



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA



ENSURING INFORMATION SECURITY THROUGH THE USE OF CRYPTOGRAPHY

DATO' TS. DR. HAJI AMIRUDIN ABDUL WAHAB
CHIEF EXECUTIVE OFFICER
CYBERSECURITY MALAYSIA

09 JUNE 2020



MALAYSIA AIMS TO BECOME A DIGITAL NATION

Mobile Devices

BYOD
Bring Your Own Device

Free WiFi

Hacking Tools

SOCIAL NETWORK

CLOUD COMPUTING

VOLUME
Large amounts of data.

VELOCITY
Needs to be analyzed quickly.

VARIETY
Different types of structured and unstructured data.

WhatsApp

LINE

facebook

twitter

WeChat

Instagram

TALK

Digital economy hitting 20 per cent of Malaysia's GDP by 2020 easily achievable, says expert

17/04/2015 Fri 12:24 in Malaysia by Rezwana Manjur
Malaysia pushes to become a 'digital nation'

[in](#) [f](#) [t](#) [w](#)



DIGITAL ENVIRONMENT IS ALREADY COMPLEX

- Technology convergent adds more complexities

FINTECH

The Internet of THINGS

- Anything Any Device
- Anytime Any Content
- Anyone Anybody
- Any Service Any Business
- Any Where

Autonomous Driving

Google's modified Toyota Prius uses an array of sensors to drive. (Other components, not shown, include a 3D map.)

LiDAR:
A rotating sensor on the roof scans more than 200 feet in all directions to generate a precise three-dimensional map of the car's surroundings.

VIDEO CAMERA:
A camera mounted near the rear-view mirror detects traffic.

5G

TEST

Five Domains: Land, Sea, Air, Space, Cyber

INDUSTRY 4.0

PLATFORM INDUSTRIE 4.0

ARTIFICIAL INTELLIGENCE

BLOCK CHAIN TECHNOLOGY

THE FUTURE OF AI

SUSTAINABLE DEVELOPMENT GOAL

INCREASE IN ONLINE USAGE

APR
2020

DIGITAL AROUND THE WORLD IN APRIL 2020

THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND MOBILE, INTERNET, AND SOCIAL MEDIA USE

TOTAL
POPULATION



7.77
BILLION

URBANISATION:
55%

UNIQUE MOBILE
PHONE USERS



5.16
BILLION

PENETRATION:
66%

INTERNET
USERS



4.57
BILLION

PENETRATION:
59%

ACTIVE SOCIAL
MEDIA USERS



3.81
BILLION

PENETRATION:
49%

7

SOURCES: POPULATION: UNITED NATIONS; LOCAL GOVERNMENT BODIES; **MOBILE:** GSMA INTELLIGENCE; **INTERNET:** ITU; GLOBALWEBINDEX; GSMA INTELLIGENCE, LOCAL TELECOMS REGULATORY AUTHORITIES AND GOVERNMENT BODIES; APJIL; KEPIOS ANALYSIS; **SOCIAL MEDIA:** PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; COMPANY ANNOUNCEMENTS AND EARNINGS REPORTS; CNNIC; CAFEBAZAAR; KEPIOS ANALYSIS. ALL LATEST AVAILABLE DATA IN APRIL 2020. **COMPARABILITY ADVISORY:** SOURCE AND BASE CHANGES.

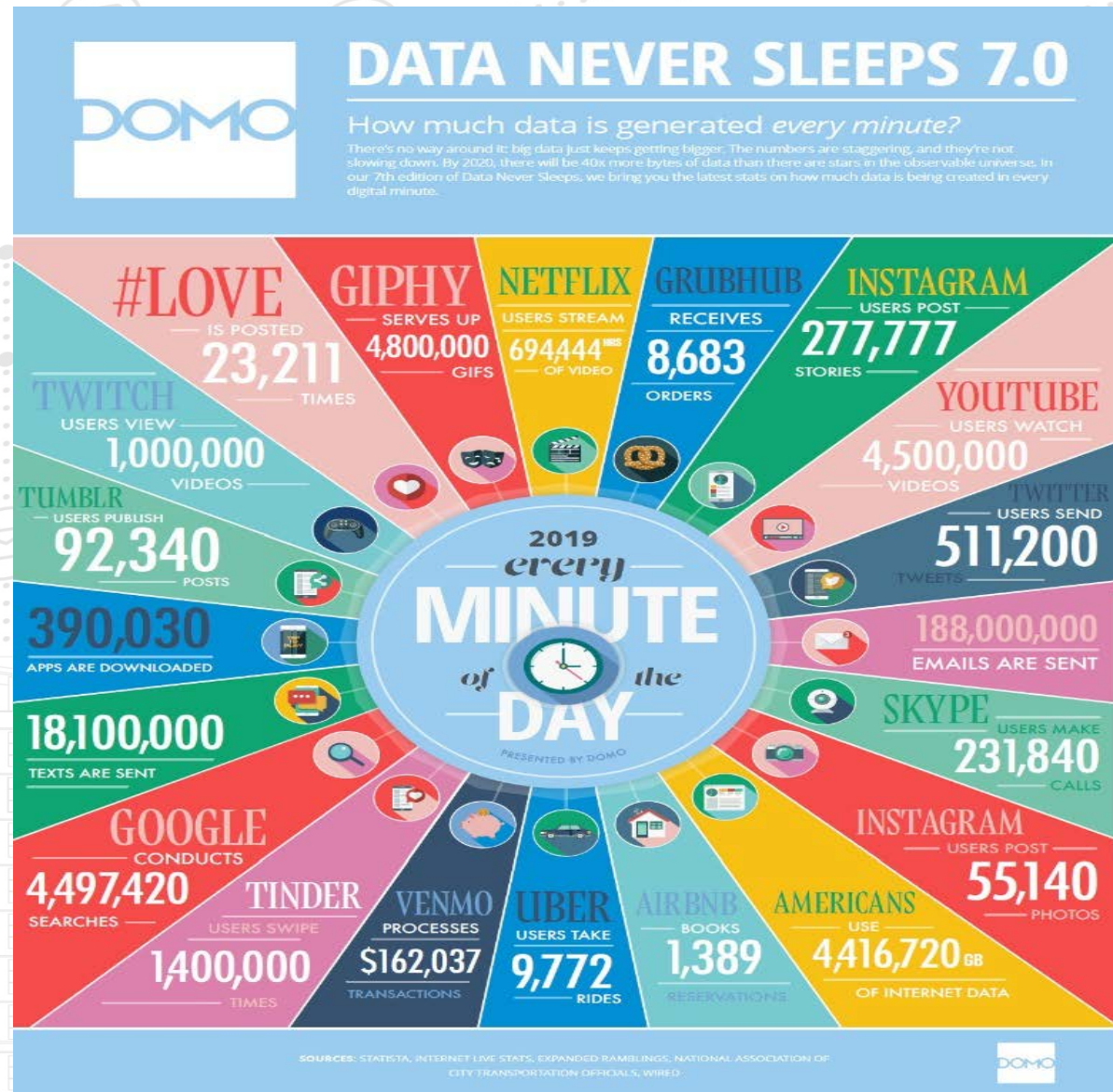
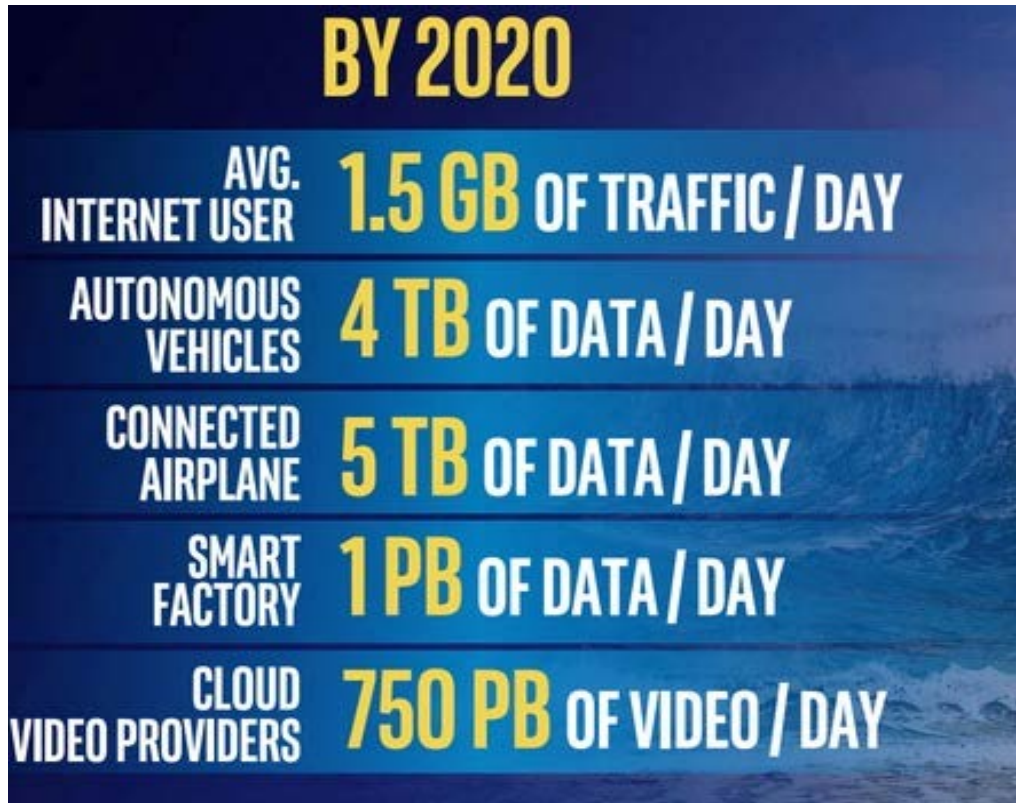
we
are
social



