Corporate Profile
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About CyberSecurity Malaysia</td>
<td>01</td>
</tr>
<tr>
<td>Vision</td>
<td>01</td>
</tr>
<tr>
<td>Mission</td>
<td>01</td>
</tr>
<tr>
<td>Core Values</td>
<td>02</td>
</tr>
<tr>
<td>History</td>
<td>02</td>
</tr>
<tr>
<td>Milestones</td>
<td>03</td>
</tr>
<tr>
<td>Services</td>
<td>07</td>
</tr>
<tr>
<td>1  Cyber Security Emergency Services</td>
<td>07</td>
</tr>
<tr>
<td>1.1 Cyber999 Help Centre</td>
<td>07</td>
</tr>
<tr>
<td>1.2 CyberCSI</td>
<td>07</td>
</tr>
<tr>
<td>2  Security Quality Management Services</td>
<td>08</td>
</tr>
<tr>
<td>2.1 Security Management &amp; Best Practices</td>
<td>08</td>
</tr>
<tr>
<td>2.2 Security Assurance</td>
<td>08</td>
</tr>
<tr>
<td>2.3 Cyber Security Certification</td>
<td>09</td>
</tr>
<tr>
<td>3  Infosecurity Professional Development And Outreach</td>
<td>11</td>
</tr>
<tr>
<td>3.1 Infosecurity Professional Development</td>
<td>11</td>
</tr>
<tr>
<td>3.2 Outreach</td>
<td>11</td>
</tr>
<tr>
<td>4  Cyber Security Strategic Engagement And Research</td>
<td>12</td>
</tr>
<tr>
<td>4.1 Industry Development</td>
<td>12</td>
</tr>
<tr>
<td>4.2 Government &amp; Multilateral Engagement</td>
<td>12</td>
</tr>
<tr>
<td>4.3 Research</td>
<td>13</td>
</tr>
</tbody>
</table>
Vision, Mission and Core Values

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

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

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

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

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

History of CyberSecurity Malaysia

Our journey started with the creation of the Malaysia Computer Emergency Response Team or MyCERT (www.mycert.org.my) on 13 January 1997 as a unit under MIMOS Berhad (www.mimos.my). On 24 January 1998, the National Information Technology Council or NITC (www.nitc.my) proposed for the establishment of an agency to address emerging ICT security issues in Malaysia. As a result, the National ICT Security & Emergency Response Centre (NISER) was created in 2001 as a department in MIMOS Berhad, and the Malaysia Computer Emergency Response Team (MyCERT) was placed under NISER.

On 28 September 2005, the Cabinet decided for NISER to be spun off from MIMOS Berhad as a separate entity under MOSTI. On 30 March 2007, NISER was registered as a not-for-profit Company Limited by Guarantee (CLG), wholly owned by the Government of Malaysia, under the purview of MOSTI.

During NITC meeting No. 1/2006, the Government decided to begin the implementation process of the National Cyber Security Policy (NCSP). NISER was given the mandate to provide technical support to the Government for the implementation of the NCSP. To reflect the wider mandate and larger role, NISER was renamed CyberSecurity Malaysia.

On 20 August 2007, the Prime Minister of Malaysia officiated the rebranding of NISER into CyberSecurity Malaysia, and launched the new CyberSecurity Malaysia brand name and logo.
Establishment of the National ICT Security & Emergency Response Centre (NISER)

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 Jan 1997</td>
<td>The Malaysia Computer Emergency Response Team (MyCERT) was established under MIMOS Berhad</td>
</tr>
<tr>
<td>24 Jan 1998</td>
<td>The Government of Malaysia through the National Information Technology Council (NITC) meeting 6/98, decided to establish the National ICT Security &amp; Emergency Response Centre (NISER) to assist in addressing information security issues at national level</td>
</tr>
<tr>
<td>30 Oct 1998</td>
<td>Jawatankuasa IT dan Internet Kerajaan (JITIK) or Government’s Internet and IT Committee decided to place NISER under MIMOS Berhad until it is ready to be spun off as a separate entity. MyCERT became a part of NISER</td>
</tr>
<tr>
<td>28 May 1999</td>
<td>The Strategic Thrust Information Committee (STIC) meeting 1/99 expanded the function of NISER to include national cyber defence by “creating, monitoring, and updating the defense and security systems against cyber threats” together with other Government agencies</td>
</tr>
<tr>
<td>01 Nov 2000</td>
<td>NISER became fully operational</td>
</tr>
</tbody>
</table>

