MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

STAYING AHEAD OF EMERGING SECURITY CHALLENGES IN DIGITAL INDUSTRIAL REVOLUTION - MALAYSIA'S PERSPECTIVE

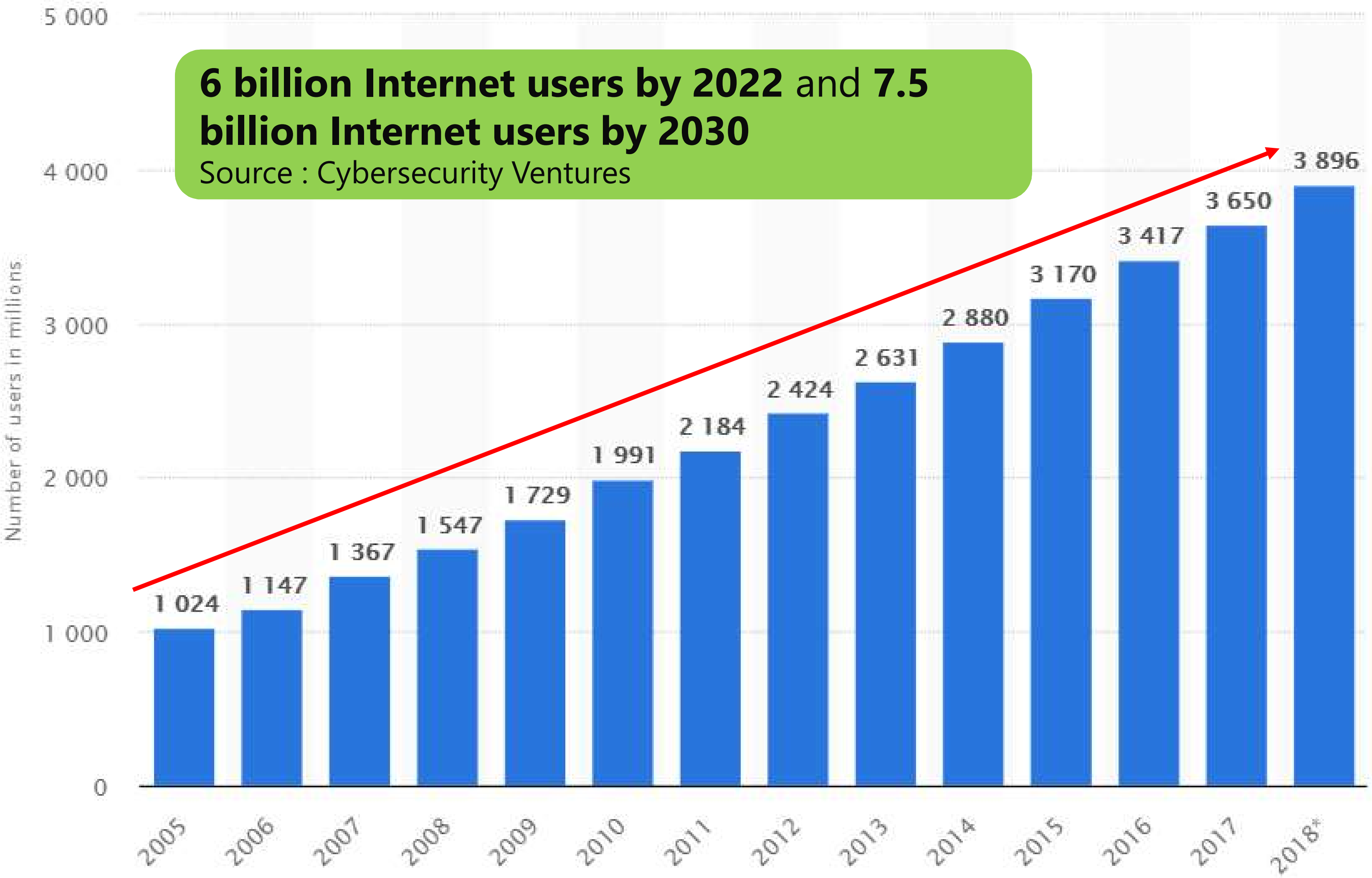
by

Dato' Dr. Haji Amirudin bin Abdul Wahab
Chief Executive Officer
CyberSecurity Malaysia

16 May 2019

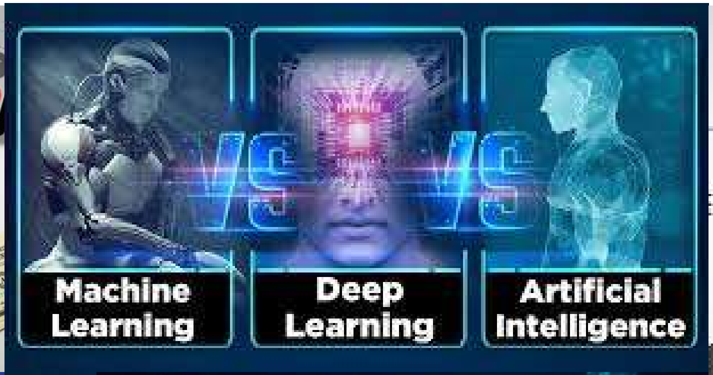
OUR DIGITAL WORLD TODAY

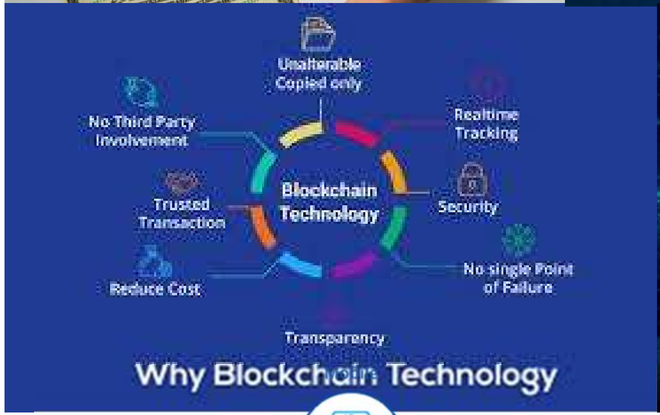
WE ARE MOVING INTO A MORE INTERCONNECTED CYBERSPACE

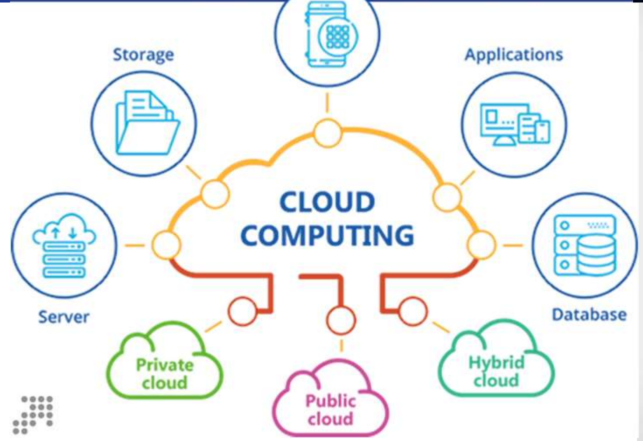


6 billion Internet users by 2022 and **7.5 billion Internet users by 2030**
Source : Cybersecurity Ventures

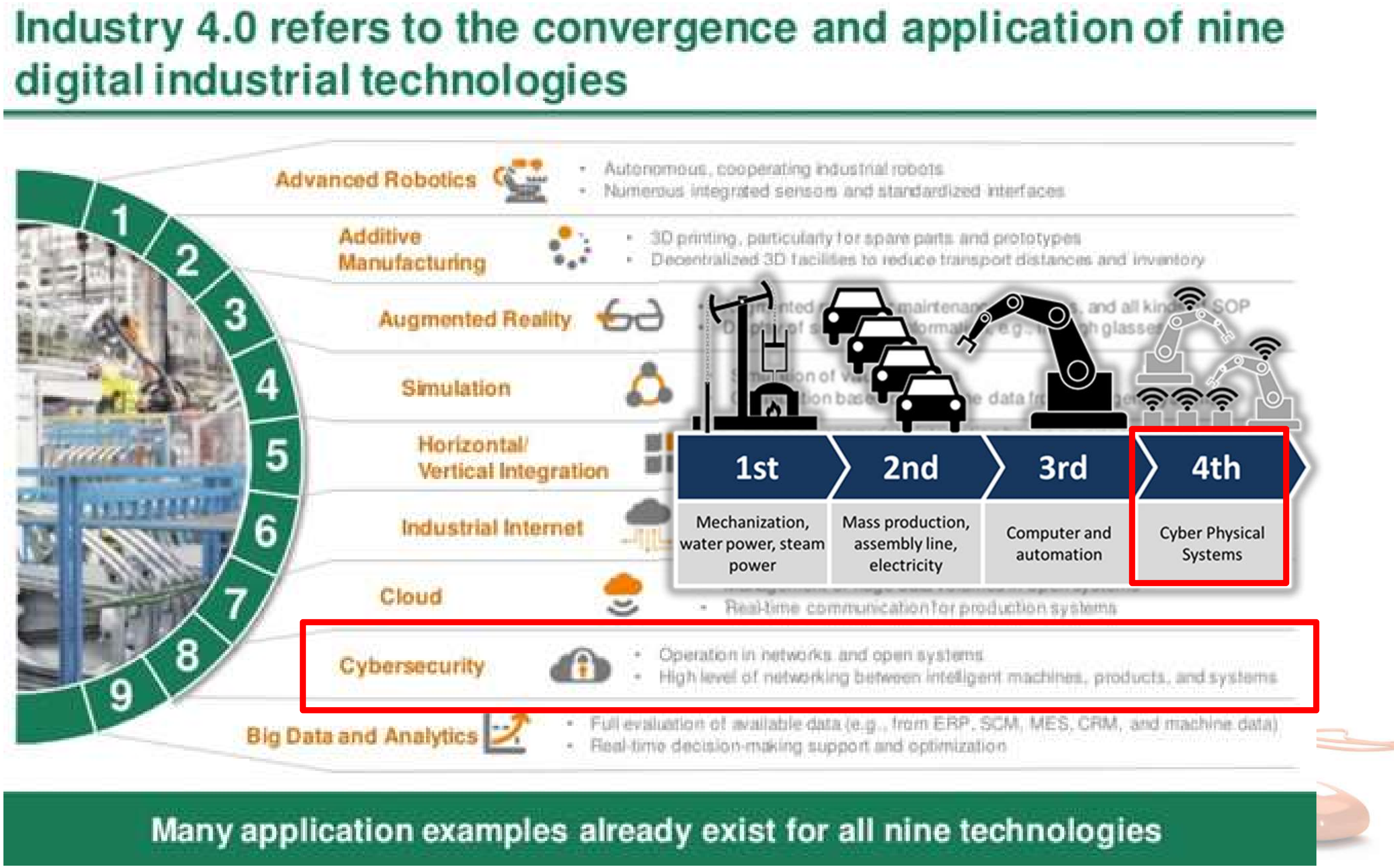
CONVERGENCE OF NEW TECHNOLOGIES INTO CYBER SPACE
- Add More Complexities







INDUSTRY 4.0 IS A SET OF RAPIDLY EVOLVING AND CONVERGING TECHNOLOGIES



Industry 4.0 refers to the convergence and application of nine digital industrial technologies

Advanced Robotics
- Autonomous, cooperating industrial robots
- Numerous integrated sensors and standardized interfaces

Additive Manufacturing
- 3D printing, particularly for spare parts and prototypes
- Decentralized 3D facilities to reduce transport distances and inventory

Augmented Reality
- Augmented [illegible] maintenance, [illegible], and all kind of SOP
- Display of [illegible] information, e.g., through glasses

Simulation
- Simulation of [illegible]
- Optimization based on [illegible] data from [illegible]

Horizontal/ Vertical Integration

Industrial Internet

Cloud
- Real-time communication for production systems

Cybersecurity
- Operation in networks and open systems
- High level of networking between intelligent machines, products, and systems

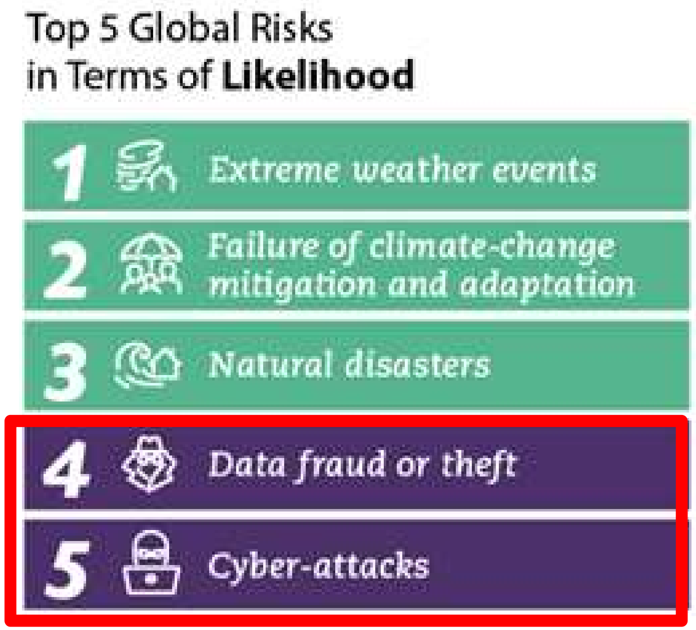
Big Data and Analytics
- Full evaluation of available data (e.g., from ERP, SCM, MES, CRM, and machine data)
- Real-time decision-making support and optimization

1st	2nd	3rd	4th
Mechanization, water power, steam power	Mass production, assembly line, electricity	Computer and automation	Cyber Physical Systems

Many application examples already exist for all nine technologies

SECURITY CHALLENGES OF 4TH INDUSTRIAL REVOLUTION (4IR)

TOP 5 RISKS IN 2019



Top 5 Global Risks in Terms of **Likelihood**

1 *Extreme weather events*

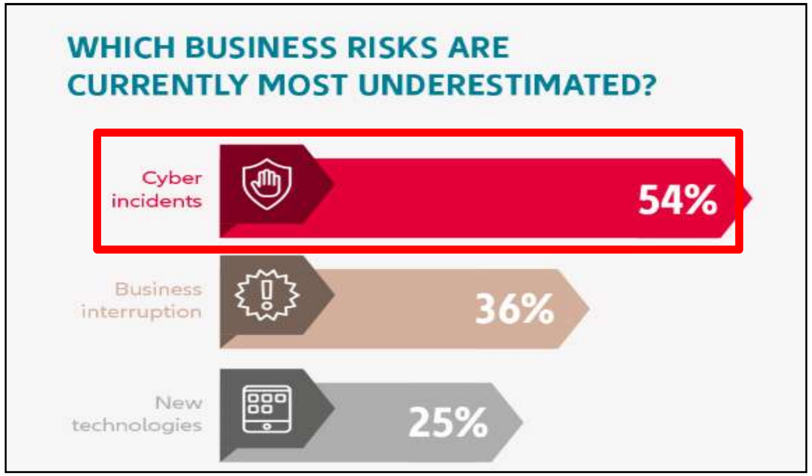
2 *Failure of climate-change mitigation and adaptation*

3 *Natural disasters*

4 *Data fraud or theft*

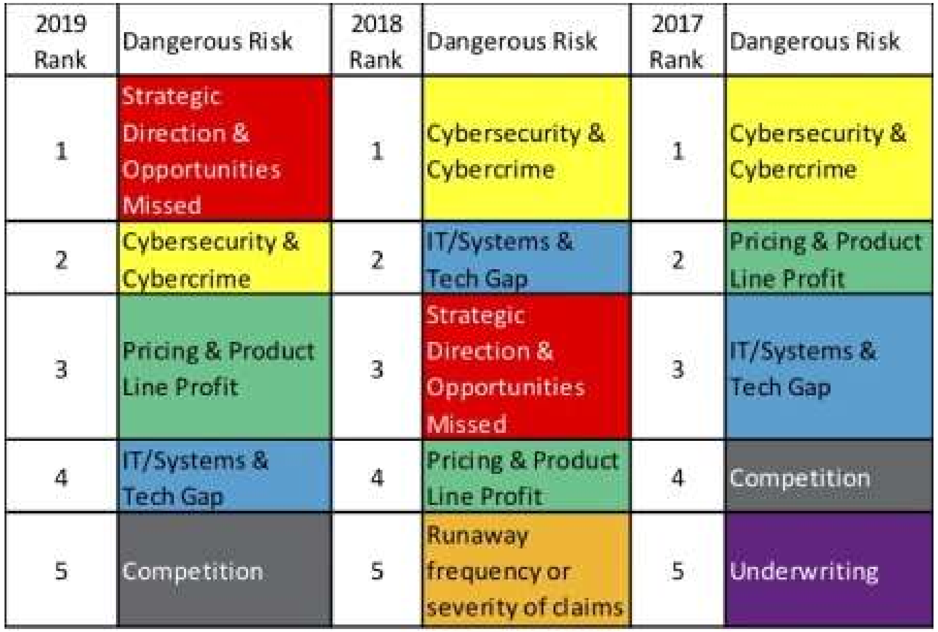
5 *Cyber-attacks*

Source : World Economic Forum – Global Risks Report 2019



Source : Allianz Global Corporate & Specialty

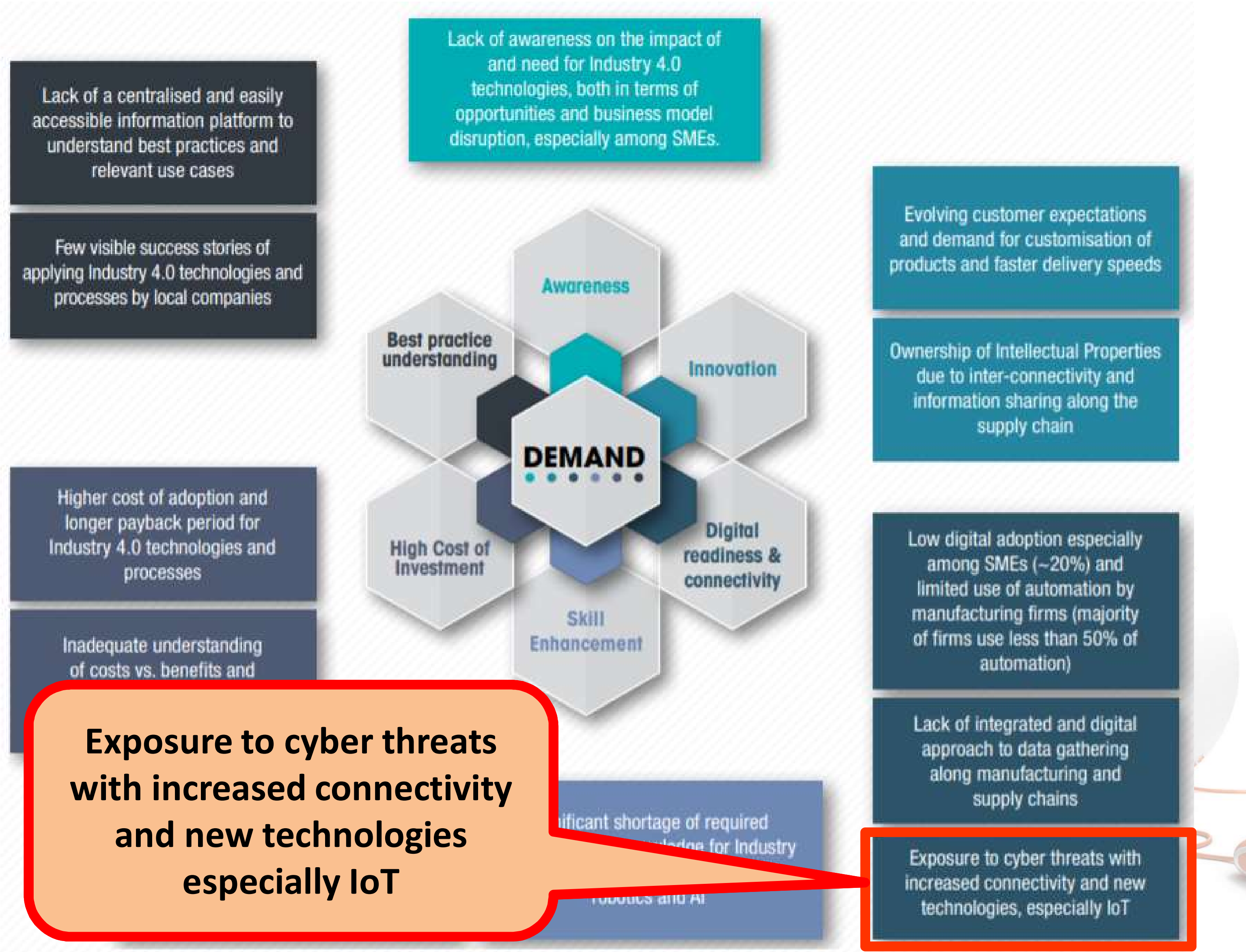
CYBER SECURITY REMAINS AMONG THE TOP 5 RISKS FOR 3 YEARS