Hootsuite®

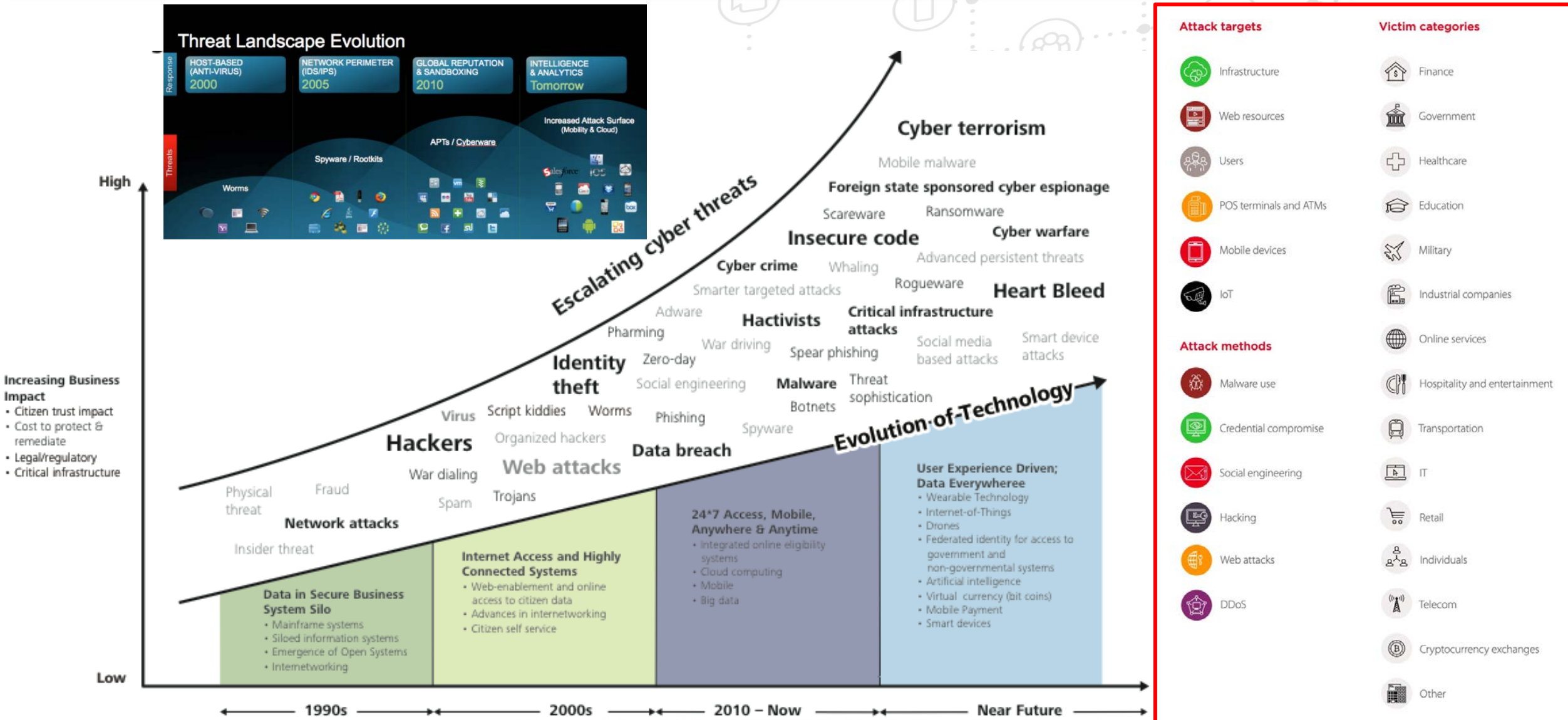
DATA TRAFFIC

THE COMING FLOOD OF DATA



THREAT EVOLUTION

- In parallel with technology advancement



As Malaysia's economy goes high tech, so do cyber threats

Cybersecurity Threats: The Risk Is Real In Malaysia

Details Published on Friday, 15 April 2016 10:42

Malaysia is among the Most Vulnerable Country to Malware Threat

Posted 13 February 2017 | By Editorial Team | Under Online Security

Berita Harian

LEBIH 3 JUTA

ANCAMAN SERANGAN SIBER 'ANONYMOUS'

ADAKAH KITA BERSEDIA

// OPEN WEB APPLICATION SECURITY PROJECT (OWASP) MALAYSIA BERI AMARAN
laman web kerajaan dengan pautan 'edu.my', 'gov.my' paling mudah diserang. Saran disingkatkan taraf

// CYBERSECURITY MALAYSIA SUDAH LAKSANA ANALISIS
teknikal dan bekerjasama dengan pihak berkaitan termasuk dari luar negara hari hadapan

North Korean hackers connect through Malaysia

FMT Reporters | January 20, 2015

A defector says Pyongyang began training computer 'warriors' in earnest in 1996.

Saturday, 20 May 2017 | MYT 8:47 AM

Cybercrime surge in Malaysia

BY ZUNAIRA SAIED

Cyber threats on the rise in Malaysia



PROTECTION OF INFORMATION AS STRATEGIC ASSET



The Fundamentals of Information Security

CYBER ESPIONAGE - Undermine Information Confidentiality

Countries with Confirmed APT 30 Targets

 India	 Thailand
 South Korea	 Saudi Arabia
 Malaysia	 United States
 Vietnam	

APT30 State-sponsored group that spied on Malaysia for 10 years - FireEye, 2015

Hacker targets info on MH370 probe

BY NICHOLAS CHENG

EXCLUSIVE: KUALA LUMPUR: The computers of high-rank agencies involved in the MH370 investigation were hacked and information was stolen.

The stolen information was allegedly being sent to a computer agency – had the transmissions blocked and the infected

PENYANGAK SIBER
INTIP MAKLUMAT KITA

// CYBERSECURITY MALAYSIA DEDAH HAMPİR SETIAP HARI ruang siber Malaysia diserang atau cuba diserang penggadam

// KEBANYAKAN SERANGAN BUKAN UNTUK LUMPuhkan sistem kerajaan, sebaliknya lebih kepada mengumpul, mencari maklumat negara

Malaysia at risk: CyberSecurity Malaysia chief covers espionage and state level attacks

This exclusive interview with CyberSecurity Malaysia's Dato' Dr Amirudin Abdul Wahab tackles themes, which are in conjunction with his opening keynote at Computerworld Malaysia Security Summit 2017.

By AvantiKumar
April 20, 2017

Source: North Korea's global spy network active in Malaysia

NATION

Thursday, 9 Mar 2017
10:22 PM MYT

Malaysia warns of Chinese hacking campaign targeting government projects

MyCERT security alert points the finger at APT40, a Chinese state-sponsored hacking crew.

To infect computers of government officials with malware and then steal confidential documents from government networks, Malaysia's Computer Emergency Response Team (MyCERT) said in a security advisory

NEWS

MyCert: Hackers targeting gov't officials for data theft

8 Feb 2020, 7:44 am · Updated 4 months ago

Evolving Cyber Threats - Cyber Espionage

Cyber Espionage

- 1998 – Moon light maze
- 2003 – Titan rain
- 2009 – operation aurora
- 2009 – Ghost net
- 2011 – Nighdragon
- 2011 – Operation shady rat (2006)
- 2012 – Red October (2007)
- 2012 – Elderwood project
- 2012 – Flame
- 2012 – Gauss (2009)
- 2012 – Shamoon
- 2014 – Mask
- 2014 – snake

Cyber Warfare

APT

APT - Advanced Persistent Threat
 PTA - Persistent Targeted Attacks

9/24/2015
 03:00 PM



Kelly Jackson Higgins

Chinese Military Behind South China Sea Cyber Espionage Attacks

An infamous advanced persistent threat hacking group known as Naikon is actually China's PLA Unit 78020 and a military intelligence expert there, traced to the attacks via his social media and other activity.



DATA LEAKAGE - Undermine Information Confidentiality

Don't leak govt secrets, civil servants warned

May 11, 2015

National security can be threatened if secrets are disseminated to foreign parties via the social media, says minister.



PUTRAJAYA: The leakage of secret information by civil servants must be curbed as they pose a danger to national security especially if they are disseminated to outside quarters via the social media.

Minister in the Prime Minister's Department Joseph Entulu Belaun warned that civil servants perpetrating these irresponsible acts would face action under the Official Secrets Act 1972 (OSA).

MALINDO AIR: DATA BREACH ALERT

PETALING JAYA, Sept 18 (Bernama) -- Malindo Airways Sdn Bhd has come to be aware that some personal data concerning our passengers hosted on a cloud based environment may have been compromised. Our in house teams along with external data service providers, Amazon Web Services (AWS) and GoQuo, our e-commerce partner are currently investigating into this breach.

Singapore, Malaysia credit card details dumped online in massive data breach

CORPORATE NEWS

Friday, 06 Mar 2020

4:10 PM MYT

By South China Morning Post



EasyJet data breached: over 9 million customers affected

The personal data of over 9 million EasyJet customers has been accessed by hackers, including over 2,000 users' credit card details

Thousands of Malaysian credit card details leaked in massive breach

Nic Ker 10/3/2020

A cybersecurity startup based in India, [Technisanct](#), recently discovered that a massive data breach has hit credit card holders in *at least* six countries in Southeast Asia: Vietnam, the Philippines, Singapore, Indonesia, Thailand, and Malaysia. The information that has purportedly been compromised is highly confidential in nature, including details such as CVV and PIN, according to [SCMP](#).

< 1 2 3 4 >

YOU MAY LIKE

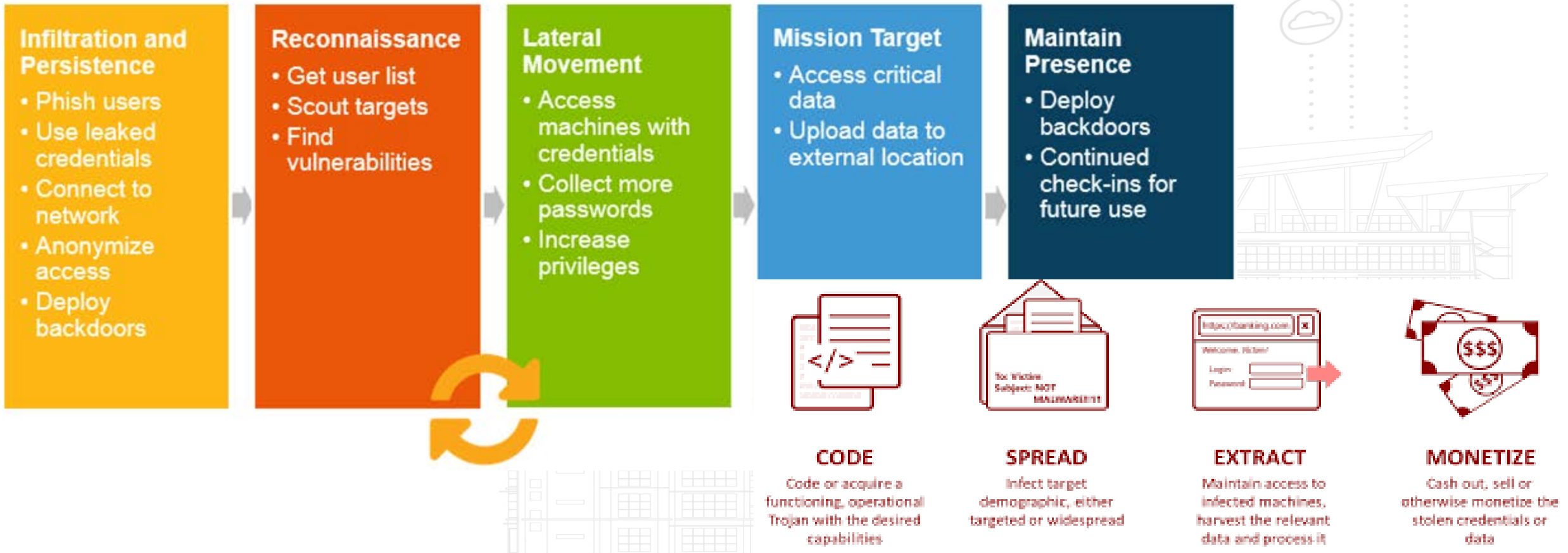
Ad taboola ▶

She was down, b
out
OurBetterWorld.c

THE USE OF COMPROMISED CREDENTIALS

- to get the access into the system and personal details

The Attack Chain



DATA LEAKAGE/BREACHED - Undermine Information Confidentiality

Malaysian government's health cover scheme in danger of data breach - group

Putrajaya's exam portal shut down, after data breach affecting millions

Published 3 weeks ago on 10 June 2018
By Zurairi Ar



Malindo Air Data Breach Exposes Millions Of Passengers' Personal Data, Including Passport Details!