Milestones - NISER

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Apr 2001</td>
<td>NISER was officially launched by the Deputy Prime Minister of Malaysia</td>
</tr>
<tr>
<td>17 Jul 2001</td>
<td>NISER organised the 1st NISER/SANS Asia Pacific Conference (the 1st professional certification program organised by NISER)</td>
</tr>
<tr>
<td>7 Nov 2001</td>
<td>NISER Panel of Experts established</td>
</tr>
<tr>
<td>29 Apr 2002</td>
<td>Launch of NISER Computer Forensic Service</td>
</tr>
<tr>
<td>19 Aug 2002</td>
<td>NISER co-founded APCERT (Asia Pacific Computer Emergency Response Team). NISER was entrusted to represent APCERT to present the report on the establishment of APCERT during the APECTEL 26th meeting in Moscow, Russia on 19-23 August 2002</td>
</tr>
<tr>
<td>16 May 2003</td>
<td>NISER was accepted to the Forum of Incident Response and Security Teams (FIRST)</td>
</tr>
</tbody>
</table>
10 Mar 2003  NISER co-launched the Information Security Management Systems (ISMS) certification scheme with SIRIM. The scheme aims to provide Malaysian organisations with the opportunity to demonstrate their compliance with international standard

26 Feb 2004  NISER led the establishment of the 1st Working Group in Business Continuity Management in Malaysia

23 Jun 2005  Proposal for the collaboration of Computer Emergency Response Teams (CERTs) among the Organisation of Islamic Cooperation (OIC) member countries was adopted during the Islamic Development Bank’s Board of Governors Meeting

4 Jul 2005  NISER established a task force for the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT). The OIC-CERT Task Force are composed of representatives from Malaysia, Pakistan, Tunisia, UAE and Nigeria

Transformation of NISER to become CyberSecurity Malaysia

28 Sep 2005  The Cabinet Meeting, through the Joint Cabinet Notes by the Ministry of Finance (MOF) and Ministry of Science, Technology and Innovation (MOSTI) No. H609/2005 agreed to spin off NISER from MIMOS Berhad.

14 Mar 2006  NISER was incorporated as a Company Limited By Guarantee. This marks the official spun off from MIMOS Berhad to become a separate agency and a National Body to monitor the National e-Security aspects, under the purview of MOSTI

1 Jun 2006  NISER operated independently and segregated from MIMOS Berhad

17 Nov 2006  Physical relocation of NISER’s operation and corporate office from MIMOS Berhad’s office at Technology Park Malaysia to Sapura@Mines Building at The Mines Resort City

30 Mar 2007  NISER’s name was changed to CyberSecurity Malaysia to better reflect its expanded role, which include coordination and implementation of the National Cyber Security Policy

20 Aug 2007  CyberSecurity Malaysia’s logo and brand name were launched by the Prime Minister of Malaysia. This marked the official rebranding and transformation of NISER into CyberSecurity Malaysia
### Milestones - CyberSecurity Malaysia