2019 Rank	Dangerous Risk	2018 Rank	Dangerous Risk	2017 Rank	Dangerous Risk
1	Strategic Direction & Opportunities Missed	1	Cybersecurity & Cybercrime	1	Cybersecurity & Cybercrime
2	Cybersecurity & Cybercrime	2	IT/Systems & Tech Gap	2	Pricing & Product Line Profit
3	Pricing & Product Line Profit	3	Strategic Direction & Opportunities Missed	3	IT/Systems & Tech Gap
4	IT/Systems & Tech Gap	4	Pricing & Product Line Profit	4	Competition
5	Competition	5	Runaway frequency or severity of daims	5	Underwriting

Insurers' Survey 2019 Global Insights on Risk,
Enterprise Risk Management,
Willis Towers Watson Wire

MALAYSIA'S INDUSTRY 4.0 ISSUES & CHALLENGES



Lack of a centralised and easily accessible information platform to understand best practices and relevant use cases

Few visible success stories of applying Industry 4.0 technologies and processes by local companies

Lack of awareness on the impact of and need for Industry 4.0 technologies, both in terms of opportunities and business model disruption, especially among SMEs.

Evolving customer expectations and demand for customisation of products and faster delivery speeds

Ownership of Intellectual Properties due to inter-connectivity and information sharing along the supply chain

Higher cost of adoption and longer payback period for Industry 4.0 technologies and processes

Inadequate understanding of costs vs. benefits and

Low digital adoption especially among SMEs (~20%) and limited use of automation by manufacturing firms (majority of firms use less than 50% of automation)

Lack of integrated and digital approach to data gathering along manufacturing and supply chains

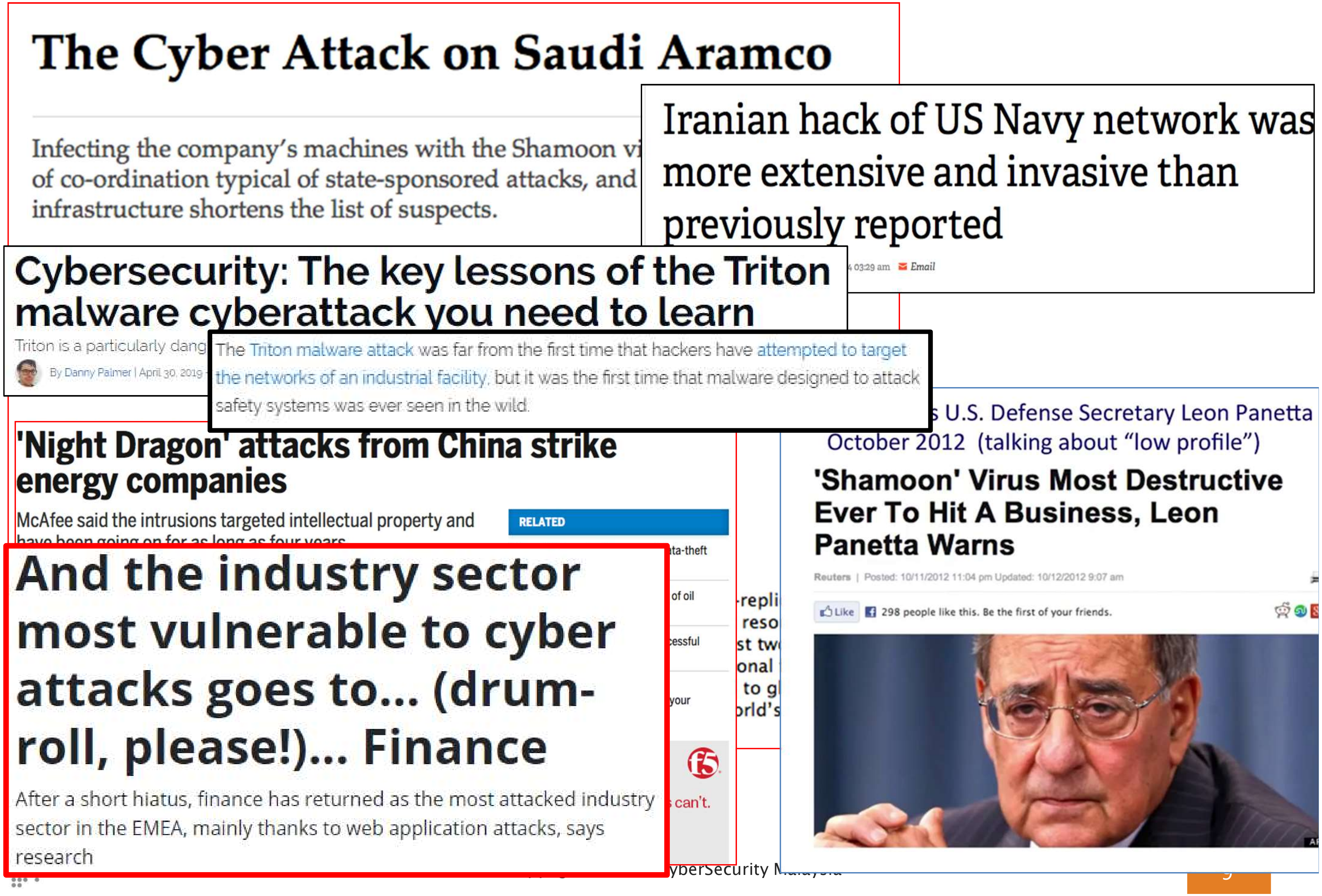
...ificant shortage of required ...wledge for Industry ... robotics and AI

Exposure to cyber threats with increased connectivity and new technologies, especially IoT

Exposure to cyber threats with increased connectivity and new technologies especially IoT

National Industry 4.0 Framework

RISING TREND OF CYBER ATTACKS ON INDUSTRIAL SECTORS



The Cyber Attack on Saudi Aramco

Infecting the company's machines with the Shamoon vi
of co-ordination typical of state-sponsored attacks, and
infrastructure shortens the list of suspects.

Iranian hack of US Navy network was more extensive and invasive than previously reported

4 03:29 am ✉ Email

Cybersecurity: The key lessons of the Triton malware cyberattack you need to learn

Triton is a particularly dang

By Danny Palmer | April 30, 2019

The Triton malware attack was far from the first time that hackers have attempted to target the networks of an industrial facility, but it was the first time that malware designed to attack safety systems was ever seen in the wild.

'Night Dragon' attacks from China strike energy companies

McAfee said the intrusions targeted intellectual property and have been going on for as long as four years

RELATED

ata-theft

of oil

essful

your

can't.

-repli
reso
st tw
onal
to gl
orld's

s U.S. Defense Secretary Leon Panetta
October 2012 (talking about "low profile")

'Shamoon' Virus Most Destructive Ever To Hit A Business, Leon Panetta Warns

Reuters | Posted: 10/11/2012 11:04 pm Updated: 10/12/2012 9:07 am

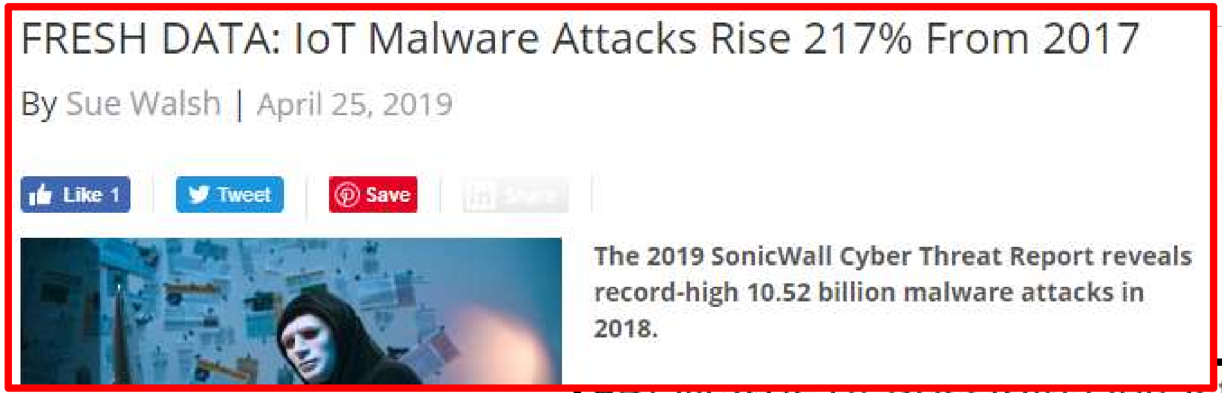
Like 298 people like this. Be the first of your friends.

And the industry sector most vulnerable to cyber attacks goes to… (drum-roll, please!)… Finance

After a short hiatus, finance has returned as the most attacked industry sector in the EMEA, mainly thanks to web application attacks, says research

MORE CONNECTED DEVICES INTRODUCE MORE VULNERABILITIES AND CYBER RISKS

Attacks on Internet of Things devices will increase rapidly due to hypergrowth in the number of connected objects, poor security hygiene, and the high value of data on IoT devices.

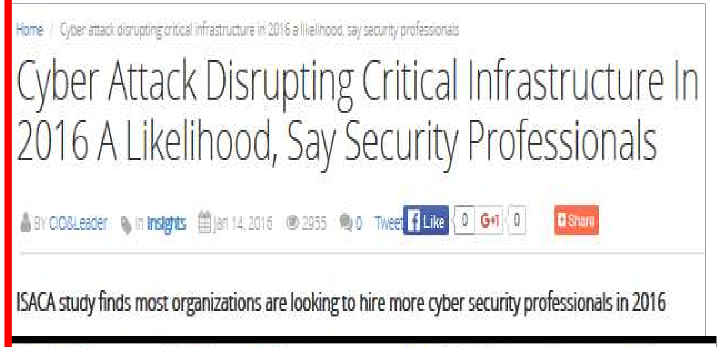


FRESH DATA: IoT Malware Attacks Rise 217% From 2017

By Sue Walsh | April 25, 2019

Like 1 Tweet Save Share

The 2019 SonicWall Cyber Threat Report reveals record-high 10.52 billion malware attacks in 2018.



Home / Cyber attack disrupting critical infrastructure in 2016 a likelihood, say security professionals

Cyber Attack Disrupting Critical Infrastructure In 2016 A Likelihood, Say Security Professionals

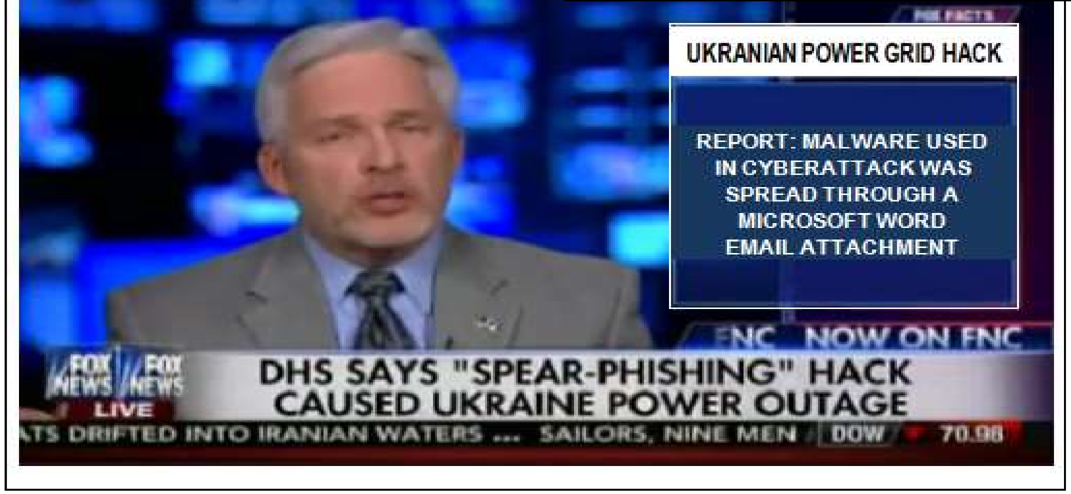
BY CIO&Leader In Insights Jan 14, 2016 2955 0 Tweet Like 0 G+1 0 Share

ISACA study finds most organizations are looking to hire more cyber security professionals in 2016

FBI Warns of Possible Devastating Attacks on IoT Networks

By Sue Walsh | August 22, 2018

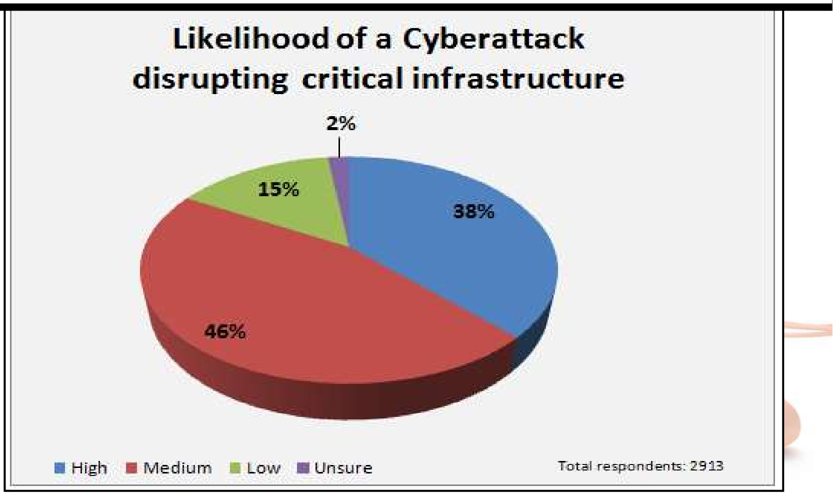
Fox News Channel - Happening



UKRANIAN POWER GRID HACK

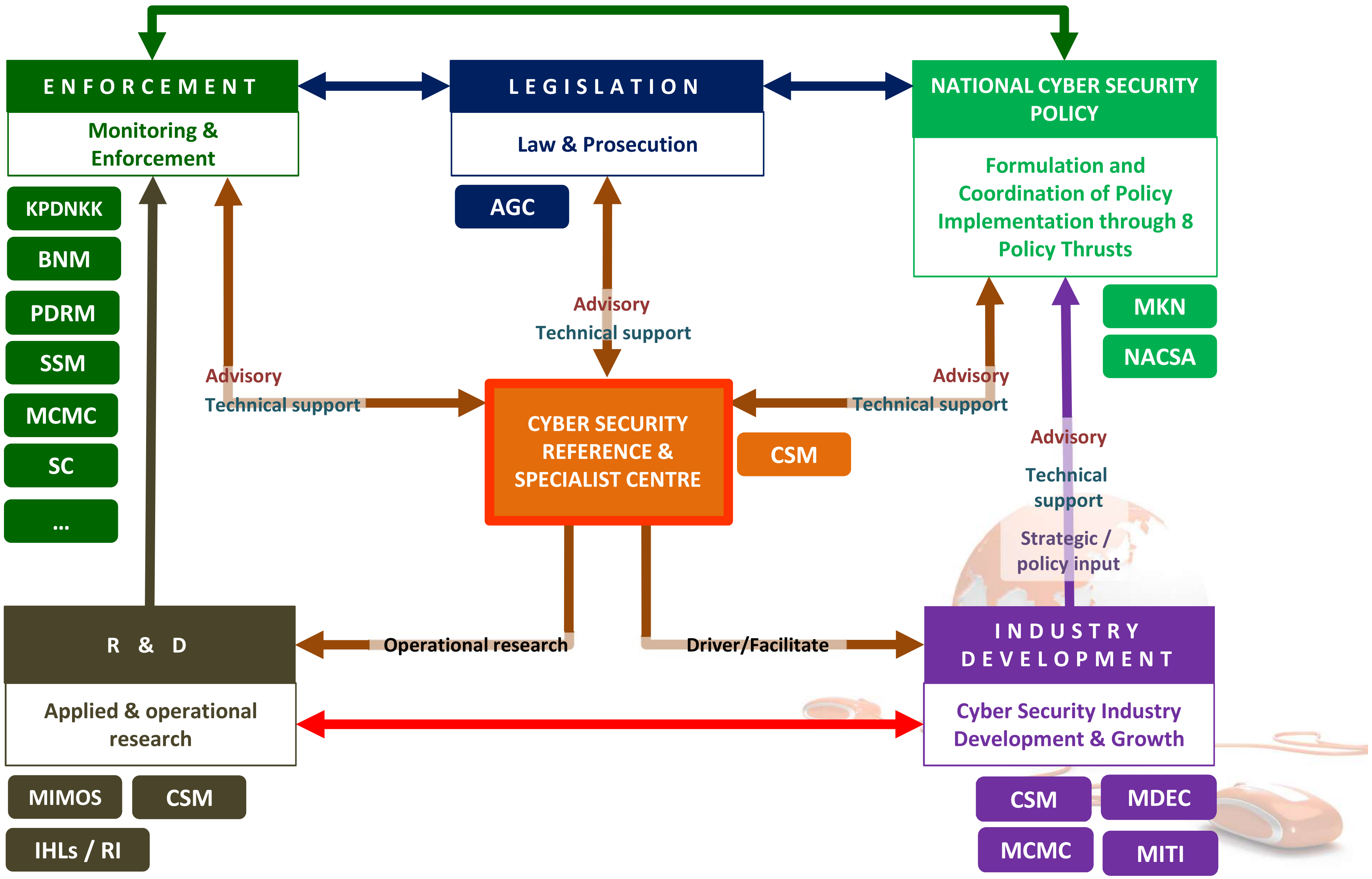
REPORT: MALWARE USED IN CYBERATTACK WAS SPREAD THROUGH A MICROSOFT WORD EMAIL ATTACHMENT