Published 19 hours ago on September 19, 2019
By Esther Liew



Thousands of Malaysian credit card details leaked in massive breach

Nic Ker 10/3/2020

A cybersecurity startup based in India, Technisanct, recently discovered that a massive data breach has hit credit card holders in *at least* six countries in Southeast Asia: Vietnam, the Philippines, Singapore, Indonesia, Thailand, and Malaysia. The information that has purportedly been compromised is highly confidential in nature, including details such as CVV and PIN, according to SCMP.

YOU MAY LIKE

Ad taboola



Malaysia data breach traced to Netherlands and Hong Kong

Personal details of 220,000 Malaysian organ donors and their next of kin leaked online



TRENDS OF HACKTIVISM & WEB DEFACEMENTS

- Undermine Information Integrity



Deface By Kambeng Merah : Credit To DarkJawa

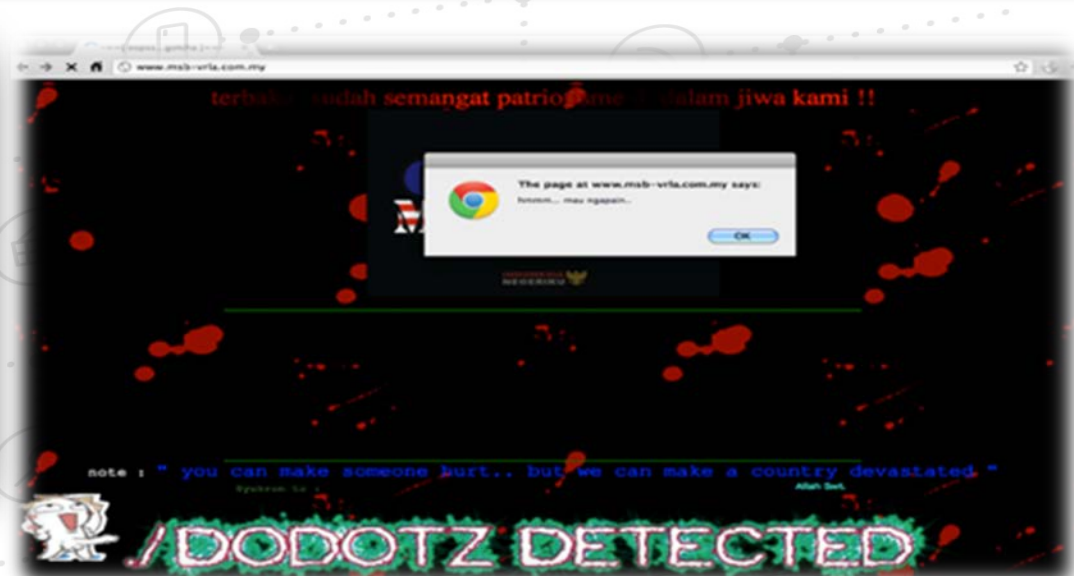
DO NOT BLOCKED US FROM FREEDOM OF USING INTERNET !!

Some Of MALAYSIAN Voice!

Setelah dimaklumkan penutupan dan penapisan internet yang berlaku dengan serentak hari ini ramai pengguna internet kecewa dengan tindakan yang sebegini...

Penulis: Puanita ku ingin kau tahu(SKMD)

“OPERATION MALAYSIA” by ANONYMOUS
(14 - 19 June '11) – 210 websites defaced



DALAM NEGERI

ARKIB : 18/02/2013

Tingkatkan keselamatan laman web elak digodam - KSN

KUALA LUMPUR 18 Feb. - Ketua Setiausaha Negara, Datuk Seri Ali Hamsa mengarahkan agar tahap keselamatan laman web rasmi setiap kementerian dipertingkatkan bagi menangkis ancaman penggodam.

Beliau berkata, keadaan masih terkawal walaupun sistem e-Akhbar dan e-Press milik Jabatan Penerangan disyaki telah digodam hari ini.

"Saya percaya ini adalah tindakan pihak tidak bertanggungjawab, bagaimanapun saya percaya kementerian yang bertanggungjawab akan menjalankan siasatan berhubung perkara itu.

WEB DEFACEMENT - Undermine Information Integrity



Cyber-attacks: Most hackers are local, says minister



Lee Long Hui
Jun 17, 11
4:04am

TEXT SIZE 1 2 3

Share 10 friends can read this story for free Like 30

The federal government believes that most of the cyber-attacks against government websites over the past few days originated locally.



Science, Tech and Innovation Minister Max K. Ongkili (left) that initial investigations estimated that u

Government Websites Hacked - Again

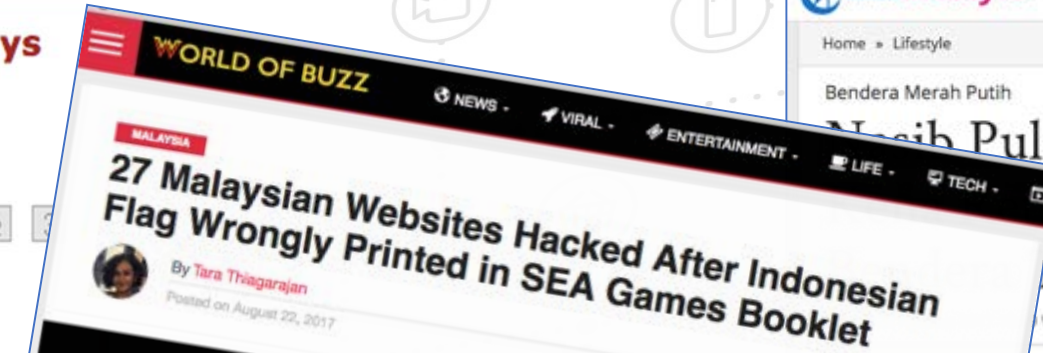
Details Published on Thursday, 02 January 2014 10:29



KUALA LUMPUR: Hackers launched attacks on a slew of websites in Malaysia last night, defacing at least two government portals on New Year's Eve.

The Education Ministry(MOE) portal apparently had its main landing site replaced with a plain black page which said "Hacked", with one "EviSha0w Team" claiming responsibility.

At the time of writing, the MOE website was inaccessible, though various screen captures depicting the defacement was posted up by netizens.



RANSOMWARE DENIES ACCESS TO INFORMATION ASSETS

- Undermine Information Availability



TODAY'S TOP STORIES

Ransomware takes Hollywood hospital offline, \$3.6M demanded by attackers

hpmc
 Credit: [Hollywood Presbyterian Medical Center](#)

Network has been offline fore more than a week, \$3.6 million demanded as ransom

CSO | Feb 14, 2016 3:43 PM PT

MORE LIKE THIS

hollywood ransom to get access back to its encrypted files
 Hospital pays \$17,000 ransom to get access back to its encrypted files

2015 hacks
 The most innovative and damaging hacks of



WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack?

WannaCry caused chaos
 By Danny Palmer | May 11, 2018

Orang biasa pun sudah boleh lancar serangan siber guna 'ransomware'

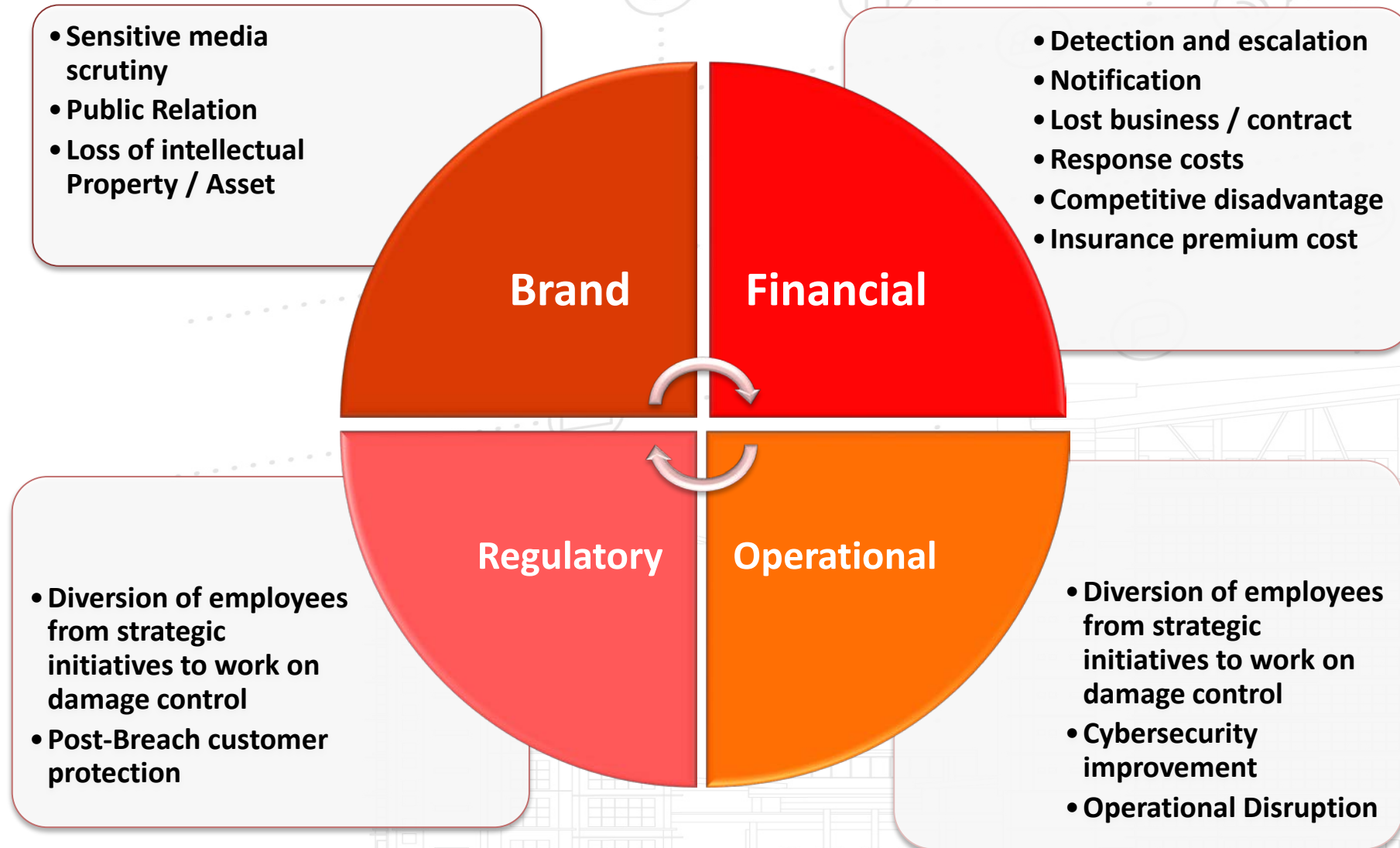
Ian Johan Ariff, Astro Awani | Mei 04, 2020 21:00 +08 | Durasi: 2 minit, 25 saat