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Jul 2008</td>
<td>CyberSecurity Malaysia coordinated the first National Cyber Crisis Exercise (Cyber Drill) codenamed X-Maya in collaboration with the National Security Council.</td>
</tr>
<tr>
<td>15 Jan 2009</td>
<td>CyberSecurity Malaysia was elected as Chair of the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), thus making Malaysia the first country to chair the OIC-CERT.</td>
</tr>
<tr>
<td>22 Jun 2009</td>
<td>The Malaysian Government gazetted the role of CyberSecurity Malaysia by Order of the Ministers of Federal Government Vol.53, No.13, dated 22 June 2009 (revised and gazetted on 26 June 2013 [PU. (A) 184] by identifying CyberSecurity Malaysia as an agency that provides specialised cybersecurity services and continuously identifies possible areas that may be detrimental to national security and public safety.</td>
</tr>
<tr>
<td>07 Jul 2009</td>
<td>The Minister of Science, Technology and Innovation, Malaysia launched CyberSecurity Malaysia's Cyber999 Help Centre for the public.</td>
</tr>
<tr>
<td>08 Jul 2009</td>
<td>Created Malaysia Cyber Security Awards to honour organisational and individual contribution and commitment to cyber security. The inaugural Award Ceremony and Gala Dinner was held at the Kuala Lumpur Convention Centre in Kuala Lumpur, Malaysia.</td>
</tr>
<tr>
<td>02 Nov 2009</td>
<td>Official opening of the first regional office, serving the Northern Region, at the Perak Techno-Trade Centre in Ipoh, Perak.</td>
</tr>
<tr>
<td>01 Dec 2009</td>
<td>The Minister of Science, Technology and Innovation, Malaysia launched CyberSecurity Malaysia’s Malware Research Centre during the World Computer Security Day celebration in Kuala Lumpur.</td>
</tr>
<tr>
<td>15 Mar 2010</td>
<td>The Security Assurance Lab obtained MS ISO/IEC 17025:2005 accreditations on this day. This lab provides vulnerability assessment for ICT equipment and systems.</td>
</tr>
<tr>
<td>24 Sep 2010</td>
<td>The Deputy Prime Minister of Malaysia, who is also the Minister of Education launched ‘CyberSAFE in School’, a cyber security awareness programme for primary and secondary students, and teachers.</td>
</tr>
<tr>
<td>26 Nov 2010</td>
<td>The Government of Malaysia appointed CyberSecurity Malaysia as the Certifier and Evaluator of Malaysia Trustmark for the private sector.</td>
</tr>
<tr>
<td>01 May 2011</td>
<td>Established the Information Security Management System Audit and Certification Scheme (CSM27001) in support of the National Cyber Security Policy (NCSP).</td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>27 Sep 2011</td>
<td>The Common Criteria Recognition Arrangement (CCRA) unanimously accepted Malaysia as a Certificate Authorizing Participant, which makes Malaysia the first country among ASEAN member countries to have developed a Certification Body (CB) that is authorised by CCRA to produce the internationally recognised Common Criteria certificates that comply with the ISO/IEC 15408. (The Government appointed CyberSecurity Malaysia as the sole CB for Common Criteria on 08 October 2008).</td>
</tr>
<tr>
<td>28 Sep 2011</td>
<td>Malaysia was re-elected as the OIC-CERT Chair for a second term (2012 – 2013).</td>
</tr>
<tr>
<td>03 Nov 2011</td>
<td>The digital forensic laboratory of CyberSecurity Malaysia became the first forensic laboratory in Malaysia and the Asia Pacific region to be accredited by ASCLD/LAB for ‘Digital &amp; Multimedia Evidence’ discipline. This accreditation is based on ISO/IEC 17025: 2005 and the ASCLD/LAB - International 2011 supplemental requirement specifically for a digital forensics laboratory.</td>
</tr>
<tr>
<td>30 Nov 2011</td>
<td>CyberSecurity Malaysia became a member of the World Trustmark Alliance (WTA), which was formerly known as the Asia Pacific Trustmark Alliance (ATA).</td>
</tr>
<tr>
<td>31 Dec 2012</td>
<td>During the OIC-CERT 4th Annual General Meeting (AGM) the members elected Malaysia (through CyberSecurity Malaysia) as the OIC-CERT Secretariat for 2013 – 2015 terms, in addition to being the Chair of the OIC-CERT.</td>
</tr>
<tr>
<td>03 Jul 2013</td>
<td>Launched the Malaysia Trustmark for Private Sector (MTPS) at Putrajaya International Convention Centre.</td>
</tr>
<tr>
<td>19 Nov 2013</td>
<td>During the OIC-CERT 5th Annual General Meeting (AGM) the members elected Malaysia (through CyberSecurity Malaysia) as the permanent secretariat of the OIC-CERT.</td>
</tr>
<tr>
<td>26 Nov 2013</td>
<td>The Deputy Prime Minister of Malaysia launched the <em>Dasar dan Mekanisme Pengurusan Krisis Siber Negara</em> (Policy and Mechanism for National Cyber Crisis Management) for the National Security Council. Paragraph 16.1, Order No. 24 of the <em>Dasar dan Mekanisme Pengurusan Krisis Siber Negara</em> states that CyberSecurity Malaysia, as the specialist agency, is required to support as well as provide technical assistance and training services for national cyber crisis management.</td>
</tr>
</tbody>
</table>
1. Cyber Security Emergency Services