DHS SAYS "SPEAR-PHISHING" HACK CAUSED UKRAINE POWER OUTAGE



MALAYSIA’S CYBER SECURITY INITIATIVES

CYBER SECURITY ECOSYSTEM IN MALAYSIA

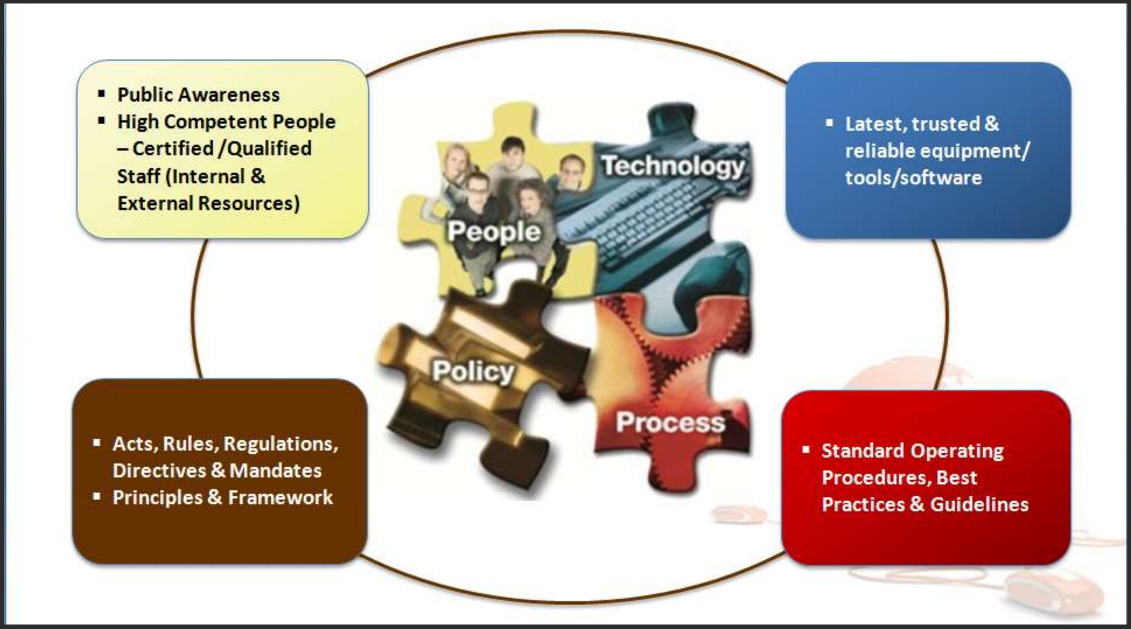


HOLISTIC APPROACH

- 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.**

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.



- Public Awareness
- High Competent People – Certified /Qualified Staff (Internal & External Resources)

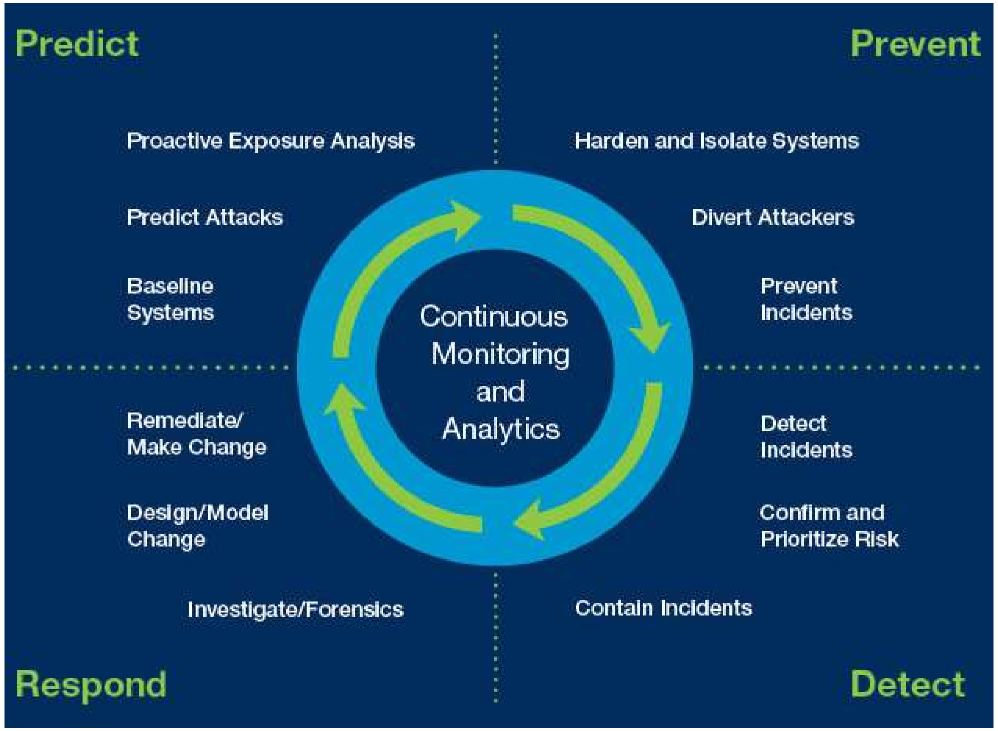
- Latest, trusted & reliable equipment/ tools/software

- Acts, Rules, Regulations, Directives & Mandates
- Principles & Framework

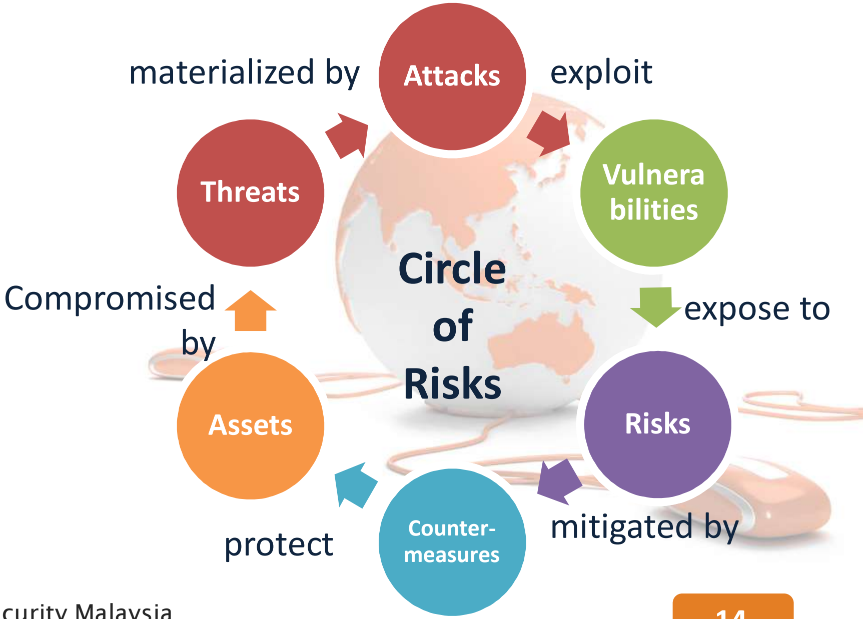
- Standard Operating Procedures, Best Practices & Guidelines

ENSURING CONTINUITY OF BUSINESS OPERATION via ADAPTIVE SECURITY

- **To be more proactive, dynamic and integrated in cyber security approach**

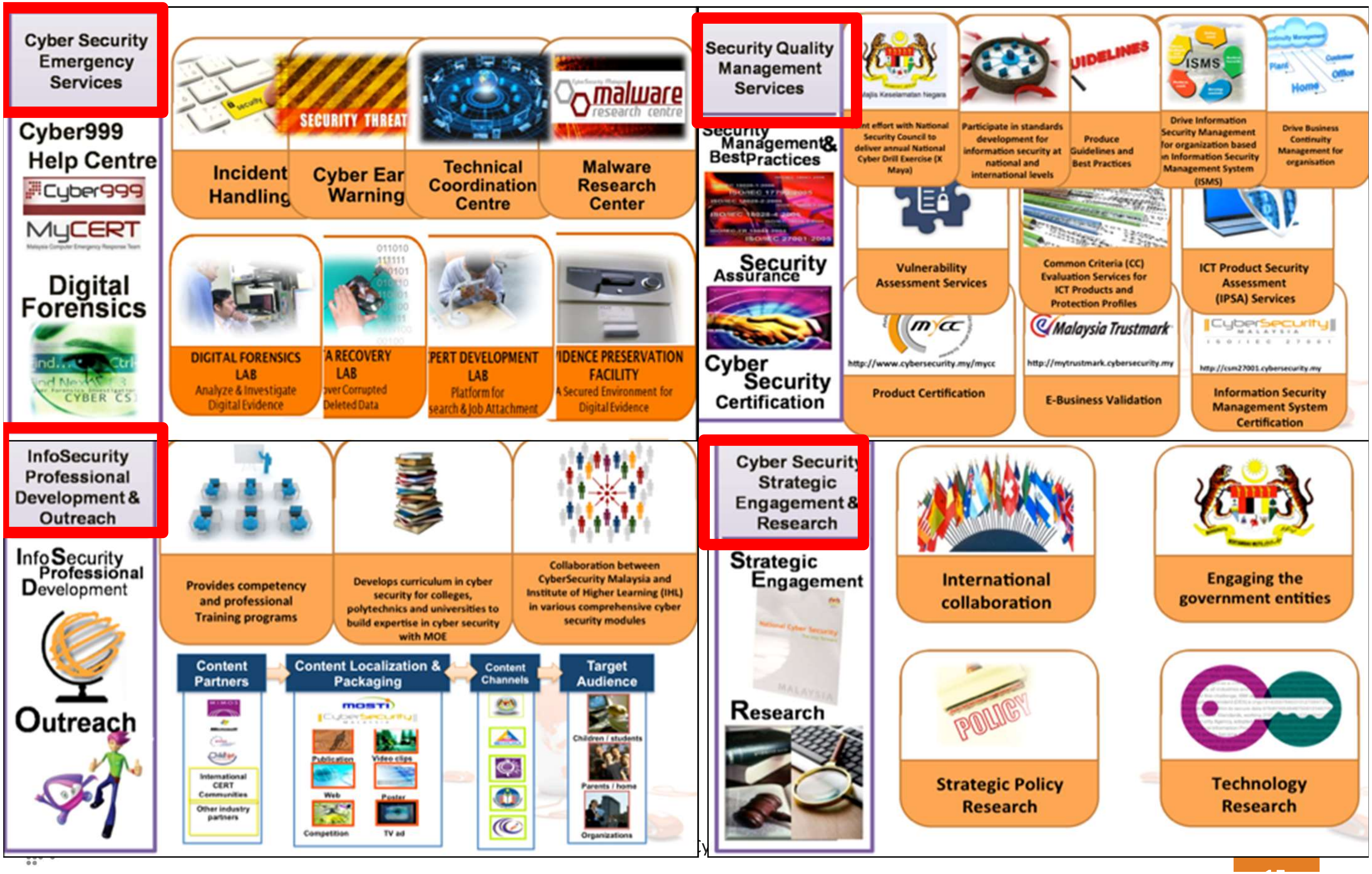


The cost to organizations comes at each stage of the incident response lifecycle — **detection, notification, responses, post-incidents**, and the **cost of business losses**.



MALAYSIA'S CYBER SECURITY SERVICES

- via Proactive and Responsive Services



Cyber Security Emergency Services

Cyber999 Help Centre

Cyber999

MyCERT

Digital Forensics

Incident Handling

Cyber Early Warning

Technical Coordination Centre

Malware Research Center

DIGITAL FORENSICS LAB
Analyze & Investigate Digital Evidence

DATA RECOVERY LAB
Recover Corrupted Deleted Data

EXPERT DEVELOPMENT LAB
Platform for Research & Job Attachment

EVIDENCE PRESERVATION FACILITY
A Secured Environment for Digital Evidence

Security Quality Management Services

Security Management & Best Practices

- Joint effort with National Security Council to deliver annual National Cyber Drill Exercise (X Maya)
- Participate in standards development for information security at national and international levels
- Produce Guidelines and Best Practices
- Drive Information Security Management for organization based on Information Security Management System (ISMS)
- Drive Business Continuity Management for organisation

Security Assurance

- Vulnerability Assessment Services
- Common Criteria (CC) Evaluation Services for ICT Products and Protection Profiles
- ICT Product Security Assessment (IPSA) Services

Cyber Security Certification

- Product Certification — http://www.cybersecurity.my/mycc
- E-Business Validation — http://mytrustmark.cybersecurity.my
- Information Security Management System Certification — http://csm27001.cybersecurity.my

InfoSecurity Professional Development & Outreach

InfoSecurity Professional Development

- Provides competency and professional Training programs
- Develops curriculum in cyber security for colleges, polytechnics and universities to build expertise in cyber security with MOE
- Collaboration between CyberSecurity Malaysia and Institute of Higher Learning (IHL) in various comprehensive cyber security modules

Outreach

Content Partners → Content Localization & Packaging ↔ Content Channels → Target Audience

Content Partners: International CERT Communities; Other industry partners

Content Localization & Packaging: Publication; Video clips; Web; Poster; Competition; TV ad

Target Audience: Children / students; Parents / home; Organizations

Cyber Security Strategic Engagement & Research

Strategic Engagement

- International collaboration
- Engaging the government entities

Research

- Strategic Policy Research
- Technology Research

POLICY

MALAYSIA'S CYBER DEFENCE INITIATIVES - NATIONAL CYBER SECURITY POLICY (NCSP)

Vision

"Malaysia's CNII shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation"

Critical National Information Infrastructure (CNII)

Thrust 1: Effective Governance

Thrust 2: Legislative & Regulatory Framework

Thrust 3: Cyber Security Technology Framework

Thrust 4: Culture of Security & Capacity Building

Thrust 5: R&D Towards Self Reliance

Thrust 6: Compliance & Enforcement

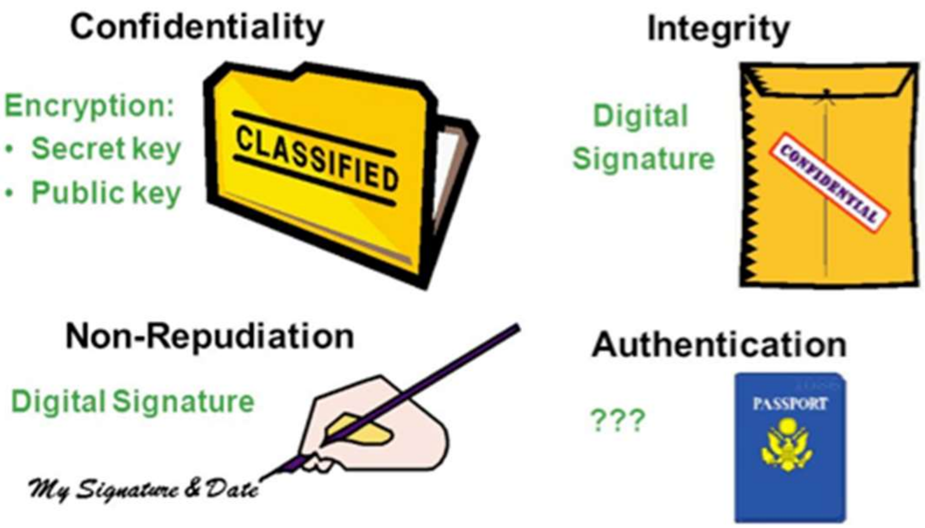
Thrust 7: Cyber Security Emergency Readiness

Thrust 8: International Cooperation

ADDRESSING FUNDAMENTAL ASPECTS OF CYBER SECURITY
- In Machine-Machine Environment

National Cryptography Policy 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