WannaCry ransomware attack in Malaysia confirmed

Posted on 16 May 2017 - 06:41pm
 Last updated on 17 May 2017 - 12:14am
 Amar Shah Mohsen
newsdesk@thesundaily.com

SHARE

INFORMATION INSECURITY - Causes Devastating Impacts



EMERGING CHALLENGES OF DIGITAL TRANSFORMATION IN THE A NEW NORMAL ENVIRONMENT

COVID-19 & DIGITAL TRASFORMATION - Device Usage During Covid-19

APR 2020

COVID-19: PEOPLE SPENDING MORE TIME WITH DEVICES

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 IN SELECT COUNTRIES* WHO REPORT SPENDING MORE TIME USING EACH DEVICE IN RECENT WEEKS

SMARTPHONE OR MOBILE PHONE



76%

global web index

LAPTOP COMPUTER



45%

we are social

DESKTOP COMPUTER



32%

we are social

TABLET DEVICE



22%

SMART TV OR MEDIA STREAMING DEVICE



34%

we are social

GAMES CONSOLE



17%

global web index

SMART SPEAKER



11%

we are social

SMART WATCH



6.3%

9

SOURCE: GLOBALWEBINDEX'S CORONAVIRUS MULTI-MARKET STUDY (WAVE 2, APRIL 2020). *NOTE: FIGURES REPRESENT THE FINDINGS OF A SURVEY OF INTERNET USERS AGED 16 TO 64 IN AUSTRALIA, BRAZIL, CANADA, CHINA, FRANCE, GERMANY, INDIA, IRELAND, ITALY, JAPAN, NEW ZEALAND, PHILIPPINES, SINGAPORE, SOUTH AFRICA, SPAIN, THE UNITED KINGDOM, AND THE UNITED STATES. DATA COLLECTION (FIELDWORK) TOOK PLACE BETWEEN MARCH 31 AND APRIL 02, 2020. SEE GLOBALWEBINDEX.COM FOR MORE DETAILS.

we are social

Hootsuite®

A NEW NORMAL

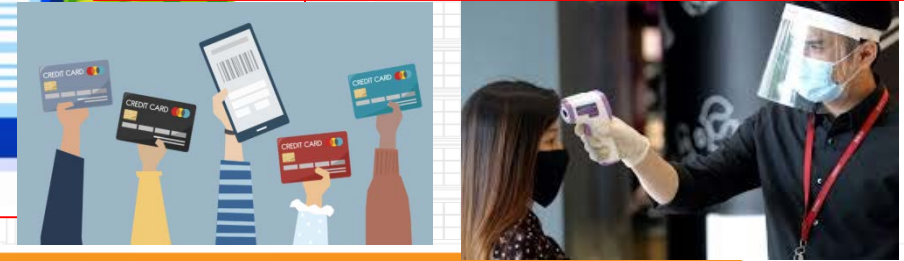


PEOPLE ARE SPEND MORE TIME ONLINE

List of eWallet in Malaysia



Online Shopping Malaysia



A NEW NORMAL WITH NEW APPS



GERAK MALAYSIA supports the Government of the spread of the virus through contact tracing.

THE RISE OF CYBER THREATS DURING COVID-19

Cyber Security Today – What’s behind data breaches, holes in two American COVID aid websites, EasyJet data breach and more



Howard Solomon @howarditwc
Published: May 20th, 2020

Scammers even more active during this MCO period

Data Loss Spikes Under COVID-19 Lockdowns

Two new reports suggest a massive gap between how organizations have prepared their cybersecurity defenses and the reality of their efficacy.

COVID-19-era data breaches go beyond unemployment insurance fraud, medical research hacks, and other hot topics. And unfortunately for public organizations and private companies, the data loss — from theft or otherwise

- Cyber scams based on COVID-19 have become prevalent in recent months, as hackers look to capitalize on the virus-driven uncertainty affecting individuals, enterprises, & governments

Minister: 220 investigation papers opened on Covid-19 fake news to date

Over 500,000 Zoom accounts sold on hacker forums, the dark web

By Lawrence Abrams

Watch out for cyber criminals during COVID-19 : Fortinet



SELASA, 26 MEI 2020

Nasional

Kes penggodaman ketika PKP cecah 80.5 peratus

Kegiatan bagi tujuan dapat maklumat sulit, jatuhkan imej seseorang

Oleh Luqman Arif Abdul Karim
luqman.arif@bh.com.my

kanaan dijual atau digunakan bagi kegiatan peras ugut.

"Ada juga siri penggodaman didalangi untuk motif menjatuhkan imej atau reputasi seseorang, selain cubaan untuk mewujudkan sentimen politik," katanya kepada BH, semalam.

Ketua pelucutan senjata Pertubuhan Bangsa-Bangsa Bersatu (PBB), Izumi Nakamitsu, kelmarin mendedahkan jenayah siber meningkat 600 peratus, membitkan e-mel berniat jahat ketika pandemik COVID-19.

"Sekiranya dalam menggunakan protokol internet (IP) sebenar, proses pengesanan akan menjadi lebih mudah. Tetapi, jika mereka menggunakan teknik 'IP spoofing', 'proxy server/IP' atau 'Botnet/Zombie Computer', pengesanan akan menjadi amat sukar," katanya mengulas sama ada CSM berupaya menjejaki anasir yang melancarkan insiden penggodaman di Malaysia.

Ditanya langkah CSM bagi menangani peningkatan insiden penggodaman dan memastikan kes-

pembayaran secara bitcoin.

"Pelbagai mesej mengenai kaedah penggunaan Internet dalam bentuk infografik, video grafik serta klip video dikeluarkan melalui Instagram, Facebook, YouTube dan LinkedIn.

"Usaha ini dilaksanakan bagi memupuk kesedaran pengguna Internet serta memberi maklumat mengenai kepentingan mengamalkan nilai etika yang tinggi di alam siber secara berterusan pada setiap masa walaupun sewaktu PKP

HOME / MALAYSIA

Ministries warned about increasing cyber threats, Zoom's security flaws

Wednesday, 08 Apr 2020 09:57 AM MYT
BY ALEXANDER WONG

sama pada 2019.

Ketua Pegawai Eksekutif CyberSecurity Malaysia (CSM), Datuk Dr Amirudin Abdul Wahab, berkata insiden pengoda-

Berdasarkan pemantauan lanjut, Amirudin berkata, sebanyak 2,726 insiden keselamatan siber dilaporkan warga digital Malaysia ke Cyber999, berbanding

April lalu.

"CSM menerusi Pak Balas Kecemasan Malaysia (MyCERT) mengeluarkan dua an-

24

New Straits Times - WEDNESDAY, MAY 13, 2020

HIGHER ED

Curbing cyber threats in online learning

ROZANA SANI
rsani@nt.com.my

HIGHER education institutions (HEI) need to take steps to tighten access of their network infrastructure as well as caution users to be more vigilant in protecting their data and privacy when engaging in online and distance learning.

Large-scale online learning was implemented in a rushed manner in such institutions in the country due to the sudden disruption of traditional in-classroom activities by the Covid-19 pandemic, leaving campus networks open to vulnerabilities.

While digital and online platforms, as well as software and applications, provide the necessary means and convenience for distance teaching and learning to take place, there are learn-

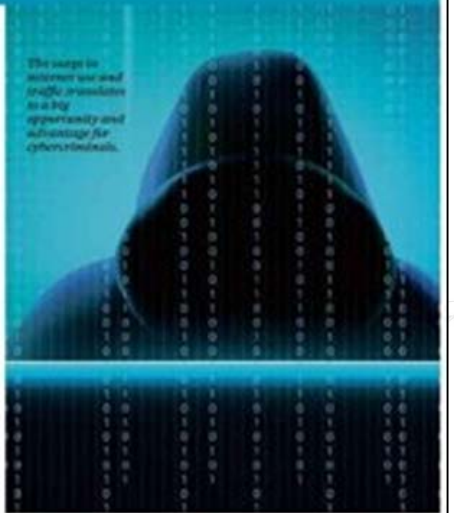
plan for months or years to find a valuable piece of information. They aim for large enterprises or government entities," he shared.

As such, Tajul Athar said there was an urgency in securing networks and educating users among the institutions.

Nurhazim who agrees with Tajul Athar's opinion said, "Once universities have gotten into the new normal, they should look to reneighbour what privacy and security controls they may have temporarily set aside when moving to online learning.

"This is especially true for the most sensitive university IT systems, such as the payroll or accounting database, as well as student information and human resource systems. Moreover, universities must train their students, lecturers and other stakeholders on how to identify online scams and phishing," he said.

CyberSecurity Malaysia said that as people worked from home the number of cyber threats rose and security controls



The urge to return work and study premises to a big opportunity and advantage for cybercriminals.



