882	961,902

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

	2009 RM	2008 RM
Tax charge for the year	355,827	-

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:

	2009 RM	2008 RM
Surplus/(deficit) before tax	1,423,310	(175,778)
Tax calculated at statutory tax rate of 25% (2008: 26%)	355,827	-
Tax effects of:		
- expenses financed by grants which are disallowed for deductions	34,141,928	24,399,940
- government grants which are tax exempt	(34,141,928)	(24,399,940)
Tax expense	355,827	-

12. Revenue

This represents consultancy service charges and seminar and training fees.

13. Income From Grants

	2009 RM	2008 RM
Development fund (Note 10(a))	21,116,908	12,065,725
Operating fund (Note 10(b))	13,025,020	12,334,215
	34,141,928	24,399,940

14. Other Income

	2009 RM	2008 RM
Tender and documentation fees	10,450	6,921
Interest income	176,909	50,956
	187,359	57,877

15. Surplus / (Deficit) Of Income Before Taxation

	2009 RM	2008 RM
This is stated after charging:-		
(a) Audit fees	15,000	11,000
Depreciation of property, plant and equipment	2,087,048	892,741
Amortisation of intangible assets	586,239	260,787
Realised loss on foreign exchange	14,736	-
Rental		
- Office space	2,331,962	1,748,391
- Motor vehicles	171,323	-
- Space area, hall and room	397,644	-
- Office equipments	140,964	-
- Parking lot	242,675	-
- Others	416,303	-
Director's emoluments		
- Director's remuneration	310,789	241,791
- Director's fees	52,499	-
(b) Employees benefit costs	14,424,715	10,142,304

The employees benefit costs excludes director's emoluments and includes contribution to the Employees Provident Fund of RM1,301,798 (2008: RM958,988).

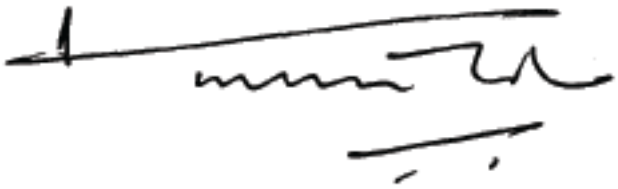
16. Capital Commitment

	2009 RM	2008 RM
Authorised capital expenditure approved but not contracted for	-	12,110,000

Statement By Directors

We, **GENERAL DATO' SERI PANGLIMA MOHD AZUMI BIN MOHAMED (RETIRED)** and **LT. COL. 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 90 to 105 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 2009 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 17 May 2010



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

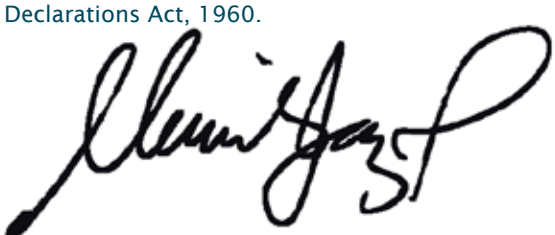
LT. COL. HUSIN BIN JAZRI (RETIRED)

Kuala Lumpur,

Date: 17 May 2010

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 90 to 105 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.



LT. COL. HUSIN BIN JAZRI (RETIRED)

Subscribed and solemnly declared by the abovenamed **LT. COL. HUSIN BIN JAZRI (RETIRED)** at Kuala Lumpur on 17 May 2010

Before me,

COMMISSIONER FOR OATHS

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

azman, wong, salleh & co (AF: 0012)
akauntan bertauliah
chartered accountants

12th floor,
wisma tun sambathan,
no. 2, jalan sultan sulaiman,
50764 kuala lumpur
tel : 03-22732688
fax : 03-22748688

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 balance sheet as at 31 December 2009 of the Company, and the income statement, statement of changes in equity and cash flow statement of the Company for the year then ended, and a summary of significant accounting policies and other explanatory notes, as set out on pages 90 to 105.

Directors' Responsibility for the Financial Statements

The Directors of the Company are responsible for the preparation and fair presentation of these financial statements in accordance with Financial Reporting Standards and the Companies Act, 1965 in Malaysia. This responsibility includes: designing, implementing and maintaining internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error; selecting and applying appropriate accounting policies; and making accounting estimates that are reasonable in the circumstances.

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 and fair presentation of the financial statements 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 2009 and of its financial performance and cash flows for the year then ended.

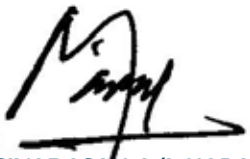
Report on Other Legal and Regulatory Requirements

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: 17 May 2010

Editorial Committee Jawatankuasa Editorial

Standing left to right:

1. **Zul Akmal Abd Manan**
   Executive, Corporate Branding & Media Relations
   Eksekutif, Penjenamaan Korporat & Perhubungan Media

2. **Azman Ismail**
   Head, Finance
   Ketua, Kewangan

3. **Siti Noriah Nordin**
   Executive, Procurement
   Eksekutif, Perolehan

4. **Azlin Samsudin**
   Executive, Legal & Secretarial
   Eksekutif, Perundangan & Kesetiausahaan

5. **Sandra Isnaji**
   Manager, Corporate Branding & Media Relations
   Pengurus, Penjenamaan Korporat & Perhubungan Media

6. **Ernieza Ismail**
   Executive, Corporate Planning & Strategy
   Eksekutif, Perancangan & Strategi Korporat

7. **Zulkifli Musnman**
   Senior Accountant, Finance
   Akauntan Kanan, Kewangan

8. **Abd Rouf Mohammed Sayuti**
   Head, Internal Audit
   Ketua, Audit Dalaman

Sitting from Left to right

1. **Razman Azrai Zainudin**
   Head, Corporate Planning & Strategy
   Ketua, Perancangan & Strategi Korporat

2. **Zahri Yunos**
   Chief Operating Officer
   Ketua Pegawai Operasi

3. **Mohd Shamil Mohd Yusoff**
   Head, Corporate Branding & Media Relations
   Ketua, Penjenamaan Korporat & Perhubungan Media

Information Security and Organizational Continuity Management

Securing Our Cyberspace

Worthy Investment for Prevention

Best Brand Internet Security 2008 & 2009

ISMS SIRIM

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

CyberSecurity MALAYSIA

An agency under MOSTI

MOSTI

Ministry of Science, Technology and Innovation

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

FORM OF PROXY

*I/We .....

of .....