Encryption:
- Secret key
- Public key

Integrity

Digital Signature

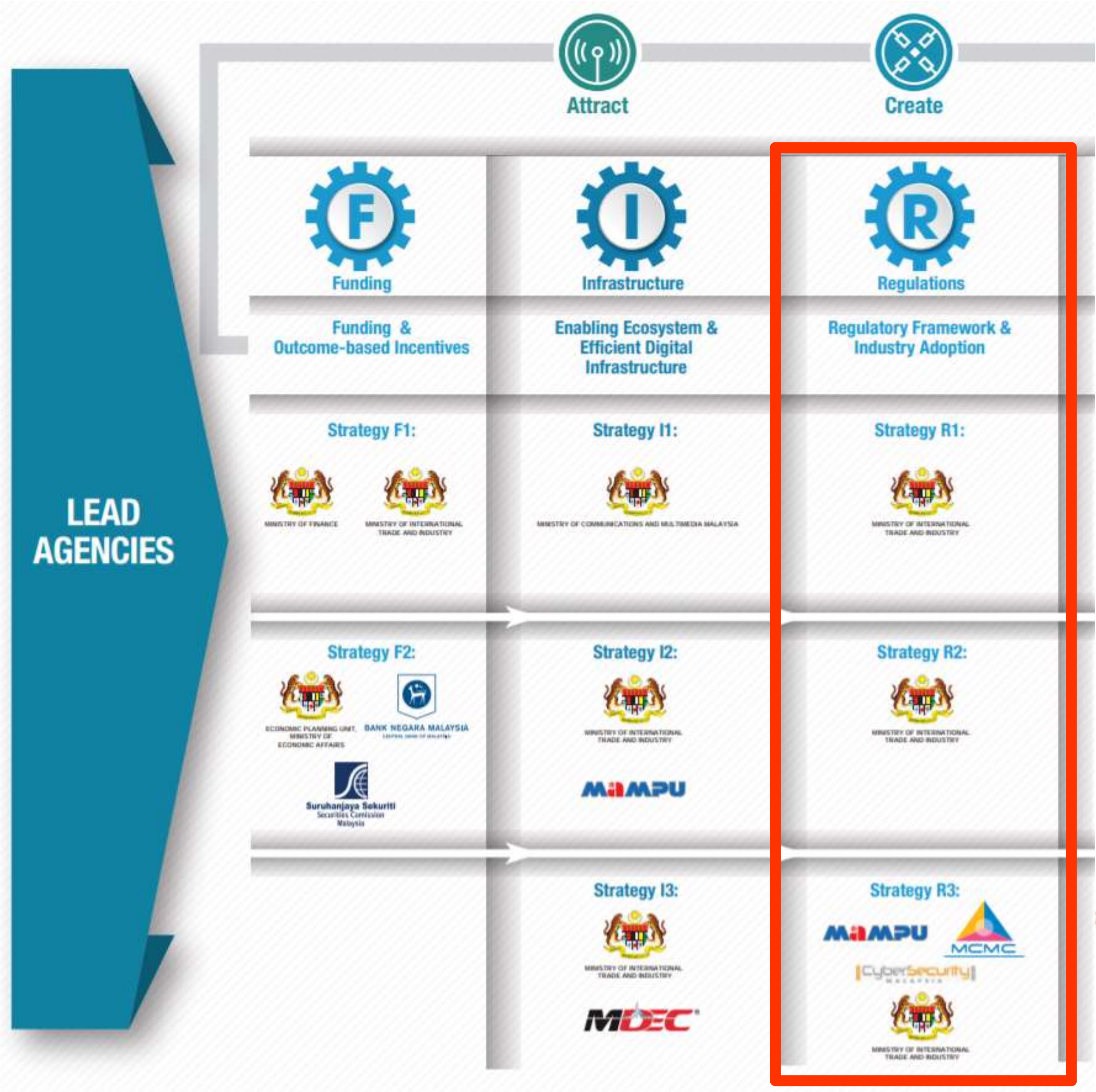
Non-Repudiation

Digital Signature

Authentication

???

CYBERSECURITY AMONG THE KEY ENABLERS OF IR 4.0


Attract
Create
LEAD AGENCIES
F
Funding
I
Infrastructure
R
Regulations
Funding & Outcome-based Incentives
Enabling Ecosystem & Efficient Digital Infrastructure
Regulatory Framework & Industry Adoption
Strategy F1:
MINISTRY OF FINANCE
MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY
Strategy I1:
MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA
Strategy R1:
MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY
Strategy F2:
ECONOMIC PLANNING UNIT, MINISTRY OF ECONOMIC AFFAIRS
BANK NEGARA MALAYSIA
Suruhanjaya Sekuriti Securities Commission Malaysia
Strategy I2:
MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY
MAMPU
Strategy R2:
MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY
Strategy I3:
MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY
MDEC
Strategy R3:
MAMPU
MCMC
CyberSecurity MALAYSIA
MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY

These enabling technologies bring a new dimension to the industrial environment, resulting in a dramatic increase in industrial productivity.

INTEGRATION & AUTOMATION

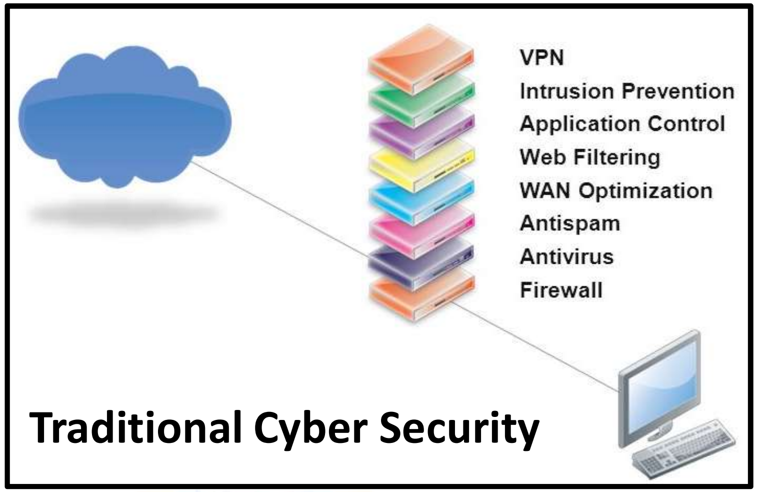
The manufacturing systems would become fully integrated and automated as a result of digital adoption that will transform the industrial environment.

STRATEGY R3:

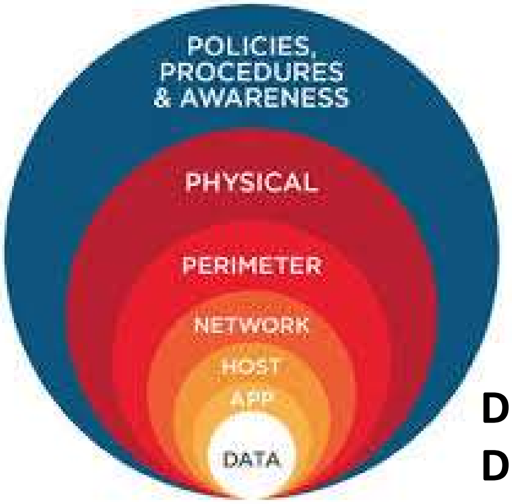
Improve data integrity, standards, sharing security to facilitate seamless integration of value chains and support intra-ministerial analysis to chart effective Industry 4.0 programs

TECHNOLOGY

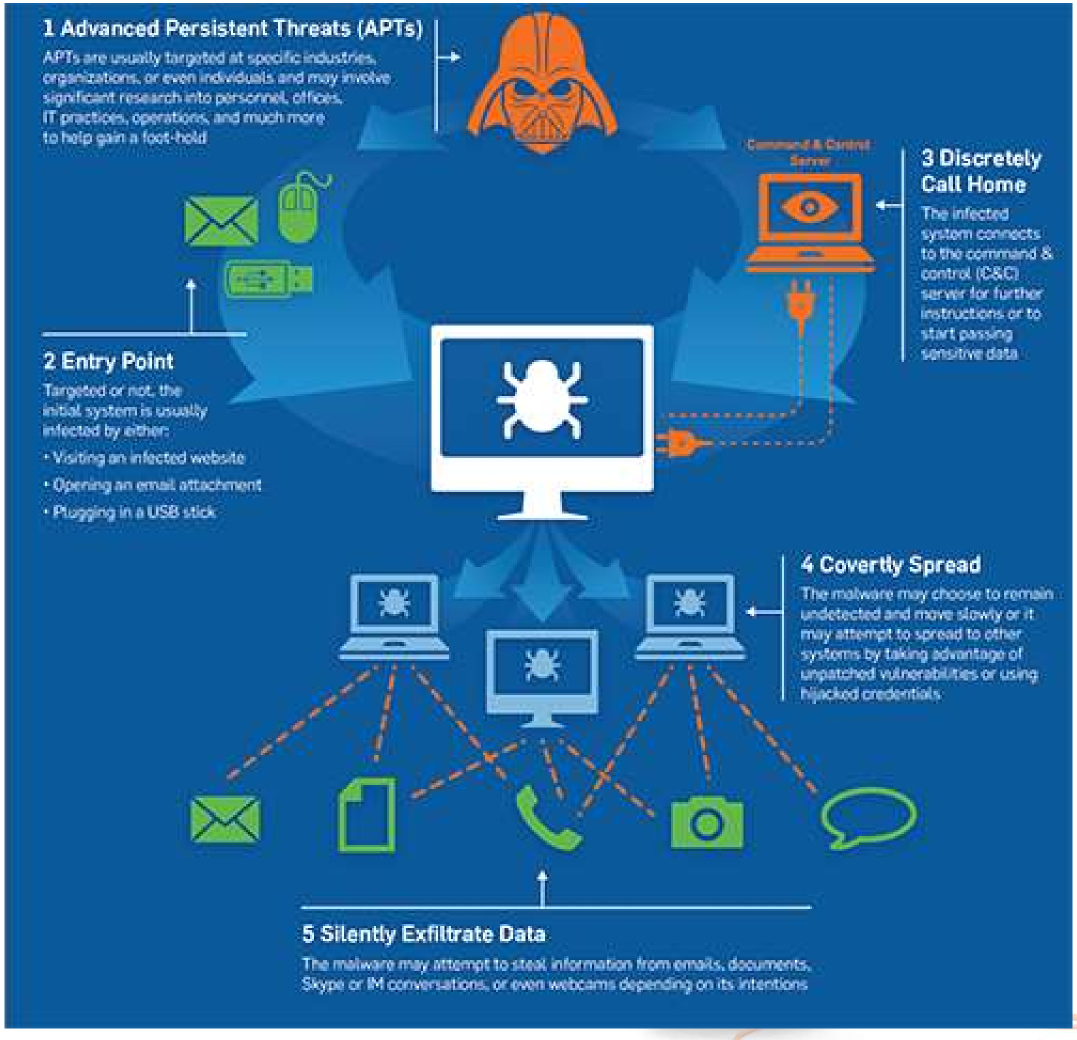
TRADITIONAL CYBER SECURITY APPROACH
- Not sufficient to deal with smart cyber threats



Traditional Cyber Security



Defense in Depth



1 Advanced Persistent Threats (APTs)

APTs are usually targeted at specific industries, organizations, or even individuals and may involve significant research into personnel, offices, IT practices, operations, and much more to help gain a foot-hold

2 Entry Point

Targeted or not, the initial system is usually infected by either:

- Visiting an infected website
- Opening an email attachment
- Plugging in a USB stick

3 Discretely Call Home

The infected system connects to the command & control (C&C) server for further instructions or to start passing sensitive data

4 Covertly Spread

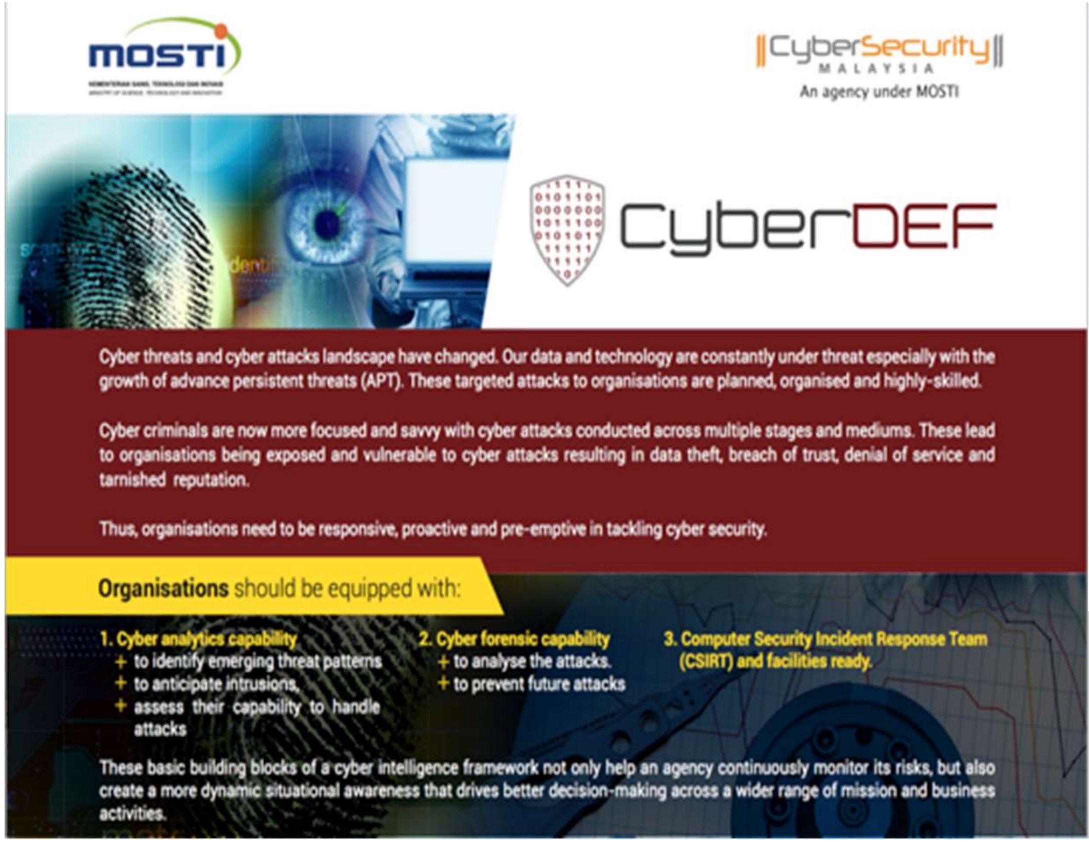
The malware may choose to remain undetected and move slowly or it may attempt to spread to other systems by taking advantage of unpatched vulnerabilities or using hijacked credentials

5 Silently Exfiltrate Data

The malware may attempt to steal information from emails, documents, Skype or IM conversations, or even webcams depending on its intentions

Traditional detection is not sufficient as most actions depend heavily on signatures and known patterns - **NOT effective to detect unique custom malware & new breed of cyber attacks**

STRENGTHENING DETECTIVE CAPABILITIES THROUGH: CyberDEF: FIRE EYE BEST CYBERSECURITY INNOVATION AWARD 2015



MOSTI

CyberSecurity MALAYSIA
An agency under MOSTI

CyberDEF

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.

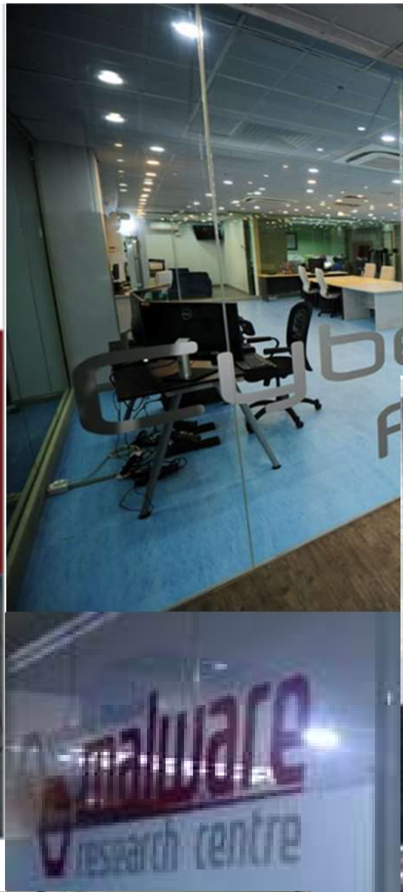
Cyber criminals are now more focused and savvy with cyber attacks conducted across multiple stages and mediums. These lead to organisations being exposed and vulnerable to cyber attacks resulting in data theft, breach of trust, denial of service and tarnished reputation.

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.

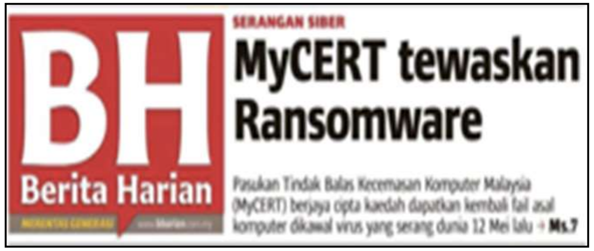


CyberD.E.F

- **Detection**
- **Eradication**
- **Forensic**

CYBERDEF SATELLITE PROJECT

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



BH Berita Harian

SERANGAN SIBER

MyCERT tewaskan Ransomware

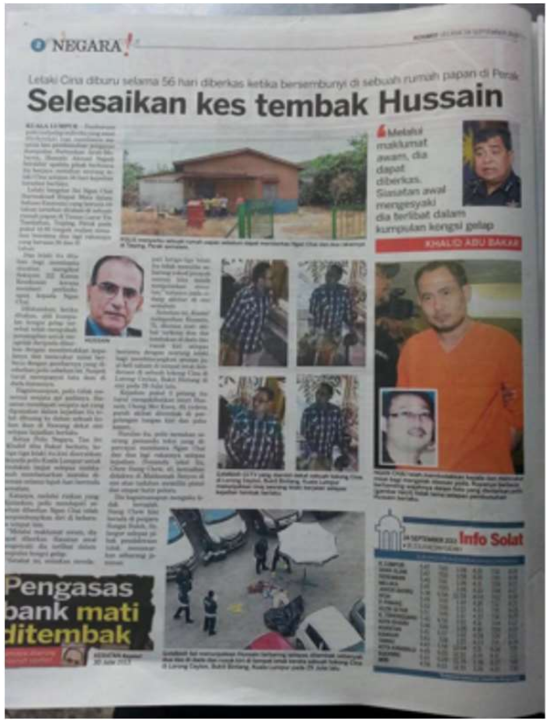
Pasukan Tindak Balas Kecemasan Komputer Malaysia (MyCERT) berjaya cipta kaedah dapatkan kembali fail asal komputer dikawal virus yang serang dunia 12 Mei lalu → Ms.7

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.

2D/3D BIOMETIC FACIAL RECOGNITION TO ASSIST LAW ENFORCEMENT

- CAMMUKA was launched 12 December 2017 in conjunction with Malaysia Commercialization Year Summit 2017.

- CamMuka is a facial recognition technology system built using the expertise of CyberSecurity Malaysia's research and development conducted by the Digital Forensics Department in Biometric Technology.



NEGARA!