Associate Professor Dr. Nurhazim



TIPS FOR STAYING SAFE IN THE CYBERWORLD

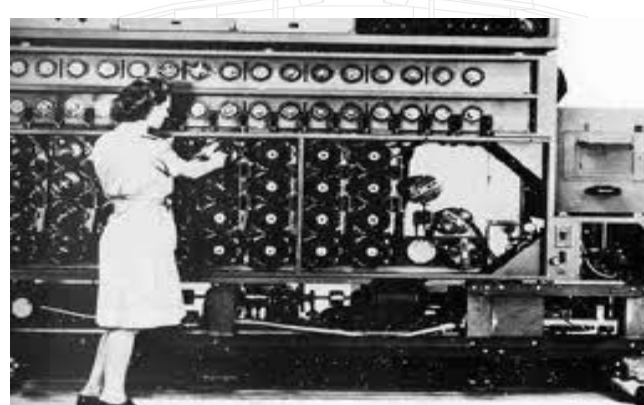
1. Install security software on all devices.
2. Use passwords and multi-factor authentication.

Cybersecurity cases rise by 82.5%

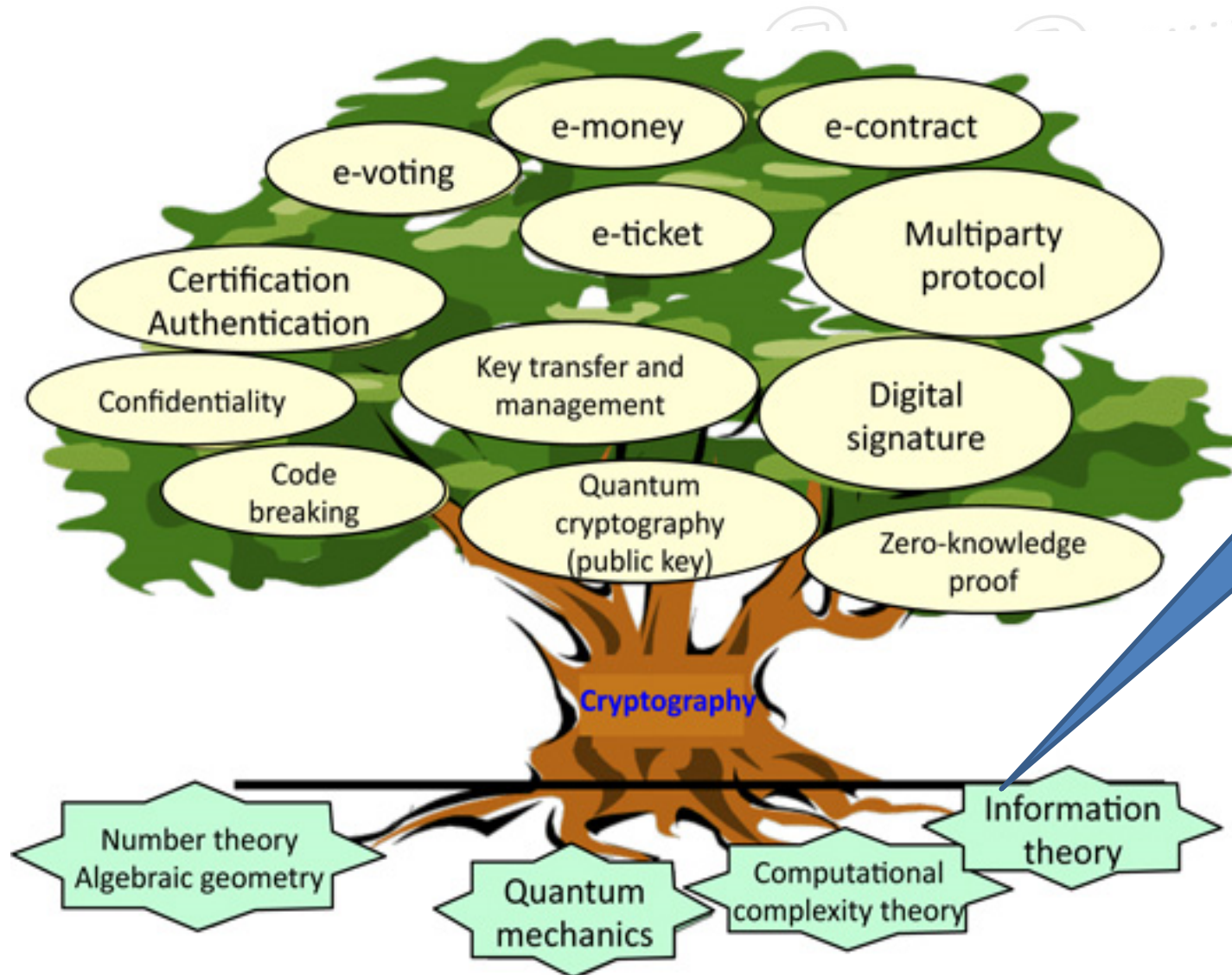
Cyber harassment, fraud spike during MCO

BIRTH OF MODERN CRYPTOGRAPHY AND COMPUTERS

- Mathematicians at Bletchley Park, UK played an integral role to break Nazi German encrypted messages during World War 2 – and has been historically acknowledged to shorten the war by 2 years.



THE MATHEMATICS OF CRYPTOGRAPHY



The root is mathematics

CRYPTOGRAPHY - The Last Line of Defense



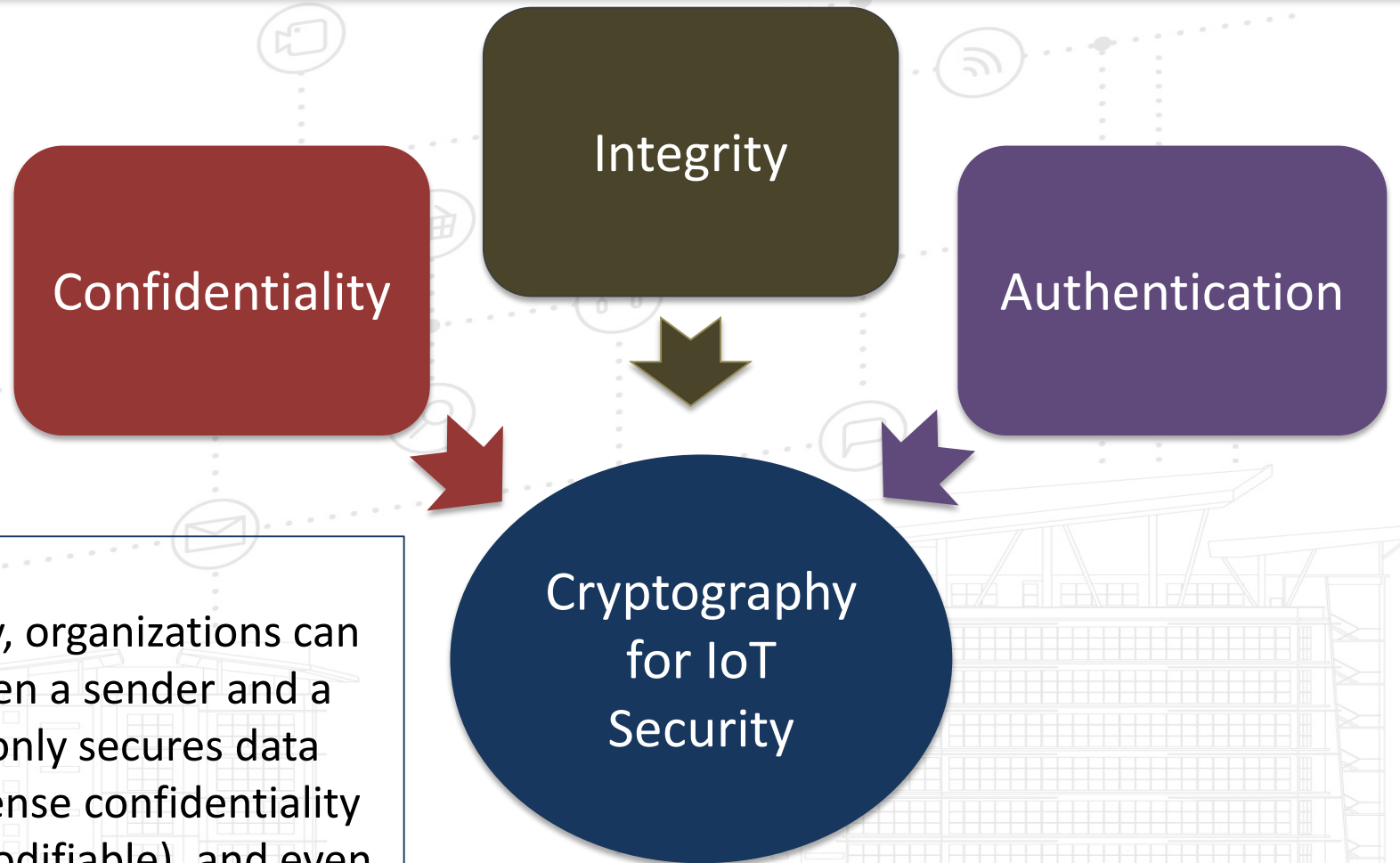
The Role of Cryptography in Information Security

Cryptography can be used to achieve several goals of information security, including confidentiality, integrity, and authentication.

- ✓ **Confidentiality:** First, cryptography protects the confidentiality (or secrecy) of information. Even when the transmission or storage medium has been compromised, the encrypted information is practically useless to unauthorized persons without the proper keys for decryption.
- ✓ **Integrity:** Cryptography can also be used to ensure the integrity (or accuracy) of information through the use of hashing algorithms and message digests.
- ✓ **Authentication:** Finally, cryptography can be used for authentication (and non-repudiation) services through digital signatures, digital certificates, or a Public Key Infrastructure (PKI).

https://www.oreilly.com/library/view/cissp-for-dummies/9781118417102/a2_13_9781118362396-ch08.html

CRYPTOGRAPHY FOR INTERNET OF THINGS



Cryptography for IoT security

By using cryptography for IoT security, organizations can ensure that the data in transit between a sender and a receiver is secure. Cryptography not only secures data from hackers, but also provides immense confidentiality (un-understandable), integrity (un-modifiable), and even authentication (only legit participants can share) to data.

CRYPTOGRAPHY - The issues are yet to be fully addressed

Report: CIA-linked encryption firm sold rigged equipment to Malaysia, other countries

Zoom security issues: Zoom buys security company, aims for end-to-end encryption

Here's a timeline of every security issue uncovered in the video chat app.