1.1 Cyber999 Help Centre

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

Other services under MyCERT:
• Cyber Early Warning System (such as issuance of cyber security advisories)
• Malware Research Centre (including developing security tools like DontPhishMe, the anti-phishing add-on for Internet browsers)
• Technical coordination for national cyber emergencies and coordination of cyber drills at national and international level

For more information, please visit www.mycert.org.my.

1.2 CyberCSI

The CyberCSI Digital Forensics Services include:
• Analysis of digital evidence
• First Responder for Digital Evidence
• Consultation on Quality Management
• Expert Witness
• Recovery of corrupted and deleted data
• Data sanitisation

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

CyberSecurity Malaysia’s digital forensic laboratory is the first forensic laboratory in Malaysia and in the Asia Pacific region that is accredited by the American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD/LAB) for ‘Digital & Multimedia Evidence’ discipline, based on ISO/ IEC 17025:2005 and the ASCLD/ LAB - International 2011 supplemental requirement specifically for a digital forensics laboratory.
2. Security Quality Management Services

2.1 Security Management & Best Practices

CyberSecurity Malaysia develops guidelines and best practices related to information security. It also promotes Information Security Management System (ISMS) and contributes towards standardisation development at national and international level.

CyberSecurity Malaysia is a member of WG7 under TC5 responsible for development of Malaysia Standard: Information Security Management Guidelines for Industrial Automation and Control Systems (IACS).

CyberSecurity Malaysia is also a member in standards development activities for WG/G/5-1 ISMS, TC-BCM and TC-Risk.

The “ISO/IEC 27037 Guidelines of Identification, Collection, Acquisition and Preservation of Digital Evidence”, which was initially proposed by CyberSecurity Malaysia in 2007, has been published as an International Standard on 22 October 2012. CyberSecurity Malaysia is a co-author of this standard.

2.2 Security Assurance

Our Security Assurance Services consist of Vulnerability Assessment Service (VAS), CyberSecurity Malaysia – Malaysia Security Evaluation Facility (CSM-MySEF) and Trustmark Technical Security Assessment (TTSA).

- **Vulnerability Assessment Service (VAS)**
  The National Vulnerability Assessment Centre (MyVAC), which is a unit within the Security Assurance Department of CyberSecurity Malaysia, provides VAS, at national level with the aim to improve the country’s resilience against cyber threats and exploitation due to vulnerabilities in information systems (such as Data Centre), networks (such as intranet), and technology (such as SCADA).

- **CyberSecurity Malaysia – Malaysia Security Evaluation Facility (CSM-MySEF)**
  CyberSecurity Malaysia operates one of the Malaysia Security Evaluation Facilities (MySEF) under the MyCC Scheme known as the CSM-MySEF, which is an ISO 17025 accredited test lab for security functional testing, security assessment, validation, auditing and evaluating a variety of ICT products and systems.