Lelaki Cina diburu selama 56 hari diberkas ketika bersembunyi di sebuah rumah papan di Perak

Selesaikan kes tembak Hussain

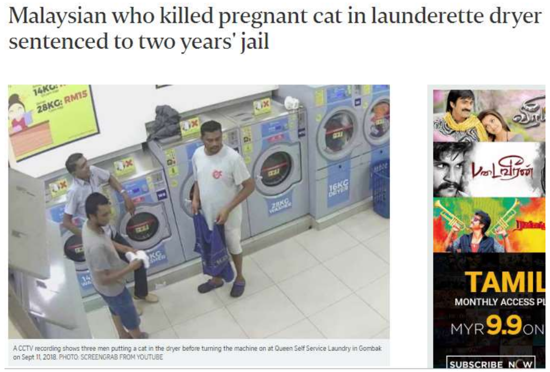
[illegible]

"Melalui maklumat awam, dia dapat diberkas. Siasatan awal mengesyaki dia terlibat dalam kumpulan kongsi gelap

KHALID ABU BAKAR

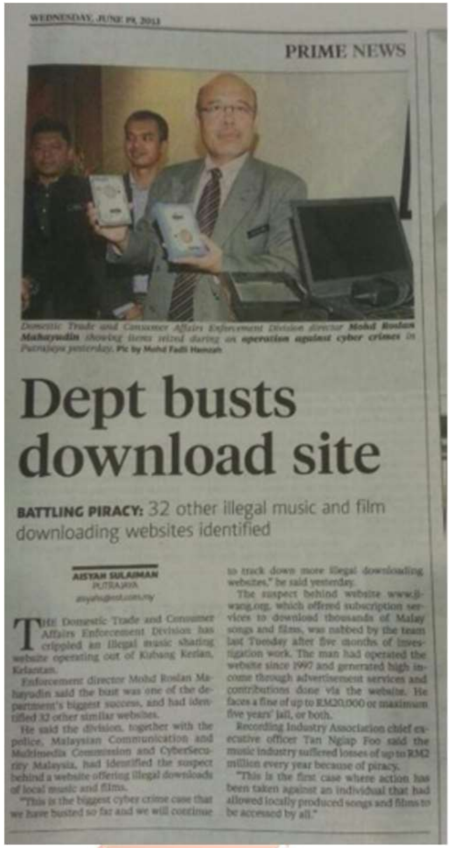
Pengasas bank mati ditembak

Info Solat



Malaysian who killed pregnant cat in launderette dryer sentenced to two years' jail

A CCTV recording shows three men putting a cat in the dryer before turning the machine on at Queen Self Service Laundry in Gombak on Sept 11, 2018. PHOTO: SCREENGRAB FROM YOUTUBE



WEDNESDAY, JUNE 19, 2013

PRIME NEWS

Domestic Trade and Consumer Affairs Enforcement Division director **Mohd Roslan Mahayudin** showing items seized during an **operation against cyber crimes** in Putrajaya yesterday. **Pic by Mohd Fadli Hamzah**

Dept busts download site

BATTLING PIRACY: 32 other illegal music and film downloading websites identified

AISYAH SULAIMAN
PUTRAJAYA
aisyahs@nst.com.my

THE Domestic Trade and Consumer Affairs Enforcement Division has crippled an illegal music sharing website operating out of Kubang Kerian, Kelantan.

Enforcement director Mohd Roslan Mahayudin said the bust was one of the department's biggest success, and had identified 32 other similar websites.

He said the division, together with the police, Malaysian Communication and Multimedia Commission and CyberSecurity Malaysia, had identified the suspect behind a website offering illegal downloads of local music and films.

"This is the biggest cyber crime case that we have busted so far and we will continue to track down more illegal downloading websites," he said yesterday.

The suspect behind website www.ji-wang.org, which offered subscription services to download thousands of Malay songs and films, was nabbed by the team last Tuesday after five months of investigation work. The man had operated the website since 1997 and generated high income through advertisement services and contributions done via the website. He faces a fine of up to RM20,000 or maximum five years' jail, or both.

Recording Industry Association chief executive officer Tan Ngiap Foo said the music industry suffered losses of up to RM2 million every year because of piracy.

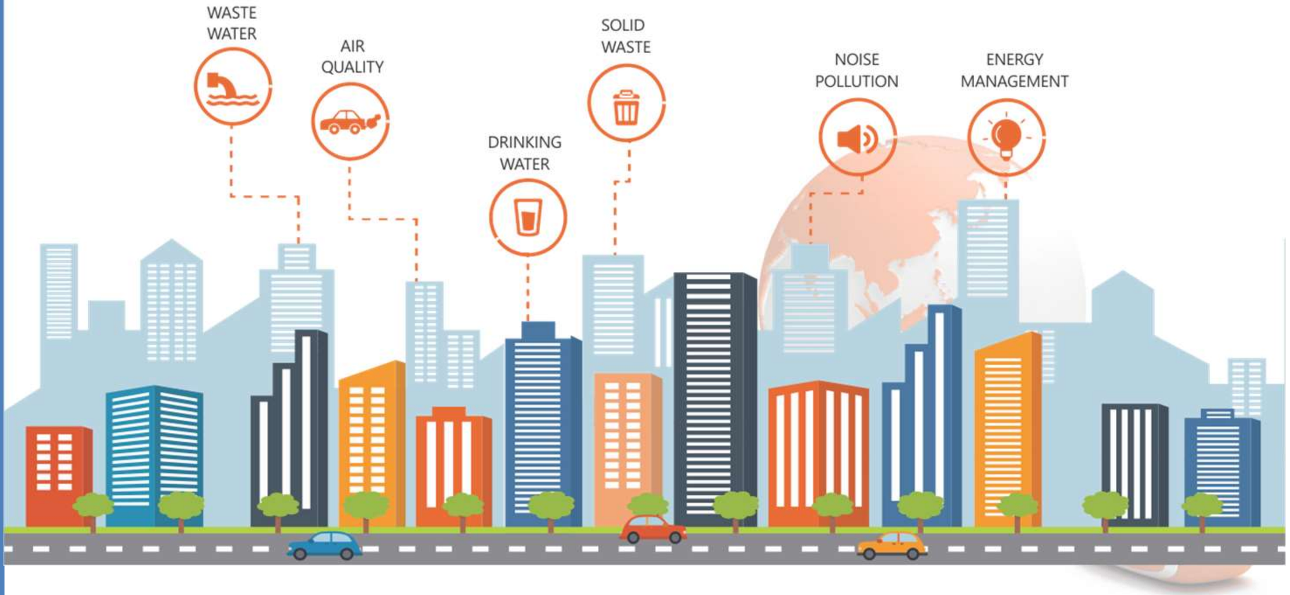
"This is the first case where action has been taken against an individual that had allowed locally produced songs and films to be accessed by all."

CASE STUDIES: 2D/3D BIOMETIC FACIAL RECOGNITION TO ASSIST LAW ENFORCEMENT

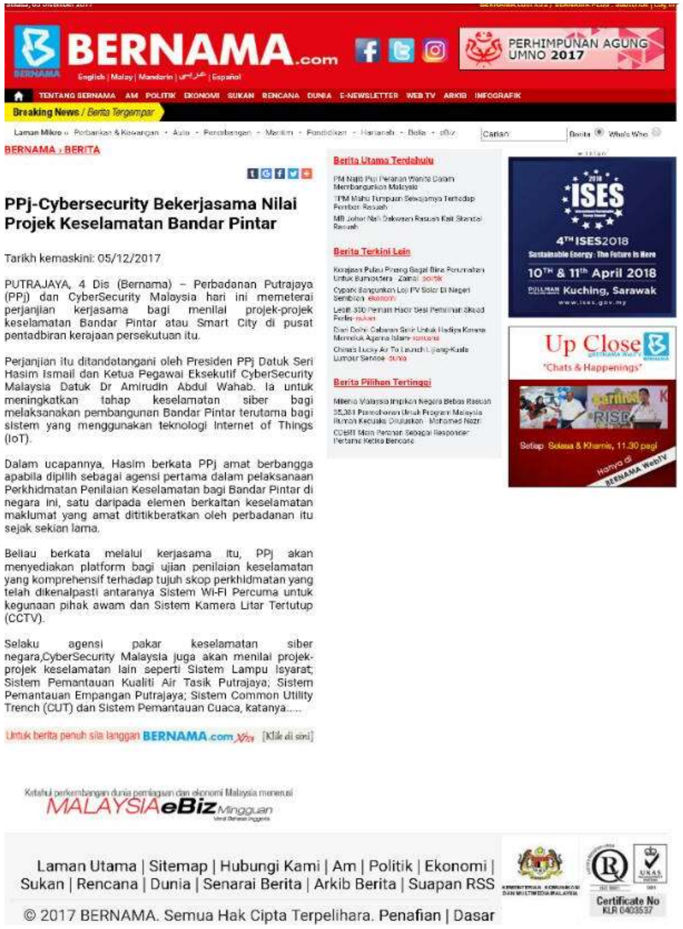
CyberSecurity Malaysia Roles Regarding Smart Cities

Vulnerability Assessment And Penetration Testing (VAPT) services on:

- Perbadanan Putrajaya (PPJ) covers on Smart City Security Testing
- Universiti Kebangsaan Malaysia Medical Centre (UKMMC) covers on Medical Devices Security Testing



PERBADANAN PUTRAJAYA FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING ON SMART CITY



BERNAMA.com
English | Malay | Mandarin | عربي | Español
PERHIMPUNAN AGUNG UMNO 2017
TENTANG BERNAMA AM POLITIK EKONOMI SUKAN RENCANA DUNIA E-NEWSLETTER WEB TV ARKIB INFOGRAFIK
Breaking News / Berita Tergempar
Laman Mikro » Perbankan & Kewangan • Auto • Perdagangan • Maritim • Pendidikan • Hartanah • Belia • eBiz
Carian: Berita ● Who's Who ○
BERNAMA › BERITA

PPj-Cybersecurity Bekerjasama Nilai Projek Keselamatan Bandar Pintar

Tarikh kemaskini: 05/12/2017

PUTRAJAYA, 4 Dis (Bernama) -- Perbadanan Putrajaya (PPj) dan CyberSecurity Malaysia hari ini memeterai perjanjian kerjasama bagi menilai projek-projek keselamatan Bandar Pintar atau Smart City di pusat pentadbiran kerajaan persekutuan itu.

Perjanjian itu ditandatangani oleh Presiden PPj Datuk Seri Hasim Ismail dan Ketua Pegawai Eksekutif CyberSecurity Malaysia Datuk Dr Amirudin Abdul Wahab. Ia untuk meningkatkan tahap keselamatan siber bagi melaksanakan pembangunan Bandar Pintar terutama bagi sistem yang menggunakan teknologi Internet of Things (IoT).

Dalam ucapannya, Hasim berkata PPj amat berbangga apabila dipilih sebagai agensi pertama dalam pelaksanaan Perkhidmatan Penilaian Keselamatan bagi Bandar Pintar di negara ini, satu daripada elemen berkaitan keselamatan maklumat yang amat dititikberatkan oleh perbadanan itu sejak sekian lama.

Beliau berkata melalui kerjasama itu, PPj akan menyediakan platform bagi ujian penilaian keselamatan yang komprehensif terhadap tujuh skop perkhidmatan yang telah dikenalpasti antaranya Sistem Wi-Fi Percuma untuk kegunaan pihak awam dan Sistem Kamera Litar Tertutup (CCTV).

Selaku agensi pakar keselamatan siber negara,CyberSecurity Malaysia juga akan menilai projek-projek keselamatan lain seperti Sistem Lampu Isyarat; Sistem Pemantauan Kualiti Air Tasik Putrajaya; Sistem Pemantauan Empangan Putrajaya; Sistem Common Utility Trench (CUT) dan Sistem Pemantauan Cuaca, katanya.....

Untuk berita penuh sila langgan BERNAMA.com Xtra [Klik di sini]

Berita Utama Terdahulu

PM Najib Puji Peranan Wanita Dalam Membangunkan Malaysia

TPM Mahu Tumpuan Sewajarnya Terhadap Pemberi Rasuah

MB Johor Nafi Dakwaan Rasuah Kait Skandal Rasuah

Berita Terkini Lain

Kerajaan Pulau Pinang Gagal Bina Perumahan Untuk Bumiputera - Zainal politik

Cypark Bangunkan Loji PV Solar Di Negeri Sembilan ekonomi

Lebih 300 Pemain Hadir Sesi Pemilihan Skuad Perlis sukan

Dian Dolhi Cabaran Sebir Untuk Hadiya Kerana Memeluk Agama Islam rencana

China's Lucky Air To Launch Lijiang-Kuala Lumpur Service dunia

Berita Pilihan Tertinggi

Milenio Malaysia Impikan Negara Bebas Rasuah

35,381 Permohonan Untuk Program Malaysia Rumah Kediaman Diluluskan - Mohamed Nazri

CDERT Main Peranan Sebagai Responder Pertama Ketika Bencana

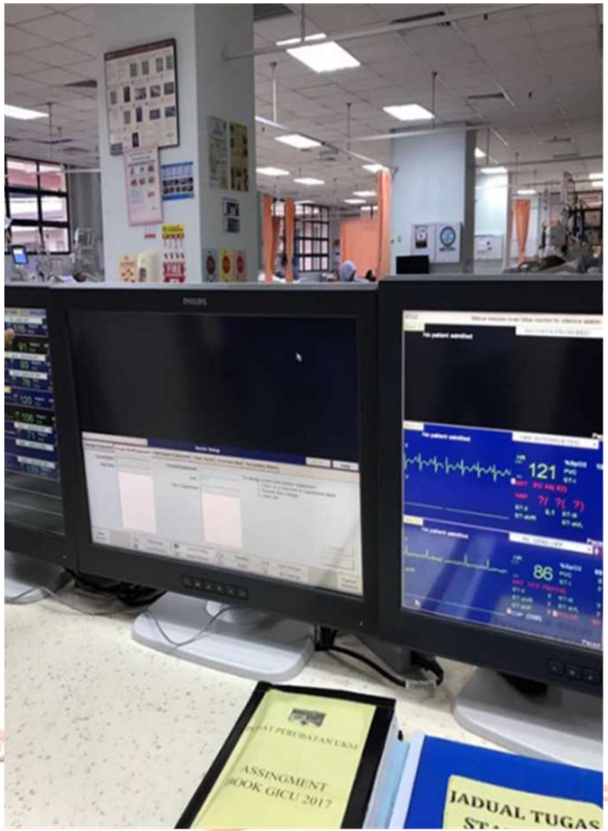
Laman Utama | Sitemap | Hubungi Kami | Am | Politik | Ekonomi | Sukan | Rencana | Dunia | Senarai Berita | Arkib Berita | Suapan RSS

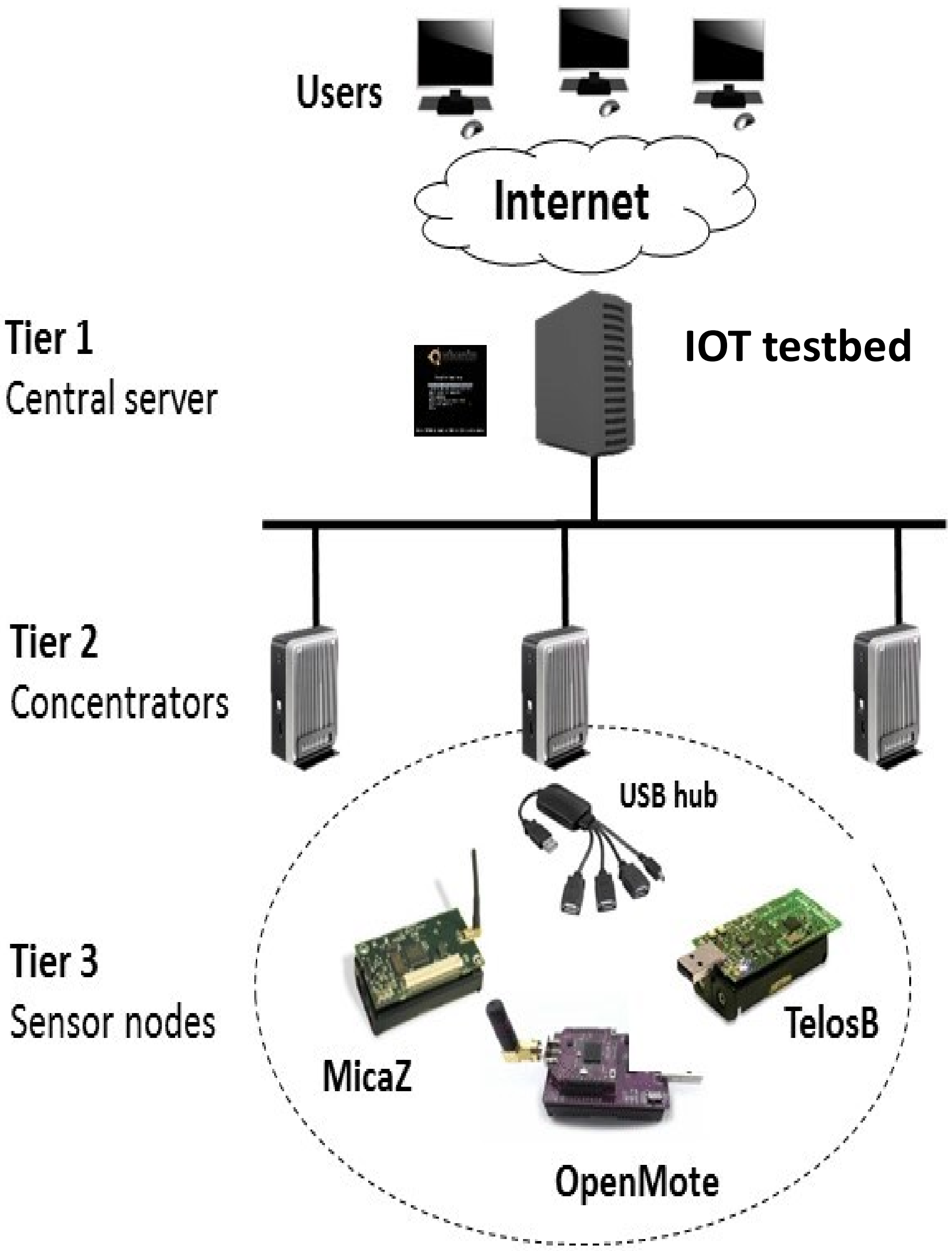
Certificate No KLR 0403537

SELAMAT DATANG KE PERBADANAN PUTRAJAYA
Welcome to Perbadanan Putrajaya

VULNERABILITY ASSESSMENT AND PENETRATION TESTING SERVICES

UNIVERSITI KEBANGSAAN MALAYSIA MEDICAL CENTER (UKMMC)





IOT SECURITY LABORATORY

CyberSecurity Malaysia recognizes the importance of having vulnerability assessment laboratories for critical information systems and technologies. The laboratory (test bed) will conduct assessments, identify common and potential vulnerabilities and investigate mitigation approaches.