Malaysia tidak guna Crypto AG untuk maklumat rahsia

Muhyiddin: No data leakage from use of Crypto AG encryption devices

By Zahratulhayat Mat Arif - February 15, 2020 @ 6:13pm

News Straits Time

REGULATION
by Kevin Helms

Apr 4, 2020

10001

Malaysia Becomes the Next Country to Approve Cryptocurrency Exchange Amid Covid-19 Crisis



MALAYSIA'S INITIATIVES IN
INFORMATION SECURITY

POLICY & PROCESS

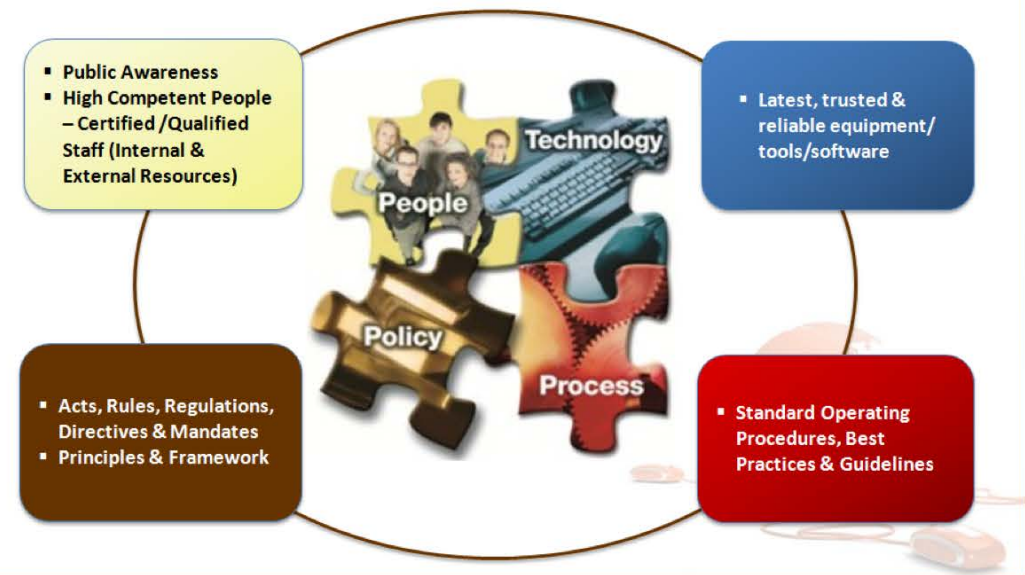


**MALAYSIA CYBER
SECURITY STRATEGY
(MCSS)**

- **Adoption of holistic approach that identifies potential threats to organization and impacts to the national security & public well-being ; and**
- **To develop the nation to become cyber resilience having the capability to safeguard the interests of its stakeholders, reputation, brand and value creating activities.**

HOLISTIC APPROACH

Cyber Resilience is the ability for an organization to resist, respond and recover from threats that will impact the information they require to do business.



ADDRESSING FUNDAMENTAL ASPECTS OF CYBER SECURITY



National Cryptography Policy (NCP)

- *Approved by The Government In January 2013*

- Comprehensive applications of cryptography in Government to Government (G2G), Government to Citizens (G2C), Government to Business (G2B) and Business to Business (B2B) activities towards ensuring a secure and trusted cyber environment. Cryptography also supports the National Digital Economy and the realization of the National Transformation Agenda to transform Malaysia into becoming an advanced and high income nation

Confidentiality

Option:
secret key
public key



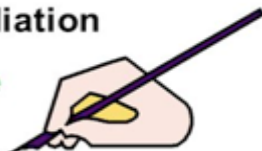
Integrity

Digital
Signature

Non-Repudiation

Digital Signature

Signature & Date



Authentic

???

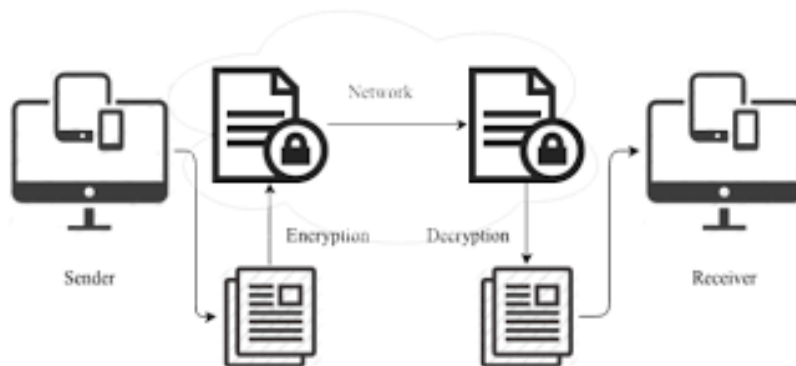
GUIDELINE FOR CRYPTOGRAPHY IMPLEMENTATION

MySEAL
Senarai Algoritma Kriptografi Terpercaya Negara

Guideline on the Usage of
Recommended AKSA MySEAL
Cryptographic Algorithms
(v1.0)

CyberSecurity Malaysia

17 December 2019



Personal Data Protection Act 2010 (PDPA)



LAWS OF MALAYSIA

ACT 709

PERSONAL DATA PROTECTION ACT 2010

Date of Royal Assent :

2 June 2010

Date of publication in the Gazette :

10 June 2010

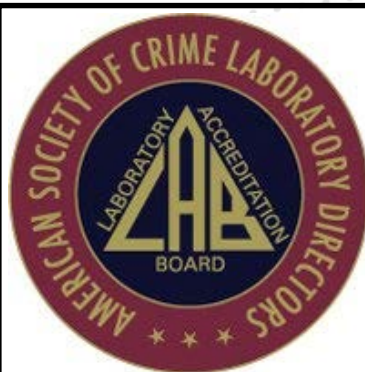
- Governs personally identifiable data collected via commercial transaction.
- Malaysia's PDPA is align with the EU's GDPR.

COMPLYING TO INTERNATIONAL STANDARD & PROCESSES:

- Common Criteria ISO/IEC 15048 , ISMS ISO/IEC 27001, ISO 17025 etc

CyberSecurity Malaysia Malaysian
Security Evaluation Facility (MySEF)

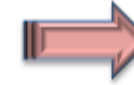
ISO  17025
ACCREDITED LABORATORY



Digital Forensic
Laboratories has been
recognized by ASCLD/LAB
as the first organization in
Asia Pacific to receive
ASCLD/LAB-International
accreditation in the field
of Computer &
Multimedia Discipline



MS ISO/IEC 17799:2007



Comprehensive Scope

- **Internal and external issues** that are relevant to organisational purpose;
- **Interested parties and their requirements** that are relevant to the ISMS;
- **interfaces and dependencies** of both internal and external activities

MS ISO/IEC 27001:2013

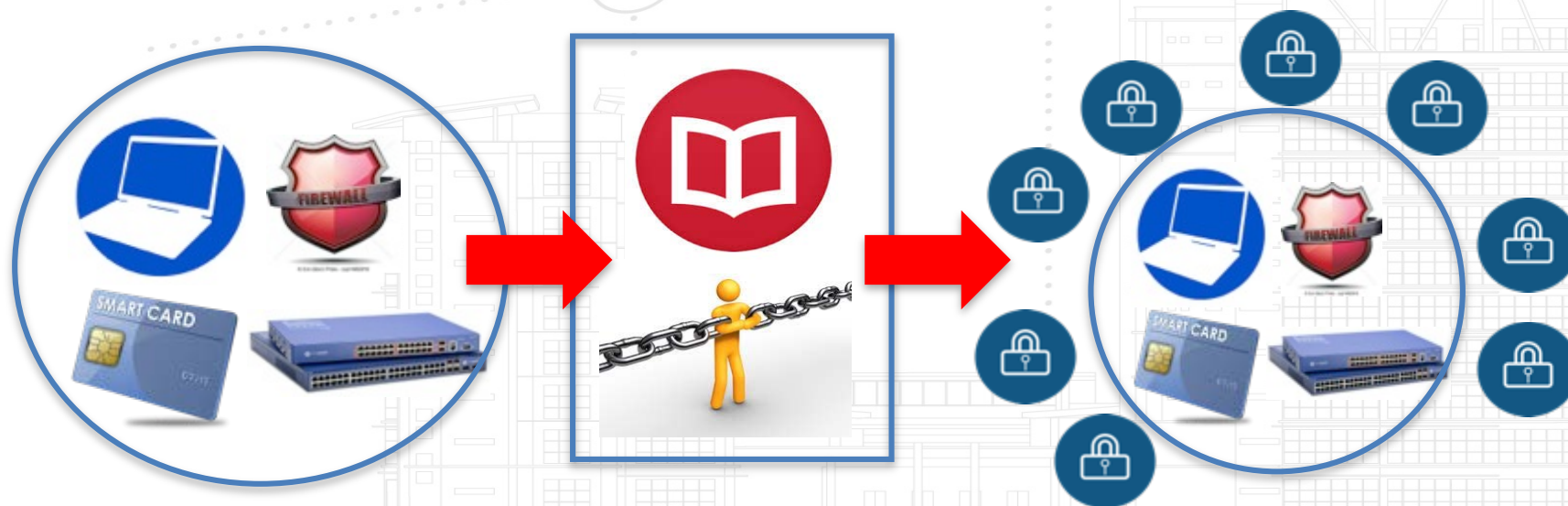
Adopted as Malaysian Standards



PROCESSING PREVENTIVE ACTION VIA ICT PRODUCTS AND SYSTEMS EVALUATION



Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme provides a systematic process for evaluating and certifying the security functionality of ICT products & systems against defined criteria or requirements of ISO/IEC 15408 Common Criteria standard.