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

.....

of .....

.....

or failing him .....

of .....

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

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

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

Note:

1. A Proxy need not be a member of the CyberSecurity Malaysia PROVIDED that a member shall not be entitled to appoint a person who is not a member as his proxy unless that person is an advocate, an approved company auditor or a person approved by the Registrar of Companies.
2. The instrument appointing a proxy shall be in writing under the hand of the appointor or his attorney duly authorized in writing or if the appointor is a body corporate, either under seal or under hand of the officer or attorney duly authorized.
3. To be valid the proxy form duly completed must be deposited at the Registered Office of the CyberSecurity Malaysia at Level 8, Block A, Mines Waterfront Business Park, No. 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan.

Cybersecurity Song

CYBERWORLD FOR YOU

THIS IS THE WORLD, IT'S MEANT FOR YOU
THIS IS YOUR WORLD, CYBER FOR YOU

WE'RE RESOURCEFUL
WE'RE PROACTIVE
WE'RE RESPONSIVE
WE BELIEVE IN GIVING

WE'RE IMPARTIAL
WE SPECIALIZE
WE'RE EFFECTIVE
TO STRIVE FOR QUALITY

THIS IS THE WORLD, IT'S MEANT FOR YOU
THIS IS THE WORLD, CYBER FOR YOU

THIS WORLD IF YOU LOOK IT BACK
IT'S FOR YOU TO TAKE IT
AND PUT IT RIGHT BACK ON THE MAP
CYBER FOR YOU BE SMART, BE SAFE, PROACTIVE AND RESPONSIVE...
CYBERWORLD FOR YOU
CYBERWORLD FOR YOU

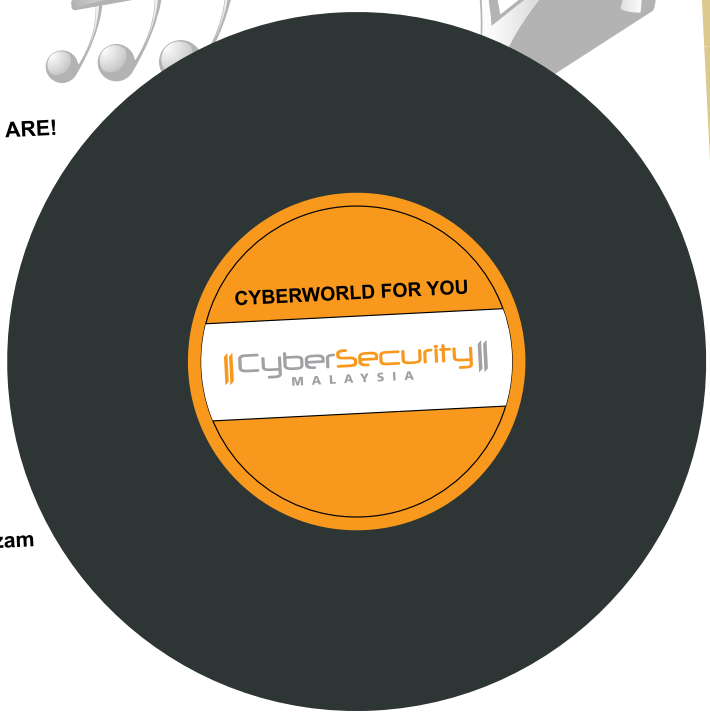
FIRST OF ALL YEAH FIRST OF ALL
WE DEFEND PROTECT & SERVE YALL
ONLINE OFFICERS OF THE INTERNET
FOR EACH PLUG & PLAY e-CONNECT
LOG ON DOT COMS
GOT A PROBLEM MAN WELL SOLVE IT THEN
CAUSE WE PRO ACT SO KNEW THAT
IT'S CYBER SECURITY FOR CYBER WORLD

C.Y.B.E.R. CYBERWORLD THAT'S WHERE YOU ARE!
C.Y.B.E.R.

QUALITY FINISH QUALITY RESISTANCE
QUALITY SERVICE QUALITY ASSISTANCE
THE BESTTEST OF THE BESTEST ONE
NEVER EVER THE BIAS ONE
INTERNET POLICE OF CYBER WAR
ON OUR GUARD WE ON THE LAW
CAUSE WE PRO ACT SO KNOW THAT
CYBER SECURITY FOR CYBER WORLD

THIS IS YOUR WORLD, CYBER FOR YOU.

Song : Dato Wan Idris
Lyricist : Col Husin & Wan Idris & Krall & Aizam



CyberSecurity MALAYSIA

CyberSecurity MALAYSIA

An Agency Under

MOSTI

Ministry of Science, Technology and Innovation

Securing Our Cyberspace

Best Brand Internet Security 2008 & 2009

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

MS ISO/IEC 17025
TESTING SAMM NO. 456

CyberSecurity Malaysia (726630-U)
Level 8, Block A, Mines Waterfront Business Park, No. 3, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia.
Phone: +603 - 8992 6888 | Fax: +603 - 8945 3205 | Email : info@cybersecurity.my | www.cybersecurity.my | www.cybersafe.my