IoT Security laboratory where vulnerabilities are simulated and hardening steps tested.

PARTNERSHIP IN CYBERSECURITY R&D ACTIVITIES

- **Staying Ahead Through Innovative & Effective Capacity Building Programs**

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

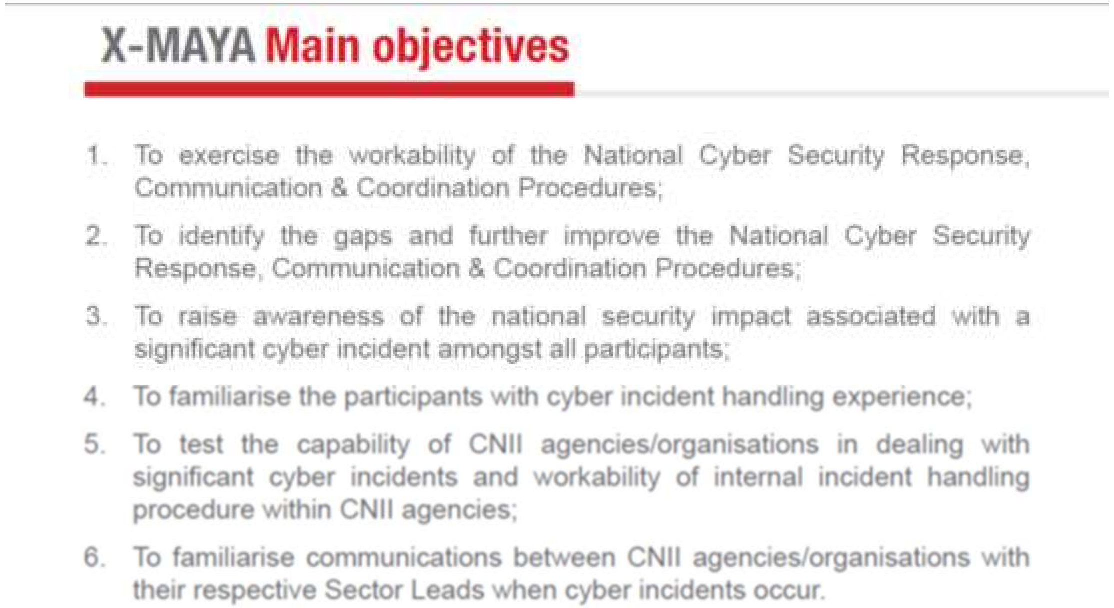
UNIMAS
UNIVERSITI TENAGA NASIONAL
UNIVERSITI KUALA LUMPUR
UNIVERSITI TEKNOLOGI MALAYSIA
UNIVERSITI UTARA MALAYSIA
CyberSecurity MALAYSIA
An agency under MOSTI
of Defence
FAMO
NICTA
UNICAM
CyberSecurity MALAYSIA
An agency under MOSTI

PROCESS

CYBER SECURITY EMERGENCY READINESS

- National Cyber Drill (X-Maya)

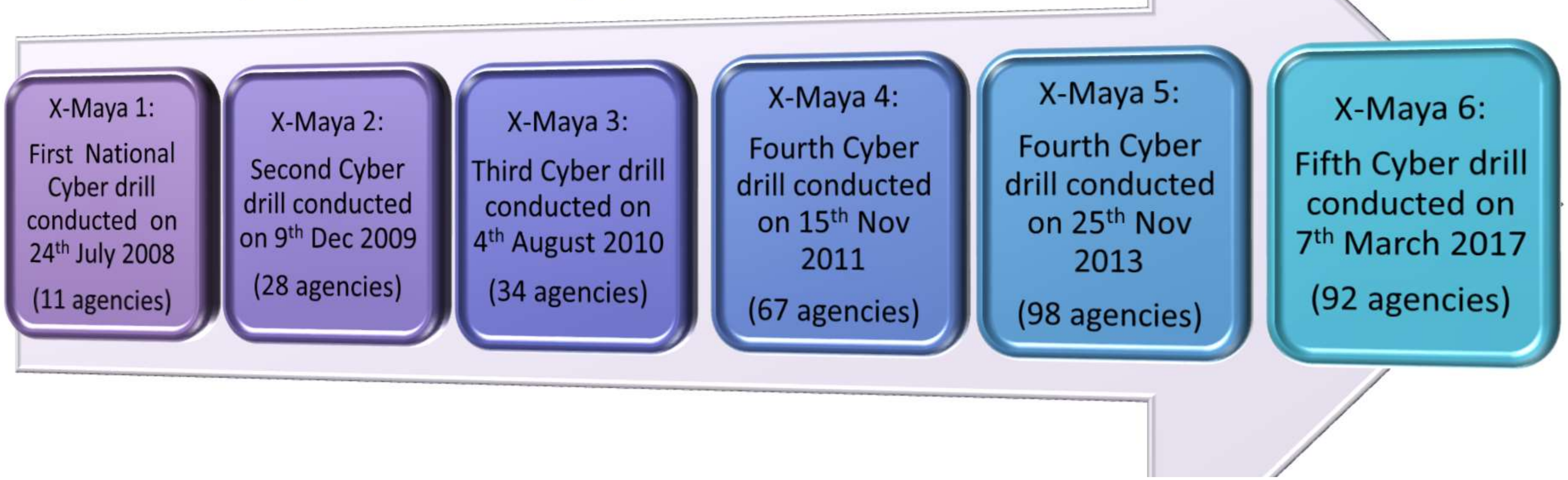
NATIONAL CYBER CRISIS DRILL (X-MAYA)



X-MAYA Main objectives

1. To exercise the workability of the National Cyber Security Response, Communication & Coordination Procedures;
2. To identify the gaps and further improve the National Cyber Security Response, Communication & Coordination Procedures;
3. To raise awareness of the national security impact associated with a significant cyber incident amongst all participants;
4. To familiarise the participants with cyber incident handling experience;
5. To test the capability of CNII agencies/organisations in dealing with significant cyber incidents and workability of internal incident handling procedure within CNII agencies;
6. To familiarise communications between CNII agencies/organisations with their respective Sector Leads when cyber incidents occur.

The National Cyber Crisis Exercise will simulate a large-scale cyber attack involving participating CNII agencies/ organisations and CNII Sector Leads



X-Maya 1: First National Cyber drill conducted on 24th July 2008 (11 agencies)

X-Maya 2: Second Cyber drill conducted on 9th Dec 2009 (28 agencies)

X-Maya 3: Third Cyber drill conducted on 4th August 2010 (34 agencies)

X-Maya 4: Fourth Cyber drill conducted on 15th Nov 2011 (67 agencies)

X-Maya 5: Fourth Cyber drill conducted on 25th Nov 2013 (98 agencies)

X-Maya 6: Fifth Cyber drill conducted on 7th March 2017 (92 agencies)

COMPLYING TO INTERNATIONAL STANDARD & PROCESSES:

- Common Criteria ISO/IEC 15048 , ISMS ISO/IEC 27001, IS0 17025 etc

CyberSecurity Malaysia Malaysian Security Evaluation Facility (MySEF)

ISO 17025

ACCREDITED LABORATORY

MALAYSIAN STANDARD MS ISO/IEC 17799:2005

INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT (FIRST REVISION) (ISO/IEC 17799:2005, IDT)

© Copyright 2005

DEPARTMENT OF STANDARDS MALAYSIA

ISO 27001:2013

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 17799:2007

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

Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme
Certified • Recognised • Assured
MSC
Malaysian Common Criteria Evaluation & Certification Scheme
myCC

csm-ace 2019
11th CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

PARTNERSHIP PROCESS AT THE DOMESTIC LEVEL

Cyber Security Malaysia – Awards, Conference & Exhibition (CSM-ACE) is a public-private-academia partnership driven event

To act as a **catalyst** in driving innovation and **growth** for the cyber security industry.

To inculcate **cyber security culture** and **awareness** at national level.

To gather **industry experts and communities** on the latest cyber security trends

To showcase **trade and investment opportunities** by assisting and allowing industry players to promote their products and services.

csm-ace 2019
11th CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

CSM-ACE 2019

CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION (CSM-ACE) 2019

23 - 27 September 2019 | Kuala Lumpur, Malaysia http://www.csm-ace.my/

The biggest cyber security industry event in Malaysia and the only 4-in-1 cyber security event in the region.

A public-private-partnership driven event and a knowledge sharing platform that recognizes contribution of individuals and organizations in the field of cyber security.

ASIA TOP 5 CONFERENCE

/Source : https://infosec-conferences.com/events/cybersecurity-conferences-asia

MALAYSIA CYBER SECURITY AWARDS 2018
- 7 Cyber Security Award

OPENING & KEYNOTE
- 4 Keynotes Session

CYBER COLLOQUIUM
- Collaboration Program with Universities

SATELITE EVENT
- NICTSED 2019
- Various Event by Partners

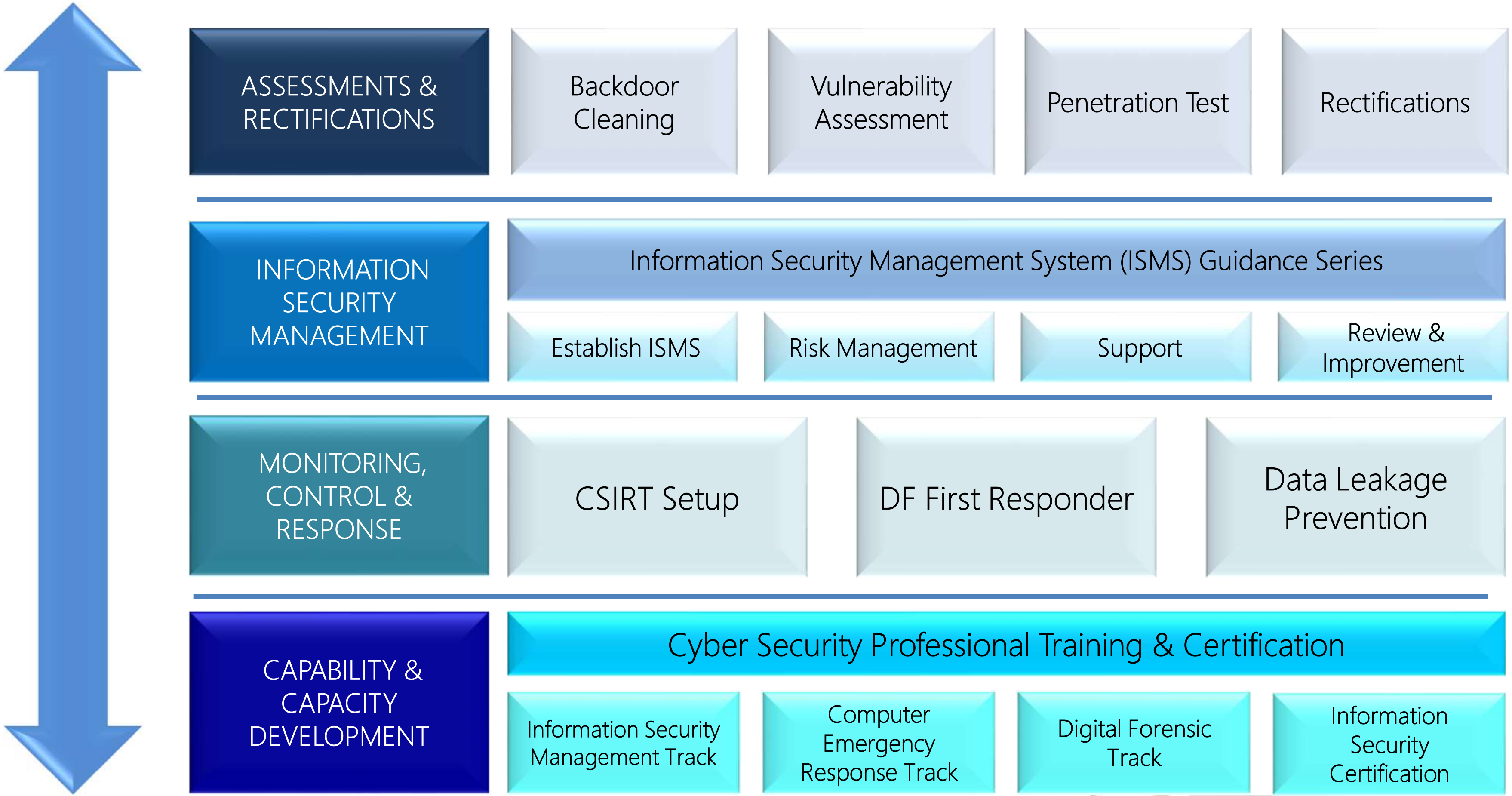
GLOBAL ACE CERTIFIED TRAINING PROGRAMS
- 9 Certified Professional Training
- HRDF Claimable

IT SECURITY EXHIBITION
- More than 40 Exhibitors
- 3 Days Exhibitions
- Business Matching

BUSINESS OPPORTUNITIES
- Tech Talk Seminar by Partners
- B2B Session
- Networking Event

CONFERENCE
- Management & Technical Track
- International Speakers
- Talking Slot Opportunities

CYBERSECURITY MALAYSIA STRUCTURED SERVICES

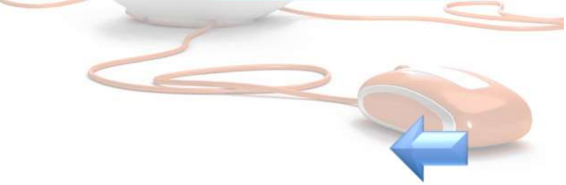


ASSESSMENTS & RECTIFICATIONS
- Backdoor Cleaning
- Vulnerability Assessment
- Penetration Test
- Rectifications

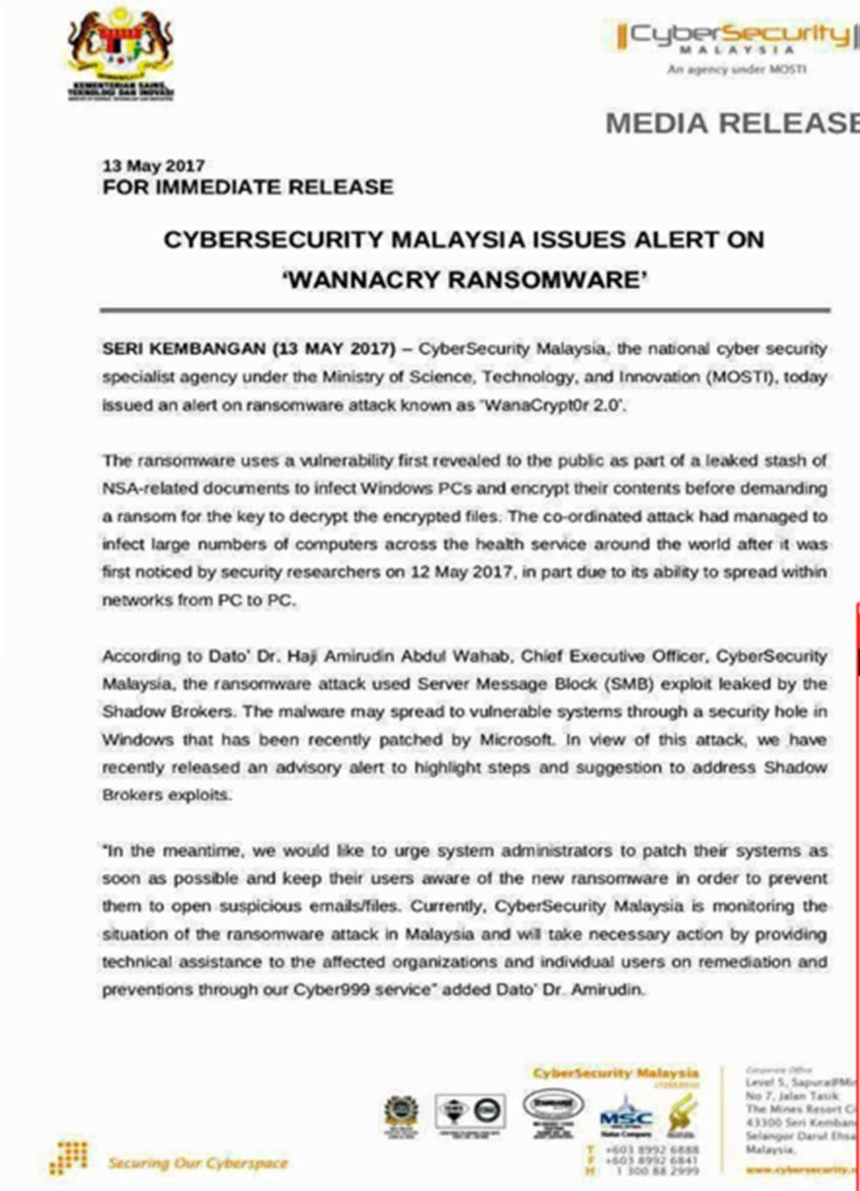
INFORMATION SECURITY MANAGEMENT
- Information Security Management System (ISMS) Guidance Series
- Establish ISMS
- Risk Management
- Support
- Review & Improvement

MONITORING, CONTROL & RESPONSE
- CSIRT Setup
- DF First Responder
- Data Leakage Prevention

CAPABILITY & CAPACITY DEVELOPMENT
- Cyber Security Professional Training & Certification
- Information Security Management Track
- Computer Emergency Response Track
- Digital Forensic Track
- Information Security Certification



PROCESS: INFORMATION SHARING IN COMBATING CYBER CRIME
- Minimizing Risks of Cyber Attacks



CyberSecurity MALAYSIA
An agency under MOSTI

MEDIA RELEASE

13 May 2017
FOR IMMEDIATE RELEASE

CYBERSECURITY MALAYSIA ISSUES ALERT ON 'WANNACRY RANSOMWARE'

SERI KEMBANGAN (13 MAY 2017) – CyberSecurity Malaysia, the national cyber security specialist agency under the Ministry of Science, Technology, and Innovation (MOSTI), today issued an alert on ransomware attack known as 'WanaCrypt0r 2.0'.