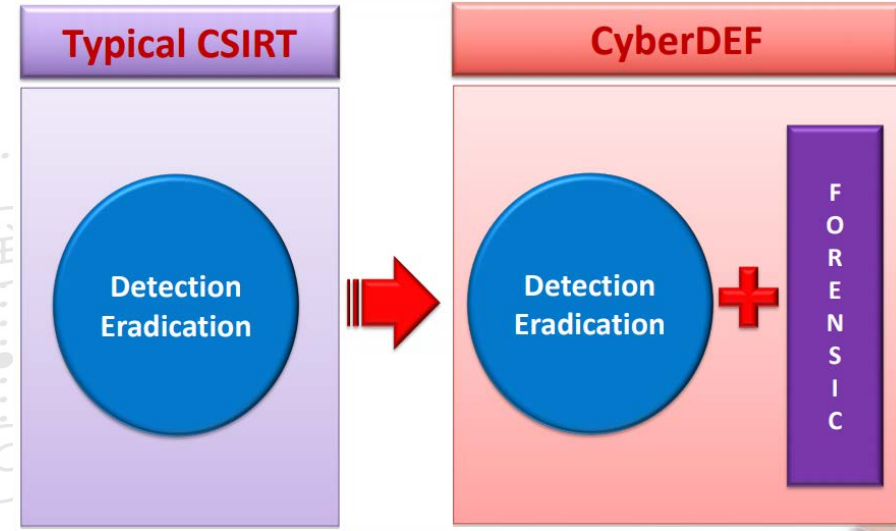
TECHNOLOGY

STRENGTHENING CYBER SECURITY **DETECTIVE** CAPABILITIES THROUGH:



CyberD.E.F

- Detection
- Eradication
- Forensic



Detection

Identify any loopholes, vulnerabilities and existing threats

1. Sensors
2. Sandbox
3. Analytics
4. Visualization

Eradication

Close loopholes, patch vulnerabilities and neutralize existing threats

Perform cyber threats exercise or drill to test the feasibility and resiliency of the new defense / prevention system

Forensics

1. E-Discovery
2. Root cause analysis
3. Investigation
4. Forensics readiness
5. Forensic compliance

Cyber threats and cyber attacks landscape have changed. Our data and technology are constantly under threat especially with the growth of advance persistent threats (APT). These targeted attacks to organisations are planned, organised and highly-skilled.

Cyber criminals are now more focused and savvy with cyber attacks conducted across multiple stages and mediums. These lead to organisations being exposed and vulnerable to cyber attacks resulting in data theft, breach of trust, denial of service and tarnished reputation.

Thus, organisations need to be responsive, proactive and pre-emptive in tackling cyber security.

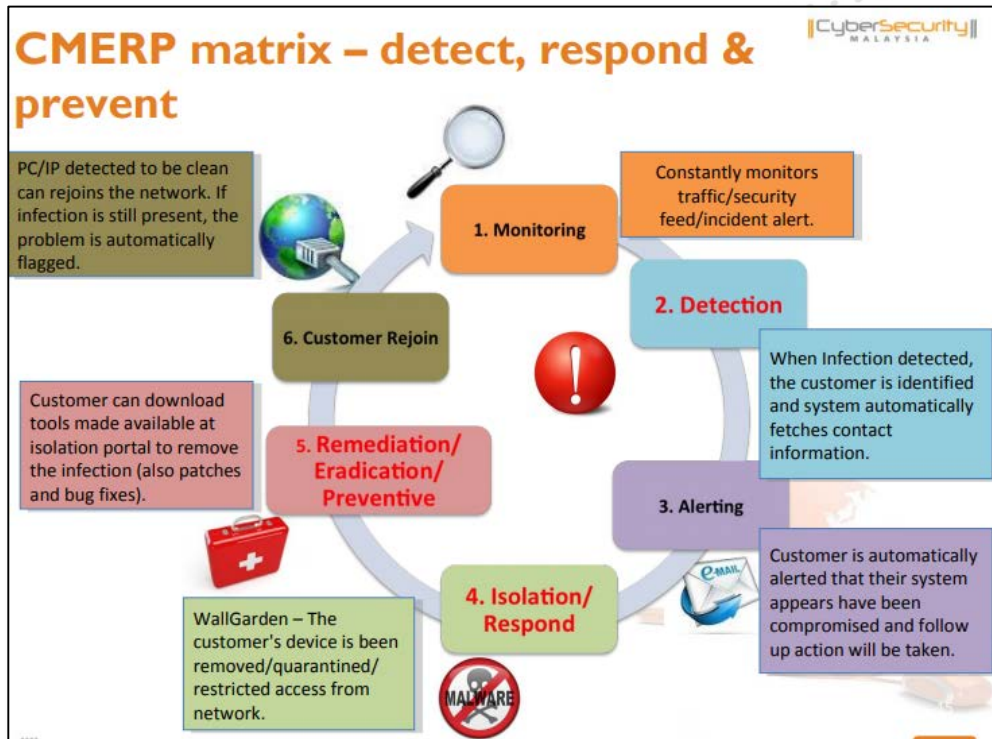
Organisations should be equipped with:

1. **Cyber analytics capability**
 - + to identify emerging threat patterns
 - + to anticipate intrusions
 - + assess their capability to handle attacks
2. **Cyber forensic capability**
 - + to analyse the attacks
 - + to prevent future attacks
3. **Computer Security Incident Response Team (CSIRT) and facilities ready.**

These basic building blocks of a cyber intelligence framework not only help an agency continuously monitor its risks, but also create a more dynamic situational awareness that drives better decision-making across a wider range of mission and business activities.

CSM-UTEM Coordinated Malware Eradication Remediation Research Project (CMERP)

CMERP’s mission is to address the computer security concerns of Malaysian Internet users. Their objectives is to reduce the number of bot/malware infection in Malaysia, provide proactive measure to safeguard and mitigate malware infection.



CMERP satellite lab to tackle malware threats in Malaysia

Bername | August 03, 2017 07:41 MYT



CSM, UTeM kongsi kepakaran pembangunan makmal satelit

Oleh Noor Azurin Mohd Sharif
bhnews@bh.com.my



DURIAN TUNGGAL: CyberSecurity Malaysia (CSM) dan Univerisiti Teknikal Malaysia Melaka (UTeM) berkongsi kepakaran bagi pembangunan Makmal Satelit Coordinated Malware Eradication and Remediation Project (CMERP) bernilai RM7.4 juta.

COLLABORATION IN CRYPTOGRAPHY

CSM collaboration with different Institution of Higher Educations (IHEs) and agencies

Research



Various research collaboration in cryptography and blockchain technology. Among others are collaboration with INSPEM UPM, UM, UNITEN and others. Research collaborations includes exchange of knowledge and expertise.

Conference & Training



CSM has co-organize several cryptography conference, including CRYPTOLOGY and MyCrypt2016. CSM has also collaborate in providing and receiving cryptography training from various IHEs and agencies.



MySEAL

Collaborate with various agencies and IPT in Malaysia and overseas to develop our own National Cryptographic Algorithm Trusted List (MySEAL) for Algoritma Kriptografi Sedia Ada (AKSA) and Algoritma Kriptografi Baharu (AKBA)



Evaluation

CSM provide cryptographic module evaluation and cryptographic algorithm conformance testing for IHEs and agencies. Our laboratory has been accredited to conduct the testing since 2018

CYBERSECURITY MALAYSIA RESEARCH & DEVELOPMENT (R&D) COLLABORATION

- Building Innovative Programs Through Effective Capacity Building

To Identify Technologies That Are Relevant and Desirable by the CNII

To Promote Collaboration with International Center's of Excellence

To Provide Domain Competency Development



STRENGTHENING CYBER SECURITY PREVENTION THROUGH TECHNOLOGY VULNERABILITY ASSESSMENT

Secure Software Development Lifecycle (SSDLC) Lab & Services



Internet of Things (IOT) Lab



Robotic Lab (4th Industry Revolution)



CSM's LAB ARE FULLY COMPLIED WITH INTERNATIONAL STANDARDS & PROCESSES

CyberSecurity Malaysia Malaysian Security Evaluation Facility (MySEF)

ISO 17025
ACCREDITED LABORATORY



MS ISO/IEC 17799:2007



Comprehensive Scope

- **Internal and external issues** that are relevant to organisational purpose;
- **Interested parties and their requirements** that are relevant to the ISMS;
- **interfaces and dependencies** of both internal and external activities

MS ISO/IEC 27001:2013

Adopted as Malaysian Standards



Digital Forensic Laboratories has been recognized by ASCLD/LAB as the first organization in Asia Pacific to receive ASCLD/LAB-International accreditation in the field of Computer & Multimedia Discipline

GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES

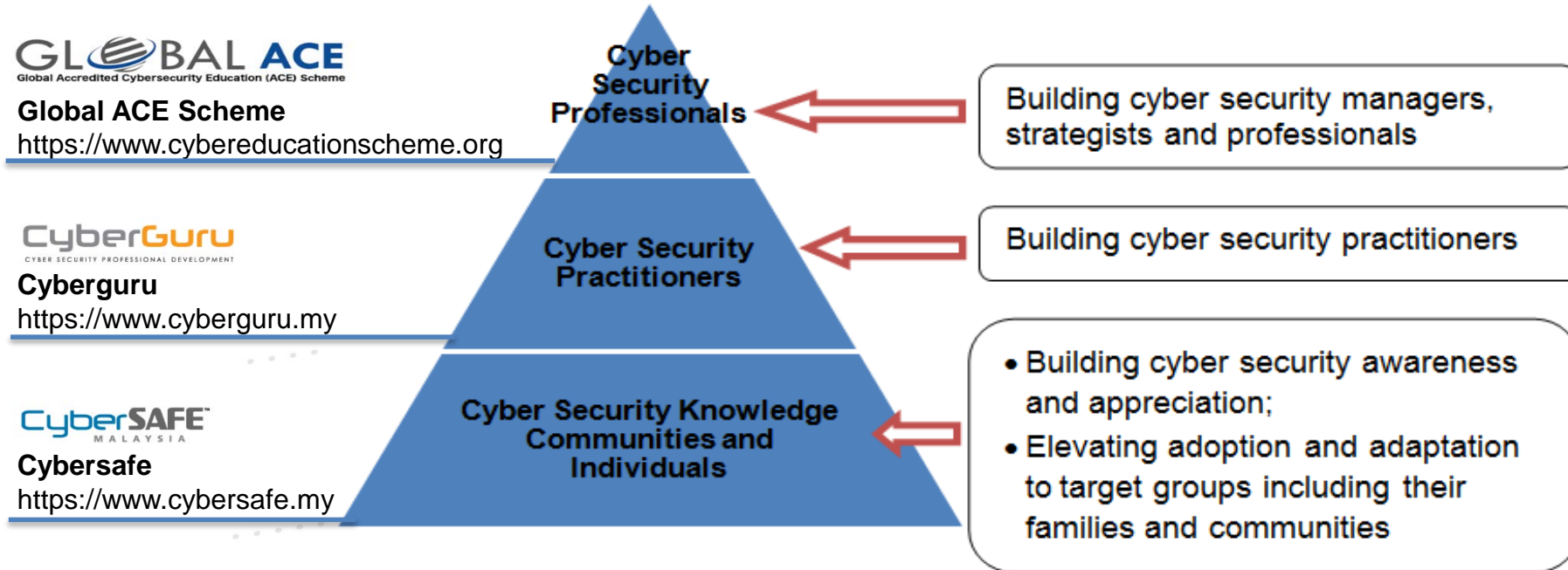
First and foremost, INTERPOL would like to thank the Council of Europe for sharing the 'Basic Guide for the Management and Procedures of a Digital Forensics Laboratory' document. The Council of Europe's guide provided a strong foundation and has been used as a model for developing this document.