CSM-MySEF also provides specialized test methods under the scheme of ICT Product Security Assessment (IPSA), which include Smart Card and related devices technology. CSM-MySEF has been appointed as National Test Lab of the National Registration Department of Malaysia (NRD) and a committee member for “Project Security Assessment on MyKAD and Third Party Gateway” known as ISO/IEC JTC1/SC17 TC9, led by NRD, to evaluate security aspects of MyKAD and its related devices.
**Trustmark Technical Security Assessment (TTSA)**

The TTSA Unit is responsible for technical audit services for the Malaysia Trustmark for Private Sector (MTPS) programme. We conduct technical assessment on e-business web portal and online payment system against the TTSA technical requirements, to verify that the organisation that owns the e-business web portal has implemented security controls based on relevant security standards and best practices. The TTSA Assessment Criteria are based on the following:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Security Domain of World Trustmark Alliance (WTA) Guidelines for Trustmark Operator (GTO)
- Open Web Application Security Project (OWASP) Guideline

### 2.3 Cyber Security Certification Services

Our certification services are the MyCC Scheme, based on the Common Criteria ISO/IEC 15408, the CSM27001 Scheme, based on Information Security Management System (ISMS) ISO/IEC 27001 and the Malaysia Trustmark, based on the World Trustmark Alliance (WTA) Guidelines for Trustmark Operator (GTO).

**MyCC Scheme**

The Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme was established in 2007. It is a systematic process of security evaluation and certification, which evaluates and certifies the security functionality of ICT products, systems and Protection Profiles against the international standard ISO/IEC 15408 known as Common Criteria (CC). The methodology used in the evaluation is also a recognised standard known as Common Evaluation Methodology (CEM) or ISO/IEC 18045.

Certificates produced by MyCC Scheme are recognised globally because Malaysia, through MyCC Scheme, is a Certificate Authorising Participant of the Common Criteria Recognition Arrangement (CCRA).

MyCC Scheme maintains certified ICT products, systems and Protection Profiles register called MyCC Scheme Certified Products Register (MyCPR). Consumers may obtain the list from [http://www.cybersecurity.my/mycc/mycpr.html](http://www.cybersecurity.my/mycc/mycpr.html).

Information about the certified ICT products is made available by the MyCC Scheme for the purposes of advising and assisting interested parties on matters relating to the information security assurance of the communications and computer technologies.

Consumers using the MyCPR should be aware that the evaluated portion of a product may not include all the security functionality of the product. Consumers of ICT products are encouraged to download the Security Target and Certification Report for evaluated products to assess its suitability to meet the security needs of their organisation.

For more information, please visit [http://www.cybersecurity.my/mycc](http://www.cybersecurity.my/mycc).

**CSM27001 Scheme**

The CyberSecurity Malaysia Information Security Management System Audit and Certification (CSM27001) Scheme was established in May 2011 in support of the National Cyber Security Policy (NCSP). It offers independent security audit based on ISO/IEC 27001, which is conducted based on the strict requirements of recognised international standard and accreditation rules. Being certified with ISO/IEC 27001 provides a degree of assurance that business processes are evaluated to ensure improved performance while reducing the likelihood of security risks being present.
We maintain a list of ISO/IEC 27001 certified organizations under the CSM27001 Scheme. The list is called ‘CSM27001 Scheme Certified Organisation Register’ or CSM27001-COR. Consumers may obtain the list from http://csm27001.cybersecurity.my/cor.html.

The information about certified organisations is made available for the purpose of assisting interested parties on matters relating to the verification and selection of the certified organisations for business transactions. However, information in the CSM27001-COR is limited to the scope given by the certified organisations against the standards and controls specified in the ISO/IEC 27001.

Consumers using the CSM27001-COR should be aware that the assessed scope may not include all the business function of the organisation.

For more information, please visit http://csm27001.cybersecurity.my

- **Malaysia Trustmark for Private Sector**

The Government of Malaysia appointed CyberSecurity Malaysia as the Malaysia Trustmark Operator and Certifier for the private sector. We launched the Malaysia Trustmark for Private Sector (MTPS) programme, on 3rd July 2013. MTPS is a mechanism to encourage secure and trusted e-business in Malaysia. Under the MTPS programme, CyberSecurity Malaysia validates the legality of an organisation that is involved in e-business, and conduct Trustmark Technical Security Assessment (TTSA) to determine whether or not adequate security controls are implemented to secure the e-business.