The ransomware uses a vulnerability first revealed to the public as part of a leaked stash of NSA-related documents to infect Windows PCs and encrypt their contents before demanding a ransom for the key to decrypt the encrypted files. The co-ordinated attack had managed to infect large numbers of computers across the health service around the world after it was first noticed by security researchers on 12 May 2017, in part due to its ability to spread within networks from PC to PC.

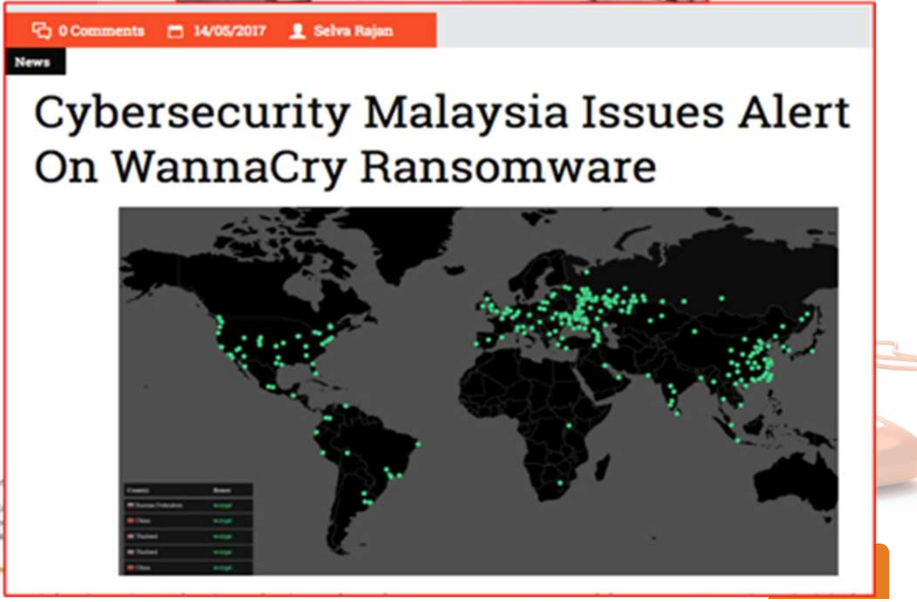
According to Dato' Dr. Haji Amirudin Abdul Wahab, Chief Executive Officer, CyberSecurity Malaysia, the ransomware attack used Server Message Block (SMB) exploit leaked by the Shadow Brokers. The malware may spread to vulnerable systems through a security hole in Windows that has been recently patched by Microsoft. In view of this attack, we have recently released an advisory alert to highlight steps and suggestion to address Shadow Brokers exploits.

"In the meantime, we would like to urge system administrators to patch their systems as soon as possible and keep their users aware of the new ransomware in order to prevent them to open suspicious emails/files. Currently, CyberSecurity Malaysia is monitoring the situation of the ransomware attack in Malaysia and will take necessary action by providing technical assistance to the affected organizations and individual users on remediation and preventions through our Cyber999 service" added Dato' Dr. Amirudin.

Securing Our Cyberspace

CyberSecurity Malaysia
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office
Level 5, Sapura@Mi
No 7, Jalan Tasik
The Mines Resort C
43300 Seri Kemban
Selangor Darul Ehsa
Malaysia.
www.cybersecurity.



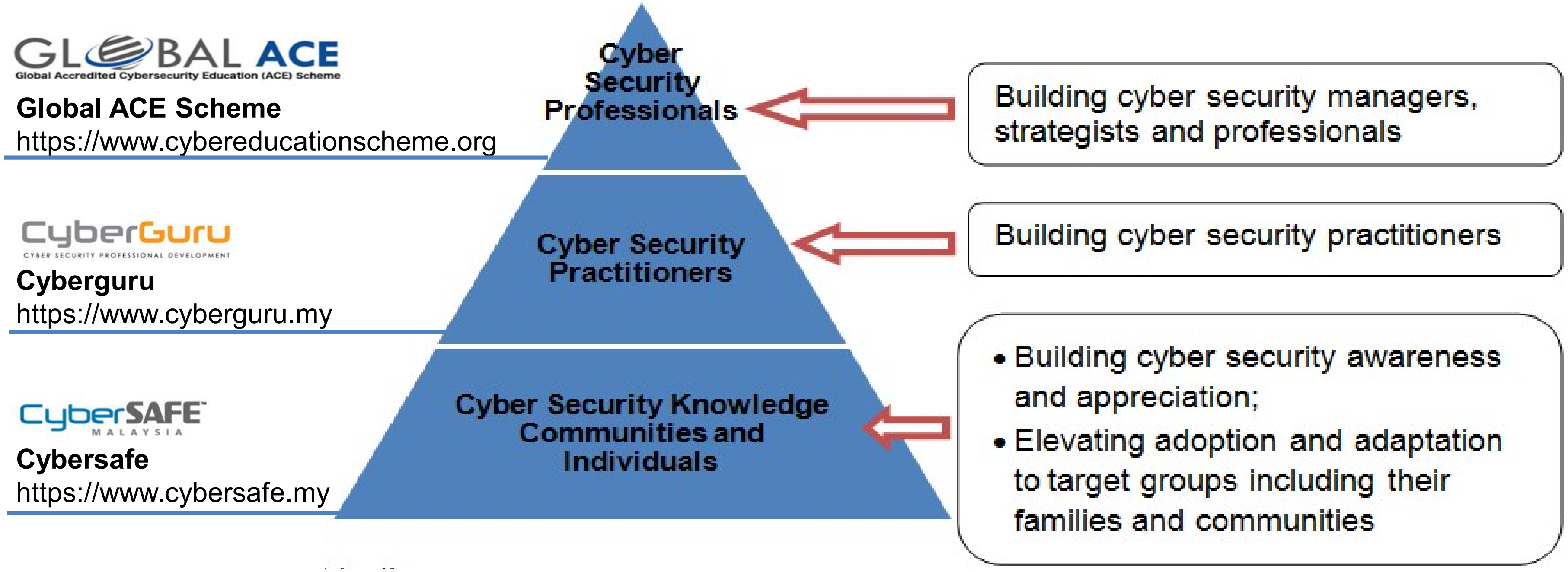
0 Comments 14/05/2017 Selva Rajan

News

Cybersecurity Malaysia Issues Alert On WannaCry Ransomware

PEOPLE

CYBER SECURITY CAPACITY BUILDING FRAMEWORK



GLOBAL ACE
Global Accredited Cybersecurity Education (ACE) Scheme

Global ACE Scheme
https://www.cybereducationscheme.org

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

Cyberguru
https://www.cyberguru.my

CyberSAFE
MALAYSIA

Cybersafe
https://www.cybersafe.my

Cyber Security Professionals
Cyber Security Practitioners
Cyber Security Knowledge Communities and Individuals

Building cyber security managers, strategists and professionals

Building cyber security practitioners

- Building cyber security awareness and appreciation;
- Elevating adoption and adaptation to target groups including their families and communities

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 initiatives

GLOBAL ACE SCHEME GOAL & OBJECTIVES

CyberSecurity MALAYSIA

GOAL

To create world class competent work-force in cyber security and promote the development of cyber security professional programmes within the region

OBJECTIVES

1 To establish a professional certification programme that is recognized globally

2 To provide cyber security professionals with the right knowledge, skills, attitude (KSA) and experience

3 To promote the development of cyber security certified programmes globally

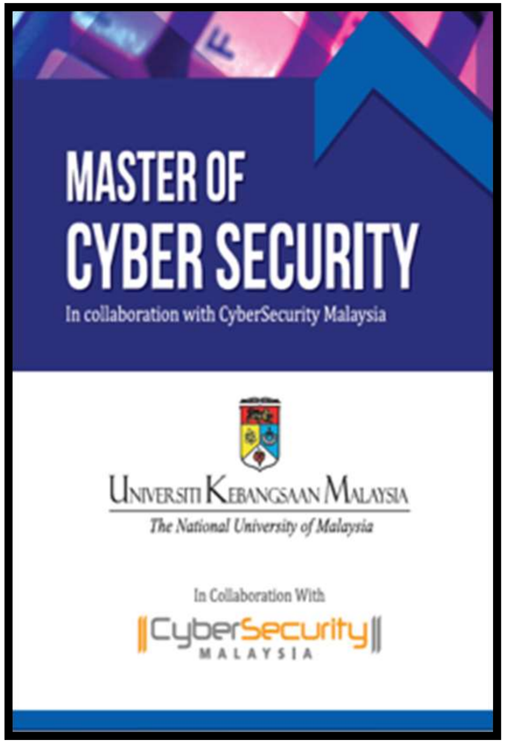
4 To ensure accredited personnel has been independently assessed, committed to a consistent and high quality service level

A large-scale systematic plan of actions & arrangements to **establish the certification plans** for **Cyber Security Professional** in collaboration with **government agencies, industry partners and Higher Learning Institutions (IHLs)**

The Scheme is developed in tandem with international standards of **ISO/IEC 9000 on processes**, **ISO/IEC 17024 on people certifications** and **ISO/IEC 27001 on security management**

PARTNERSHIP IN PRODUCING MORE CYBER SECURITY TALENTS WITH THE LOCAL UNIVERSITIES – EDUCATION PROGRAM

- Universities & Higher Learning Institutions
  - The National University of Malaysia
  - Ministry of Education
    - Department of Polytechnic Education
    - Department Of Community College Education
  - International Islamic University Malaysia (IIUM)
  - Universiti Tunku Abdul Rahman (UTAR)
  - University of Kuala Lumpur (UniKL)
  - University Putra Malaysia (UPM)
  - Multimedia University (MMU)
  - University Teknikal Malaysia Melaka (UTeM) etc



MASTER OF CYBER SECURITY

In collaboration with CyberSecurity Malaysia

UNIVERSITI KEBANGSAAN MALAYSIA

The National University of Malaysia

In Collaboration With

CyberSecurity MALAYSIA

CyberGuru

CYBER SECURITY PROFESSIONAL DEVELOPMENT

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

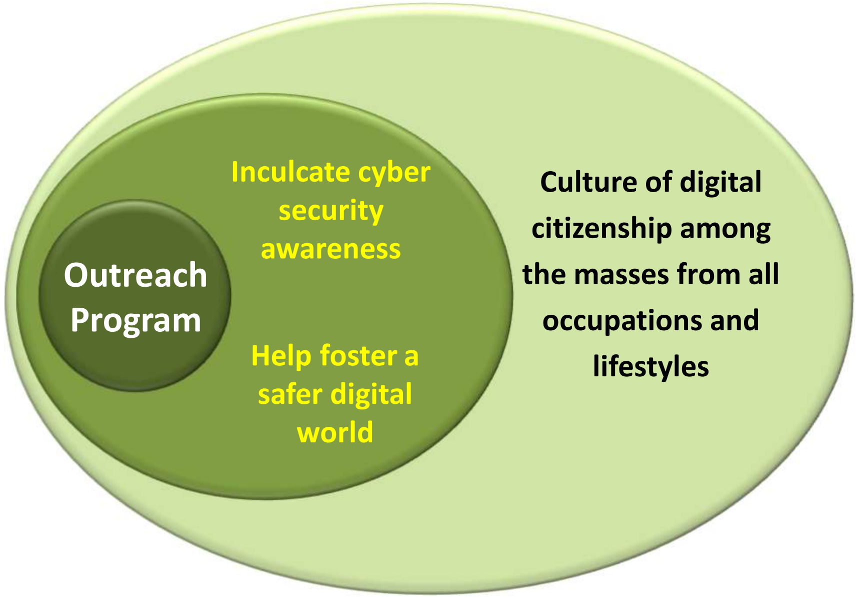
CyberSAFE
Cyber Security Awareness For Everyone

OUTREACH

CyberSecurity MALAYSIA

- **CyberSAFE** launched **YAB Deputy Prime Minister**
- Reached out to more than **34,000** students, teachers, adults and more than **190** schools / organisations
- Awareness program referred to by **Australian Communications** and **Media Authority**

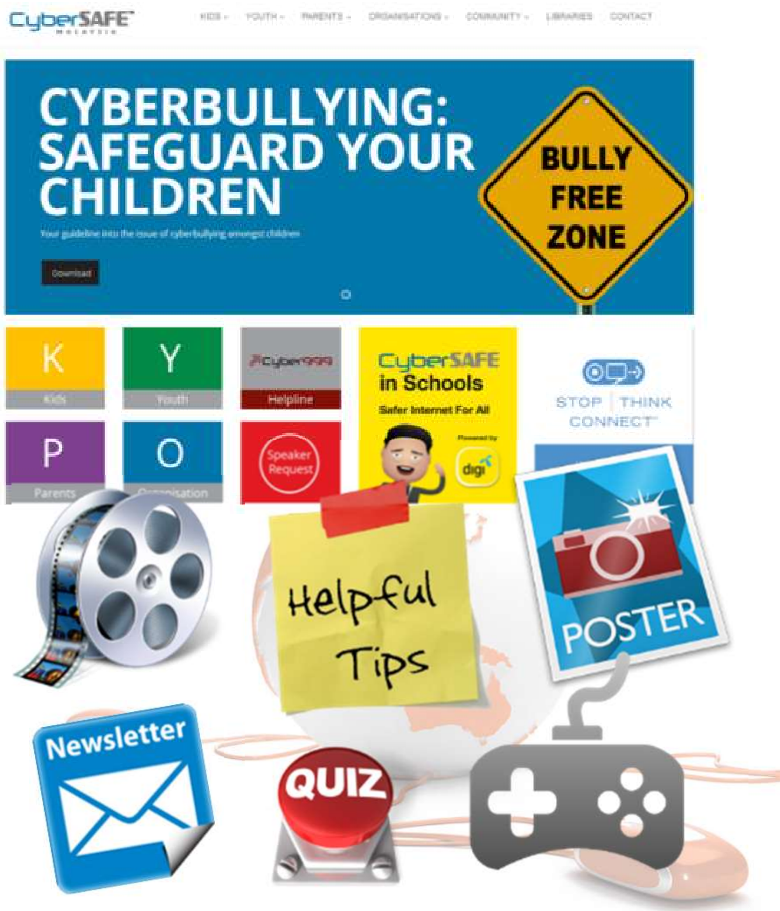
Made it a priority to provide those on the frontlines with the information, tools and resources necessary to increase the national awareness level on the importance of cyber security.


Outreach Program

Inculcate cyber security awareness

Help foster a safer digital world

Culture of digital citizenship among the masses from all occupations and lifestyles



MALAYSIA'S APPROACH IN CAPACITY BUILDING THROUGH BILATERAL & MULTI LATERAL PARTNERSHIP

CyberSecurity MALAYSIA

- As cyber threats become more diverse, persistent and sophisticated; there is a need for **bi-lateral & multi-stakeholders partnership in cyber security capacity building** to formulate a framework for the creation of a competent cybersecurity workforce both at national and regional levels

APCERT
Asia Pacific Computer Emergency Response Team

MALAYSIAN TECHNICAL COOPERATION PROGRAMME

CSCAP

CyberSecurity Malaysia in MoU with CERT Australia

By Digital News Asia | Apr 25, 2014

- *Countries to share info and knowledge on cyber-security*
- *5yr MoU lays out plans for collaborations and partnerships*

WTA
World Trustmark Alliance
Global Trust Innovation

Malaysia and India in cybersecurity pact

By Digital News Asia | Nov 25, 2015

- *MoU signed during Indian PM Narendra Modi's first official visit to Malaysia*
- *Joint activities, plus broader framework for tech and information exchange*

Cybersecurity Malaysia appointed OIC-CERT secretariat

By Digital News Asia | Jan 14, 2013

- *CyberSecurity Malaysia appointed the secretariat to OIC-CERT*
- *Cyber Drill 2013 to be conducted to assess response capability of member agencies*

CYBERSECURITY Malaysia (CSM), an agency under the Ministry of Science, Technology and Innovation (MOSTI) has been appointed the secretariat to the Organization of the Islamic Conference-Computer Emergency Response Team (OIC-CERT).

OIC-CERT
Computer Emergency Response Team
The Organisation of The Islamic Cooperation Computer Emergency Response Team (OIC-CERT)

CYBER RANGE MALAYSIA

- Cyber Range Malaysia was launched at International Islamic University Malaysia (IIUM), Gombak, Selangor on 8th September 2016.

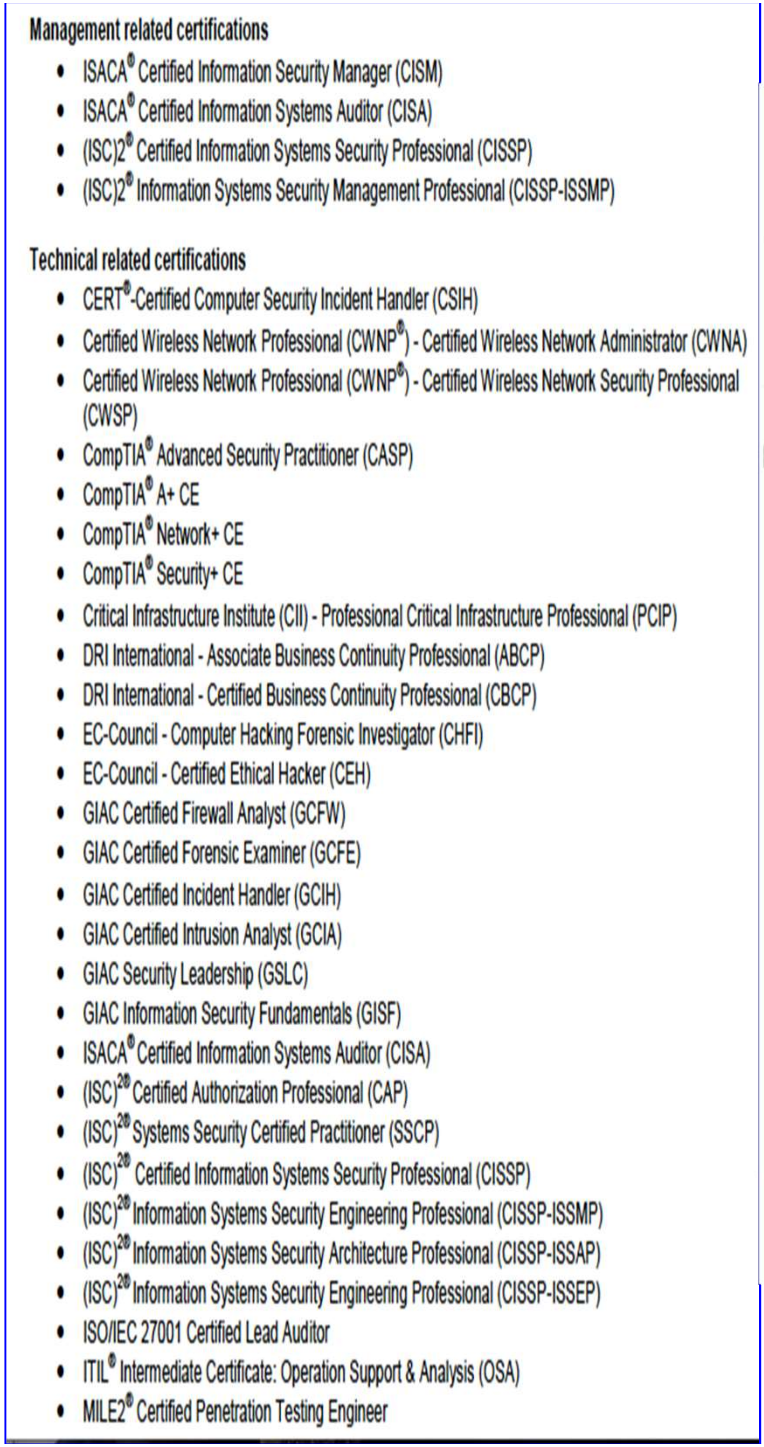
- Cyber Range Malaysia was developed to provide research program and practical training (hands-on) as well as simulation to prepare for cyber attacks. Through Cyber Range Malaysia, organizations can now utilize international standards infrastructure for cyber-attacks simulation to improve their cyber defense capabilities.