In addition, INTERPOL would like to express sincere gratitude to CyberSecurity Malaysia as the partner in making these guidelines a reality. CyberSecurity Malaysia's expertise and experience in an accredited digital forensics laboratory has been invaluable in completing this document.



PEOPLE

CYBER SECURITY CAPACITY BUILDING FRAMEWORK



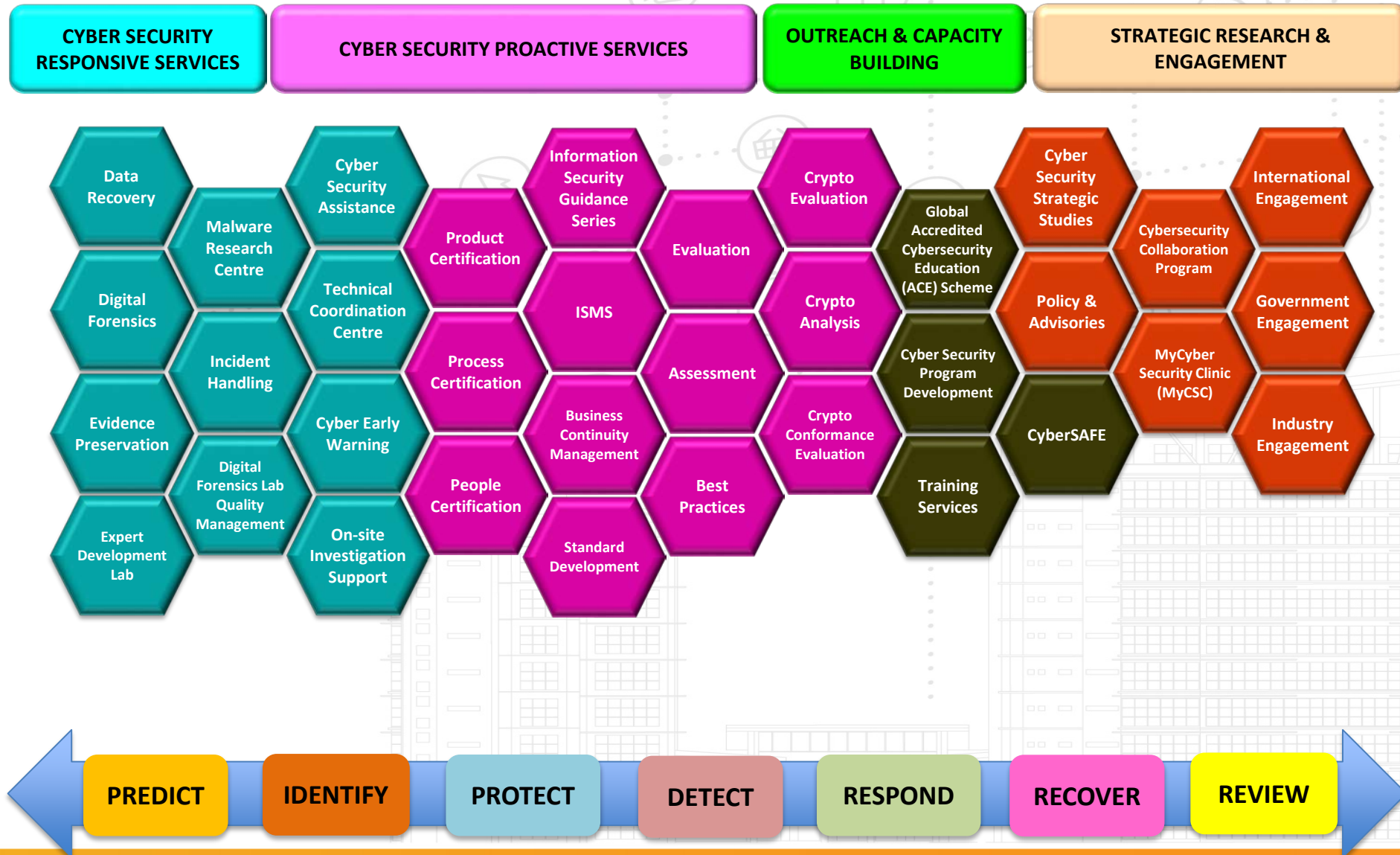
OBJECTIVES

To nurture cyber security knowledge groups and/or individuals that are resilient to cyber security incidents

To nurture cyber security practitioners that are technically capable and proficient in the operation;

To nurture cyber security professionals that are capable in strategizing, planning and executing cyber security initiatives⁴⁶

CSM SERVICES ACROSS CYBER SECURITY DOMAIN & LIFECYCLE



AWARDS AND RECOGNITION

				
<p>YBhg. Dato' Ts. Dr. Haji Amirudin Abdul Wahab, Chief Executive Office of CyberSecurity Malaysia received the Recognition of Excellence Award at the Malaysia OpenGov Leadership Forum held in Putrajaya on 20 September 2018.</p>	<p>CyberSecurity Malaysia has received DataVisionary Award from Hortonworks. It shows that CyberSecurity Malaysia is one of the few pioneers in the world for implementing Big Data, Machine Learning and Artificial Intelligence in cyber security.</p>	<p>Professional Award for Development of Professional Relations in Information Security from Russia.</p> <ul style="list-style-type: none"> General Tan Sri Dato' Seri Panglima Mohd Azumi Mohamad (Retired), Chairman of the Board of Directors, CyberSecurity Malaysia 	<p>Champion of WSIS 2016 and Best Review by WSIS Expert Group for Securing the Cyber Space Through International Collaboration of the CERT project</p> 	 <p>FireEye Best Cyber Security Innovation Award 2015</p>
			 <p>ISLA Award</p>	
<p>CyberSecurity Malaysia became the 1st winner for Asia Pacific Region, during the 1st Global CyberLympics championships (an ethical hacking competition) – Year 2011</p>	<p>The Security Assurance Lab obtained MS ISO/IEC 17025:2005 accreditations</p>	<p>CIO Excellence & Leadership Dr. Solahuddin Shamsuddin Chief Technology Officer, CSM – year 2016</p>	<p>ISLA Award: 17 honorees from Malaysia (CyberSecurity Malaysia) (2009 to 2013)</p>	<ol style="list-style-type: none"> SMEs Chapter Awards 2009 – Cybersecurity The Grammy Awards for Branding - Internet Security 2008
	<p>CyberSecurity Malaysia's CyberSAFE portal www.cybersafe.my won the Saramad Golden Award for "The Best Initiative in Child Online Protection" from among 148 participating organisations, during the 6th International Digital Media Fair & Festival 2012 (IDMF 2012) in Tehran, Iran.</p>			<p>The most outstanding CSOs in ASEAN region :</p> <ul style="list-style-type: none"> YBhg. Dato' Ts. Dr. Amirudin Abdul Wahab, Chief Executive Officer, CyberSecurity Malaysia – Year 2014

CyberSecurity Malaysia Leadership (International)



- 24 Countries**
- | | | |
|----------------------|------------|------------|
| Oman | Malaysia | Azerbaijan |
| Iran | Indonesia | Egypt |
| United Arab Emirates | Bangladesh | Brunei |
| Cote D'Ivoire | Jordan | Kazakhstan |
| Kuwait | Libya | Morocco |
| Nigeria | Pakistan | Qatar |
| Saudi Arabia | Sudan | Syria |
| Tunisia | Uzbekistan | Turkey |

- The only cybersecurity Training Provider in MTCP under the Ministry of Foreign Affairs

APCERT Asia Pacific Computer Emergency Response Team Economies

Digital Forensics Lab is the 1st in Asia Pacific region that accredited by American Society of Crime Laboratory Directors (ASCLD)/LAB certification

Chairman for 2014 & 2015 for World Trustmark Alliance Annual

CERTIFICATE AUTHORIZING

CERTIFICATE CONSUMING

- Focal point in organizing cybersecurity training for African Region, Middle East Region and Asian Region.
- Member Country Partnership Strategy (MCPS) - spearheaded cybersecurity area under Reverse Linkage Program. Assist Central Bank of Suriname to establish ISMS Framework

- Serves as cyber security expert & co-chair in the Council for Security Cooperation in the Asia Pacific (CSCAP) Malaysia

Deputy Chair of the 32 Global Expert Council Members Of APEC E-Commerce Business Alliance ECBA

CONCLUSION AND WAY FORWARD

- **Cryptography** is yet to adequately addressed in Malaysia
- To effectively **apply information security fundamentals via cryptographic innovative techniques**
- Strengthening **Public-Private-Academia Partnership and International Collaboration**
- **Cryptographic solutions to evolve in parallel with technology** by enhancing:
 - Sharing of Information amongst relevant parties
 - Cyber Incidents Response and Coordination
 - Innovative & Collaborative Research
 - Capacity Building
 - Cyber Security Awareness and Education

ANY CYBER INCIDENTS YOU CAN REPORT TO US AT:



Cyber999 Help Centre:

Cyber999 Hotline:
1-300-88-2999

Email:
cyber999@cybersecurity.my

Fax:
+603-8945 3442

Handphone:
+6019 - 266 5850 (24X7 - Emergency)

Online: Fill up online form at
http://www.mycert.org.my/report_incidents/online_form.html

SMS:
CYBER999 REPORT <EMAIL><COMPLAINT> to
15888

Cyber999

USE INTERNET PRUDENTLY. YOU DO WANT TO BECOME VICTIMS ON MISCONDUCT OF INTERNET

If you encounter any cyber security threats or incidents, report it to the help center CYBER999

CYBER999 APP

App Store - Apple iOS
<https://itunes.apple.com/us/app/cyber999-mobile-application/id888552400?mt=8>

Google Play - Android
<https://play.google.com/store/apps/details?id=com.cyber999.mobile&hl=en>



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA







Thank you

Corporate Office
CyberSecurity Malaysia
Level 7, Tower I
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

T : +603 8800 7999
F : +603 8008 7000
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

-  www.facebook.com/CyberSecurityMalaysia
-  twitter.com/cybersecuritymy
-  www.youtube.com/cybersecuritymy
-  [CyberSecurity Malaysia](#)
-  [cybersecurity_my](#)



Best Brand
Internet Security
2008 & 2009



CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : AK 4656



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



ISMS 02082013 CB 02