Organisations awarded with Malaysia Trustmark logo at their validated website will distinguish themselves by meeting related regulations and best practices, and WTA code of conduct in the domain of disclosure of information, business practices, security, privacy, and alternative dispute resolution (ADR).

Please refer to the WTA Code of Conduct at the WTA Portal http://www.wtaportal.org/code.html

We maintain a list of MTPS validated e-business website. The list is called ‘MTPS Validated Website Register’ or MTPS-VWR. Consumers may obtain the list from http://mytrustmark.cybersecurity.my/VWR.html

The information about the validated e-business website is made available for the purposes of assisting interested parties on matters relating to the trust in online purchase and services.

Consumers using the MTPS-VWR should be aware that the assessed scope only covers the website or link listed in the MTPS-VWR.

For more information please visit http://mytrustmark.cybersecurity.my
3. **InfoSecurity Professional Development and Outreach**

3.1 **InfoSecurity Professional Development**

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

For more information please visit [www.cyberguru.my](http://www.cyberguru.my)

3.2 **Outreach**

CyberSecurity Malaysia aims to inculcate cyber safety and security awareness in order to create a culture of positive Internet usage amongst people from all walks of life in Malaysia.

This is carried out through an Outreach Programme known as CyberSAFE (Cyber Security Awareness For Everyone). The CyberSAFE programme includes CyberSAFE Awareness Presentation, CyberSAFE Exhibition and customised CyberSAFE programmes, such as CyberSAFE Ambassador Programme, “CyberSAFE in Schools” for Primary and Secondary schools, CyberSAFE Mentor for Institution of Higher Learning and specific cyber awareness presentation topics for organisations.

For more information please visit [www.cybersafe.my](http://www.cybersafe.my) and [www.facebook.com/cybersafe.malaysia](http://www.facebook.com/cybersafe.malaysia)
4. Cyber Security Strategic Engagement and Research

4.1 Industry Development

Cyber security is an essential enabler for wealth-creation in this era of ICT-driven economy and inter-connected society. In addition, cyber security itself is a sizeable industry. Through its Industry Development Division, CyberSecurity Malaysia hopes to spur innovation and foster greater alliances within the local and regional ICT industry.

One of our Industry Development initiatives is producing a Cyber Security Industry Directory, which provides a comprehensive listing of Malaysian companies that offer cyber security related products and services. The Cyber Security Industry Directory connects the ICT security industry players with the business entities and general public on matters related to cyber security.

Another very important Industry Development initiative is in organising the Cyber Security Malaysia – Awards, Conference and Exhibition or CSM-ACE. CSM-ACE is an annual public-private-partnership event, and the only 3-in-1 cyber security event in the country that consists of an Awards ceremony, a Conference, and an Exhibition.

- The Malaysia Cyber Security Awards (the Awards component of the CSM-ACE) are presented to distinguished individuals and organisations in recognition of their significant contributions to the cyber security industry and the well-being of the Malaysian cyberspace.

- The Conference component is a knowledge-sharing platform to gather industry experts and community on the latest trends in cyber security.

- The Exhibition component makes CSM-ACE a place to also showcase trade and investment opportunities by assisting and allowing industry players to promote their products and services.

For more information please visit www.csm-ace.my
4.2 Government & Multilateral Engagement

Our strategic engagement with the Malaysian Government is aimed at identifying and driving various government collaborations, working relations and activities to advocate the cyber security agenda.

Other than engaging local stakeholders, we also have a Multilateral Strategic Engagement Programme to facilitate cross-border cooperation.