POTENTIAL CYBER SECURITY TALENT DEVELOPMENT

- It’s an information security competition organized by CyberSecurity Malaysia in collaboration with Standard Chartered Bank and Asia Pacific University.
- In search for the top new and highly potential cyber security talents and promoting cyber security culture among young generation.
- Promote the culture of being protective (defensive) and responsible in a cyber space.
- Spread global security awareness and provide exposure to undergraduate students about entrepreneurship career and professionalism in lucrative cyber security industry.

CYBERHEROES
CYBER HEROES
COMPETITION 2019
6th - 7th MARCH 2019 | ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION (APU)
“TOGETHER WE DEFEND”

PARTNERSHIP TO DEVELOP MORE CYBER SECURITY PROFESSIONALS

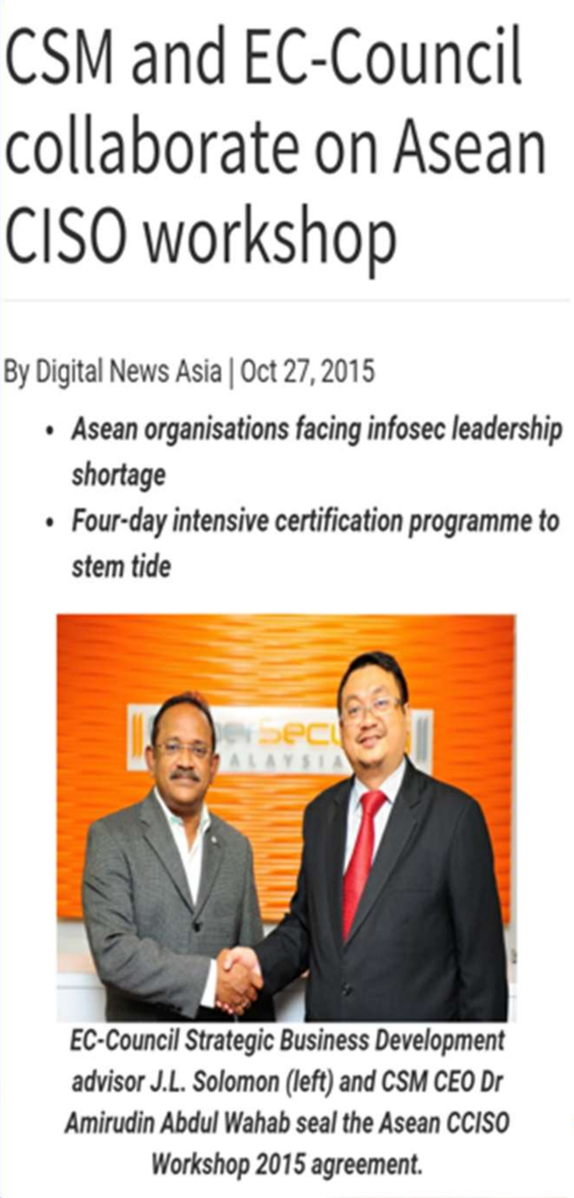


Management related certifications

- ISACA® Certified Information Security Manager (CISM)
- ISACA® Certified Information Systems Auditor (CISA)
- (ISC)2® Certified Information Systems Security Professional (CISSP)
- (ISC)2® Information Systems Security Management Professional (CISSP-ISSMP)

Technical related certifications

- CERT®-Certified Computer Security Incident Handler (CSIH)
- Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Administrator (CWNA)
- Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Security Professional (CWSP)
- CompTIA® Advanced Security Practitioner (CASP)
- CompTIA® A+ CE
- CompTIA® Network+ CE
- CompTIA® Security+ CE
- Critical Infrastructure Institute (CII) - Professional Critical Infrastructure Professional (PCIP)
- DRI International - Associate Business Continuity Professional (ABCP)
- DRI International - Certified Business Continuity Professional (CBCP)
- EC-Council - Computer Hacking Forensic Investigator (CHFI)
- EC-Council - Certified Ethical Hacker (CEH)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Forensic Examiner (GCFE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Security Leadership (GSLC)
- GIAC Information Security Fundamentals (GISF)
- ISACA® Certified Information Systems Auditor (CISA)
- (ISC)$^{2®}$ Certified Authorization Professional (CAP)
- (ISC)$^{2®}$ Systems Security Certified Practitioner (SSCP)
- (ISC)$^{2®}$ Certified Information Systems Security Professional (CISSP)
- (ISC)$^{2®}$ Information Systems Security Engineering Professional (CISSP-ISSMP)
- (ISC)$^{2®}$ Information Systems Security Architecture Professional (CISSP-ISSAP)
- (ISC)$^{2®}$ Information Systems Security Engineering Professional (CISSP-ISSEP)
- ISO/IEC 27001 Certified Lead Auditor
- ITIL® Intermediate Certificate: Operation Support & Analysis (OSA)
- MILE2® Certified Penetration Testing Engineer



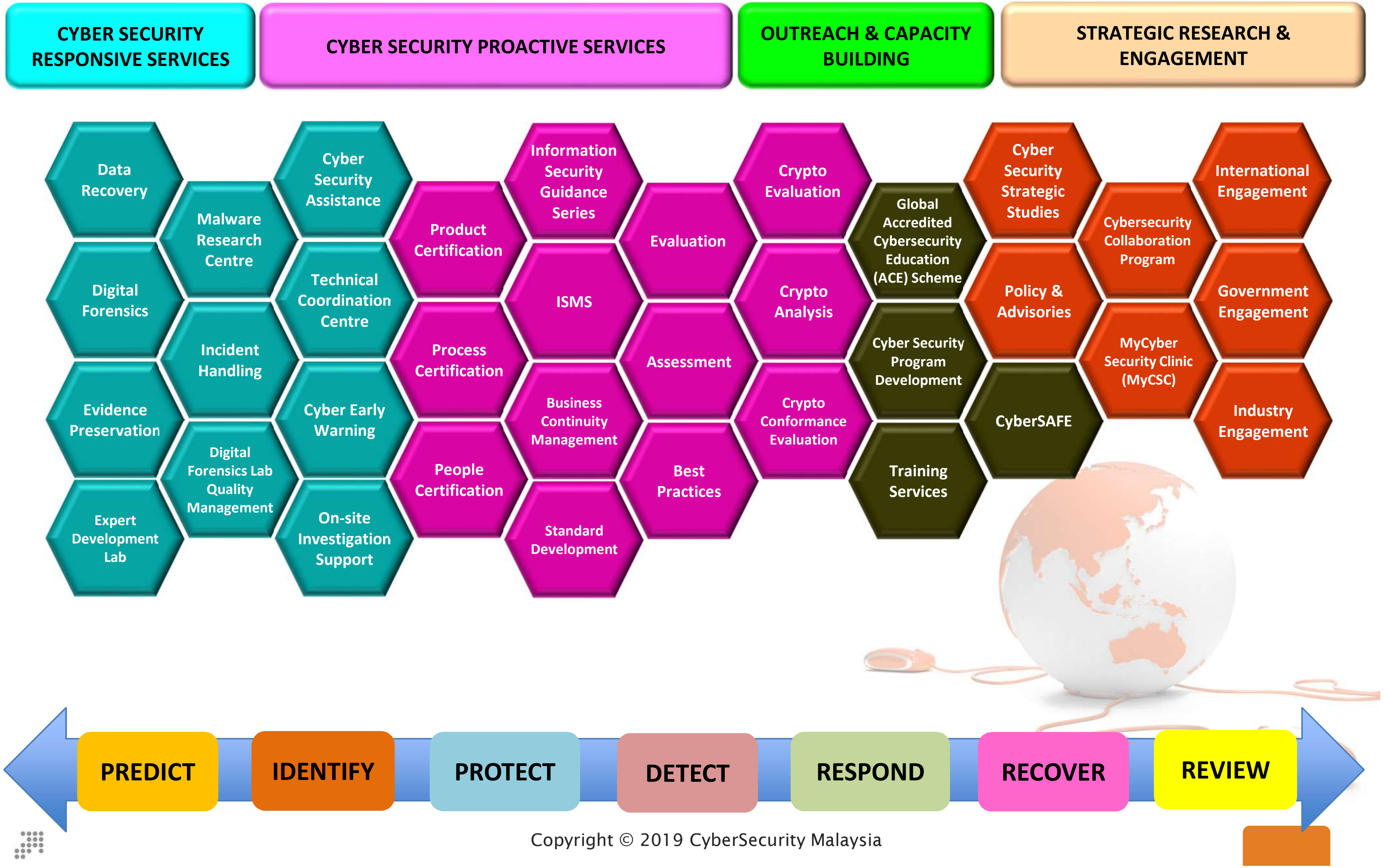
CSM and EC-Council collaborate on Asean CISO workshop

By Digital News Asia | Oct 27, 2015

- *Asean organisations facing infosec leadership shortage*
- *Four-day intensive certification programme to stem tide*

EC-Council Strategic Business Development advisor J.L. Solomon (left) and CSM CEO Dr Amirudin Abdul Wahab seal the Asean CCISO Workshop 2015 agreement.

CSM SERVICES ACROSS CYBER SECURITY DOMAIN & LIFECYCLE



CYBER SECURITY RESPONSIVE SERVICES

CYBER SECURITY PROACTIVE SERVICES

OUTREACH & CAPACITY BUILDING

STRATEGIC RESEARCH & ENGAGEMENT

Data Recovery

Digital Forensics

Evidence Preservation

Expert Development Lab

Malware Research Centre

Incident Handling

Digital Forensics Lab Quality Management

Cyber Security Assistance

Technical Coordination Centre

Cyber Early Warning

On-site Investigation Support

Product Certification

Process Certification

People Certification

Information Security Guidance Series

ISMS

Business Continuity Management

Standard Development

Evaluation

Assessment

Best Practices

Crypto Evaluation

Crypto Analysis

Crypto Conformance Evaluation

Global Accredited Cybersecurity Education (ACE) Scheme

Cyber Security Program Development

Training Services

Cyber Security Strategic Studies

Policy & Advisories

CyberSAFE

Cybersecurity Collaboration Program

MyCyber Security Clinic (MyCSC)

International Engagement

Government Engagement

Industry Engagement

PREDICT

IDENTIFY

PROTECT

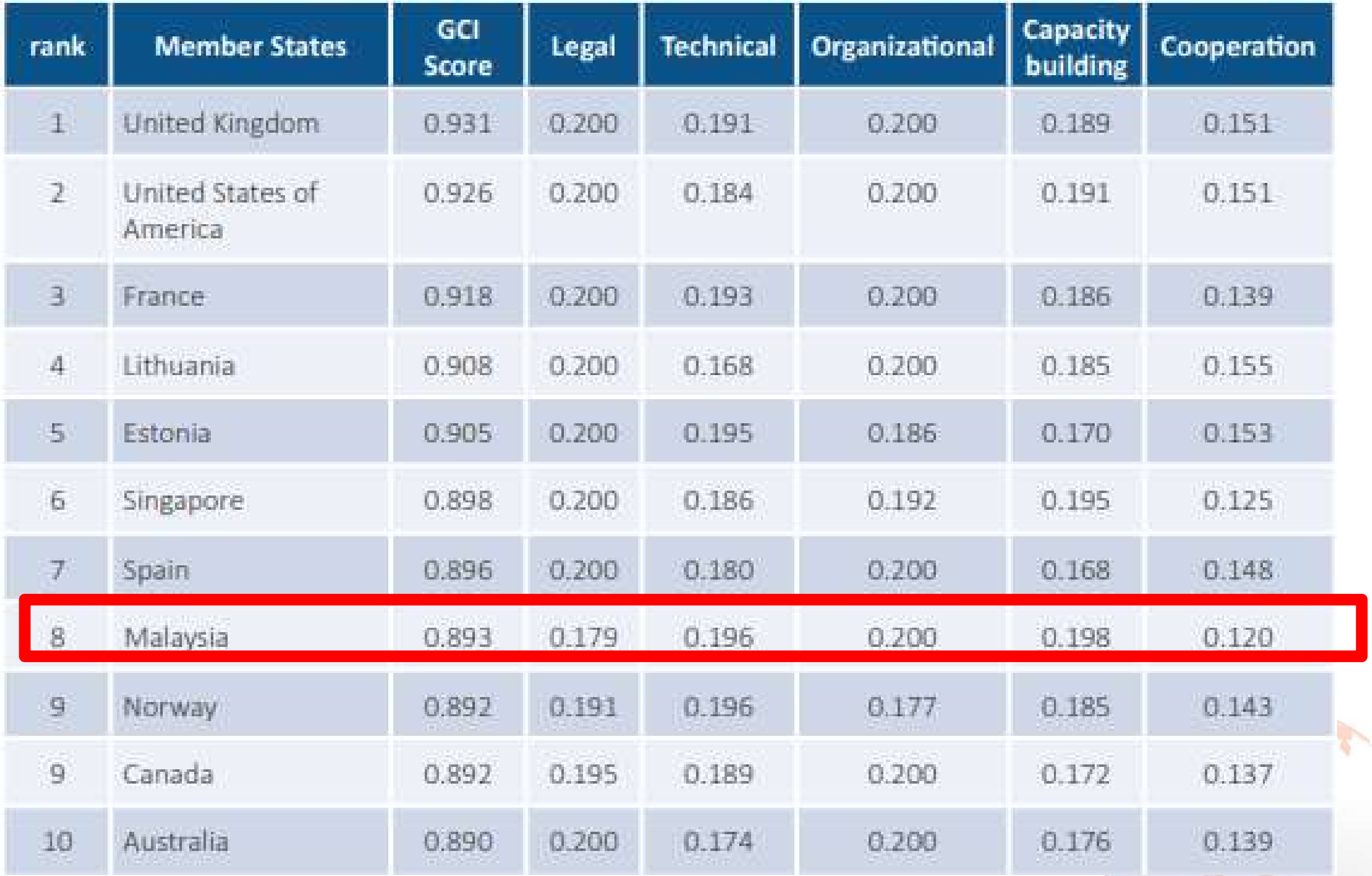
DETECT

RESPOND

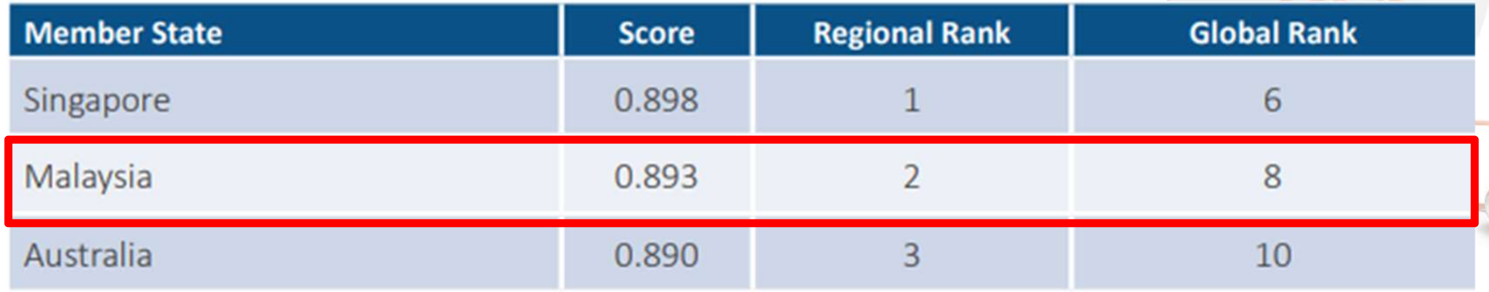
RECOVER

REVIEW

MALAYSIA'S ACHIEVEMENT IN THE I.T.U GLOBAL CYBER SECURITY INDEX 2017 – 8th in Top 10 Global Ranking and 2nd in Top 3 in Asia Pacific



rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
2	United States of America	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
9	Canada	0.892	0.195	0.189	0.200	0.172	0.137
10	Australia	0.890	0.200	0.174	0.200	0.176	0.139



Member State	Score	Regional Rank	Global Rank
Singapore	0.898	1	6
Malaysia	0.893	2	8
Australia	0.890	3	10

CONCLUSION AND WAY FORWARD

- ❖ **4IR presents a tremendous opportunity for economic growth, sustainability, and social improvement but they can’t just be sophisticated but they also need to be safe.**

- ❖ **A proactive and comprehensive measures to address evolving cyber threats in 4IR era by:**

- ➢ Having a cyber security protection that is **dynamic**, **holistic**, **innovative** and **adaptive** with a flexible, intelligent strategy to counter the advanced cyber attacks;

- ➢ Strengthening domestic and global cyber security through **inter-agency cooperation** and **Public-Private Partnership**;

- ➢ **Being prepared is the key** to prevent bigger cyber security problems in the era of 4IR.

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

Thank you

Corporate Office
Level 7, Tower 1
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

Best Brand Internet Security 2008 & 2009

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

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

MSC MALAYSIA Status Company

Best Child Online Protection Website