CyberSecurity Malaysia is actively involved in regional collaborations among Computer Emergency Response Teams (CERT). It is a member of the Steering Committee of the Asia Pacific Computer Emergency Response Team (APCERT). In November 2013, it was appointed as the permanent secretariat of the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT).

CyberSecurity Malaysia is a co-founder of both APCERT and OIC-CERT; and served as the founding Chair of both organisations.

CyberSecurity Malaysia is also the administrator of the Critical National Information Infrastructure (CNII) portal (http://cnii.cybersecurity.my) and the OIC-CERT website (http://www.oic-cert.net).

4.3 Research

One of CyberSecurity Malaysia's Strategic Goals is "To Enhance Internal Research Capacity, Capability & Facility". This goal is attained through the following:

- **Strategic Policy Research**
  This includes research initiatives pertaining to cyber laws, emerging technologies, content and new policies on cyber security climate in Malaysia. We also produce research documents for reference by stakeholders and for input to policy decision makers.

- **Cyber Technology Research**
  Research on cyber security related technology, which include cryptographic algorithm, key management, cryptanalysis and applied cryptography.

- **Malware Research Centre**
  At the centre, we operate a distributed research network for analyzing malware and computer security threats. We established collaboration with trusted parties and researchers in sharing threat research information. Other activities at the centre includes:
    - Conducting research and development work to mitigate malware threats
    - Producing advisories on the latest threats
    - Threat monitoring via the distributed honeynet project
    - Partnership with universities, other CERTs and international organizations

Visit [http://honeynet.org.my](http://honeynet.org.my) for more information on our distributed honeynet project (a.k.a. Lebahnet).
Your cyber safety is our concern

Securing Our Cyberspace

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency committed to providing a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia’s self-reliance in cyberspace. Among specialised cyber security services provided are Cyber Security Responsive Services; Cyber Security Proactive Services; Outreach and Capacity Building; Strategic Study and Engagement, and Industry and Research Development.

For more information, please visit http://www.cybersecurity.my. For general inquiry, please email to info@cybersecurity.my. Stay connected with us on www.facebook.com/CyberSecurityMalaysia and www.twitter.com/cybersecuritymy

www.cybersecurity.my

The Information Security Certification Body (ISCB) provides certification services focusing on the information security based on international standards and guidelines. There are three schemes managed by ISCB:

Product certification

The Malaysian Common Criteria Evaluation & Certification Scheme (MyCC) evaluate and certify the security functions of ICT products based on the international standard ISO/IEC 15408 also known as Common Criteria.

http://www.cybersecurity.my/mycc  mycc@cybersecurity.my

Information security management system certification


http://csm27001.cybersecurity.my  csm27001@cybersecurity.my

E-Business validation

CyberSecurity Malaysia validate the e-Commerce website security, legality and good e-Commerce behaviour under the Malaysia Trustmark for Private Sector (MTPS) programme based on the e-Commerce Code of Conduct from World Trustmark Alliance (WTA) in order to increase the recognition, privacy information protection, and dispute resolution of the e-Commerce.

http://mytrustmark.cybersecurity.my  mtps@cybersecurity.my
The Malaysian Common Criteria Evaluation & Certification Scheme (MyCC) evaluate and certify the security functions of ICT products based on the international standard ISO/IEC 15408 also known as Common Criteria.

http://www.cybersecurity.my/mycc   mycc@cybersecurity.my

Product certification


http://csm27001.cybersecurity.my   csm27001@cybersecurity.my

INFORMATION SECURITY CERTIFICATION BODY

The Information Security Certification Body (ISCB) provides certification services focusing on the information security based on international standards and guidelines.

There are three schemes managed by ISCB:

CyberSecurity Malaysia validate the e-Commerce website security, legality and good e-Commerce behaviour under the Malaysia Trustmark for Private Sector (MTPS) programme based on the e-Commerce Code of Conduct from World Trustmark Alliance (WTA) in order to increase the recognition, privacy information protection, and dispute resolution of the e-Commerce.

http://mytrustmark.cybersecurity.my  mtps@cybersecurity.my

E-Business validation

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA