PDiSA

KEMENTERIAN
KOMUNIKASI DAN DIGITAL

CyberSecurity MALAYSIA

DUNIA KESELAMATAN SIBER

Masa Kini

13 September 2023

DATO’ TS. DR. HAJI AMIRUDIN ABDUL WAHAB FASc,

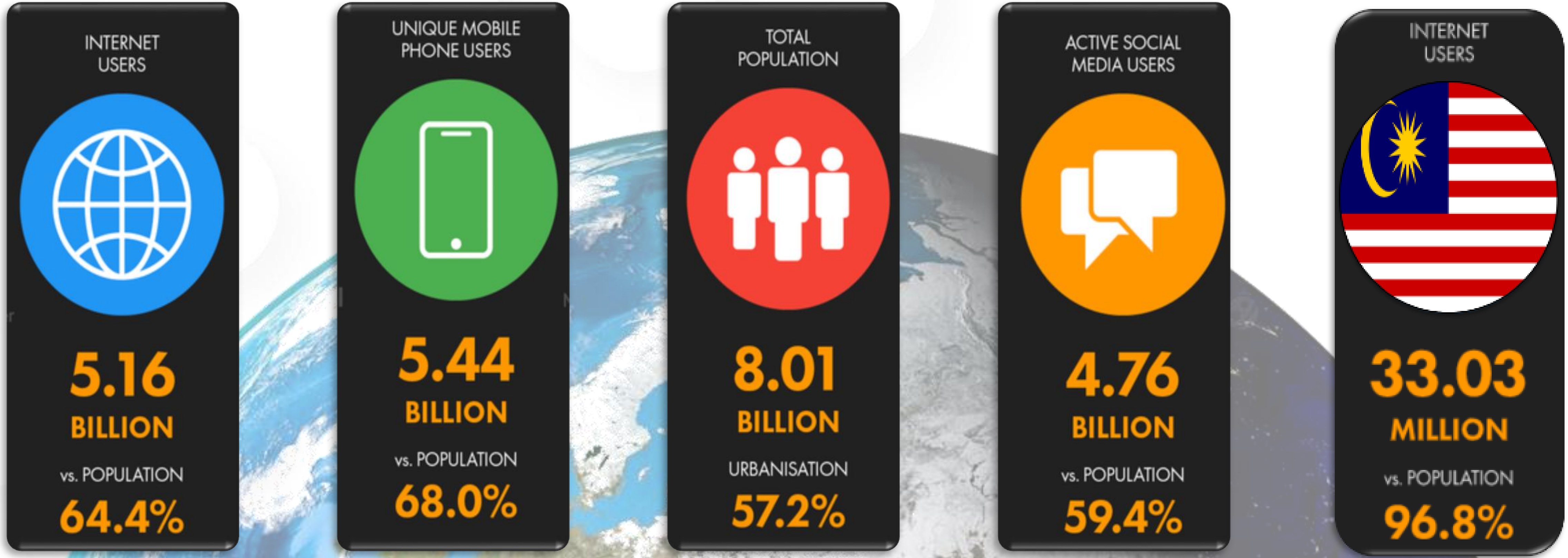
Ketua Pegawai Eksekutif
CyberSecurity Malaysia

MELINDUNGI
RUANG SIBER
ANDA

Copyright © 2023 CyberSecurity Malaysia

DUNIA DIGITAL KINI

KE ARAH RUANG SIBER YANG SALING BERKAIT



INTERNET USERS
5.16 BILLION
vs. POPULATION
64.4%

UNIQUE MOBILE PHONE USERS
5.44 BILLION
vs. POPULATION
68.0%

TOTAL POPULATION
8.01 BILLION
URBANISATION
57.2%

ACTIVE SOCIAL MEDIA USERS
4.76 BILLION
vs. POPULATION
59.4%

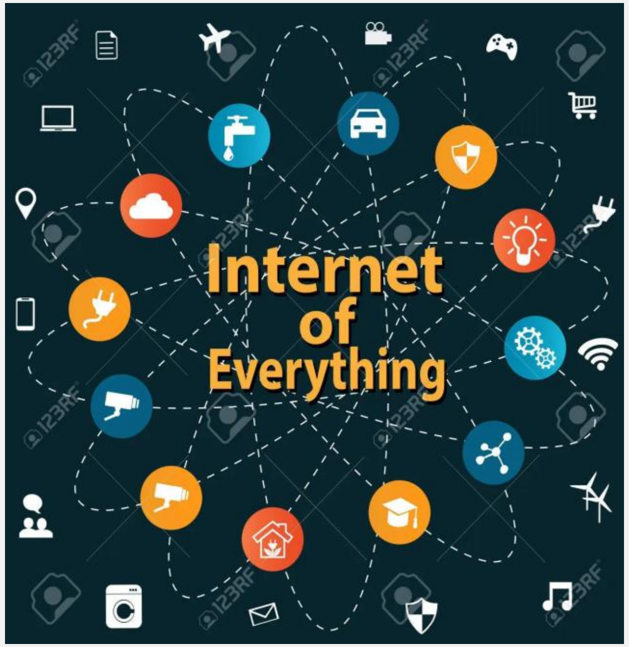
INTERNET USERS
33.03 MILLION
vs. POPULATION
96.8%

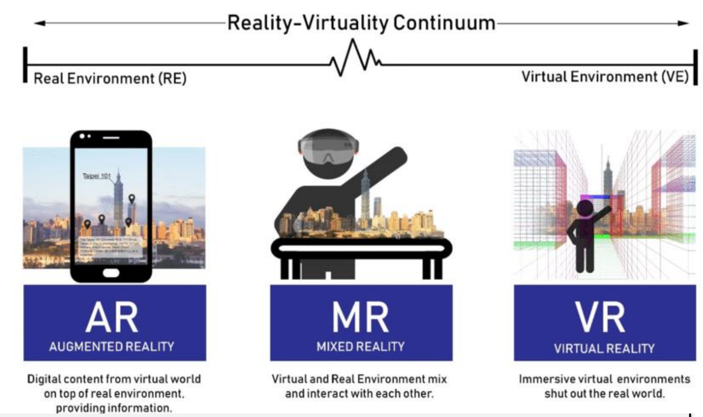
Digital 2023: Global Overview Report — DataReportal – Global Digital Insights

Copyright © 2023 CyberSecurity Malaysia

KEMUNCULAN TEKNOLOGI

Menyebabkan Landskap Siber Semakin Rumit

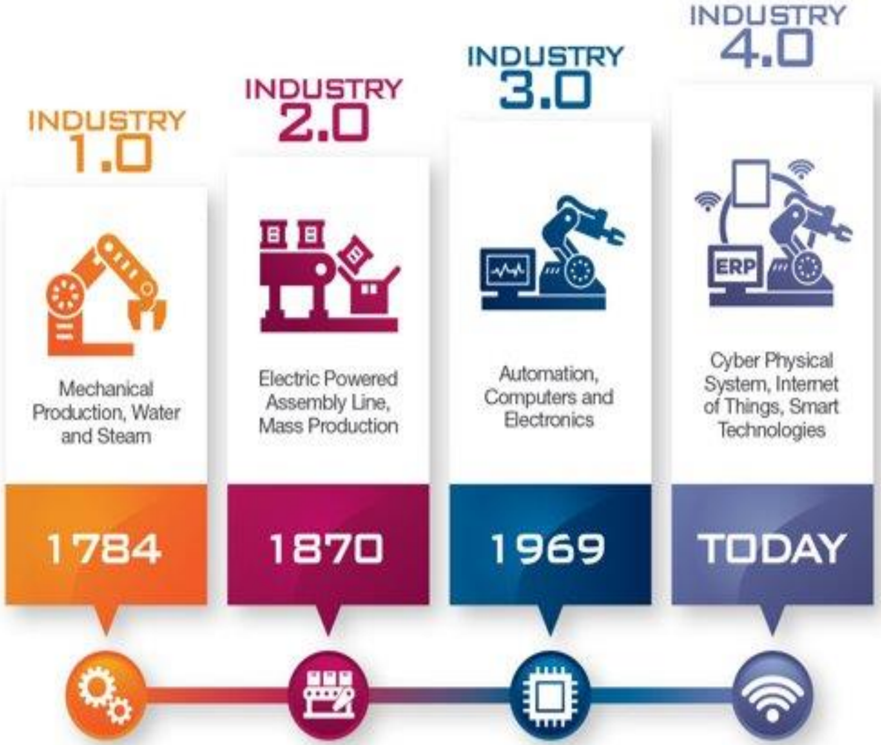



Reality-Virtuality Continuum
Real Environment (RE)
Virtual Environment (VE)
Taipei 101
AR
AUGMENTED REALITY
Digital content from virtual world on top of real environment, providing information.
MR
MIXED REALITY
Virtual and Real Environment mix and interact with each other.
VR
VIRTUAL REALITY
Immersive virtual environments shut out the real world.

Copyright © 2023 CyberSecurity Malaysia

TRANSFORMASI DIGITAL

TO ACHIEVE BY 2030
4TH INDUSTRIAL REVOLUTION


INDUSTRY 1.0
Mechanical Production, Water and Steam
1784
INDUSTRY 2.0
Electric Powered Assembly Line, Mass Production
1870
INDUSTRY 3.0
Automation, Computers and Electronics
1969
INDUSTRY 4.0
ERP
Cyber Physical System, Internet of Things, Smart Technologies
TODAY

MALAYSIA'S DIGITAL TRANSFORMATION: MALAYSIA DIGITAL ECONOMY BLUEPRINT AND THE NATIONAL 4IR POLICY

MyDIGITAL

MyDIGITAL CORPORATION
MINISTRY OF ECONOMY
WORLD ECONOMIC FORUM
Malaysia Centre for the Fourth Industrial Revolution
Shaping the Fourth Industrial Revolution
Building a Better Future for All
15 May 2023
NEW STRAITS TIMES

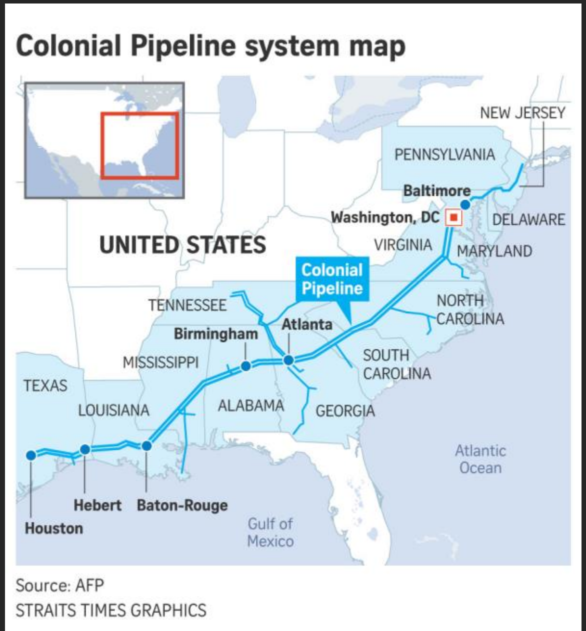
Jendela
Jalinan Digital Negara

Dalam Fasa 2 (2023-2025), transformasi digital akan diutamakan.

Dalam Fasa 3 (dari 2026 hingga 2030) akan meletakkan Malaysia sebagai peneraju serantau dalam kandungan digital dan keselamatan siber. Misi MyDIGITAL adalah untuk memastikan rakyat Malaysia mendapat manfaat daripada peluang revolusi digital.

Copyright © 2023 CyberSecurity Malaysia

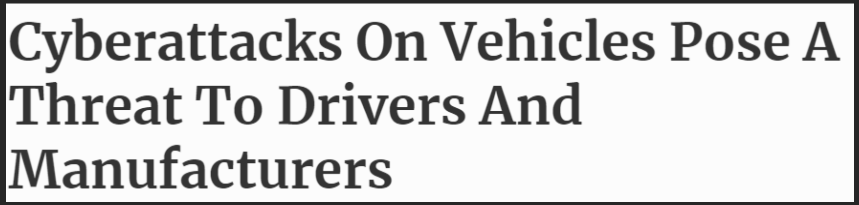
SERANGAN SIBER BERUPAYA MEMBERI KESAN FIZIKAL



Colonial Pipeline system map

Source: AFP
STRAITS TIMES GRAPHICS

Chinese cyber attack on power grid
Status of cyber security in India
#UPSC #IAS
by Rahul Saigaonker



Cyberattacks On Vehicles Pose A Threat To Drivers And Manufacturers

CYBER PHYSICAL ATTACK

TRANSFORMASI DIGITAL TIDAK TERLEPAS DARIPADA RISIKO

- Teknologi telah mengubah cara pengguna menjalankan perniagaan, menawarkan pekerja dengan capaian berterusan kepada aplikasi dan data perniagaan yang kritikal.

- Walaupun fleksibiliti ini mudah dan mengembangkan produktiviti, ia juga telah memperkenalkan risiko, cabaran dan ancaman keselamatan siber

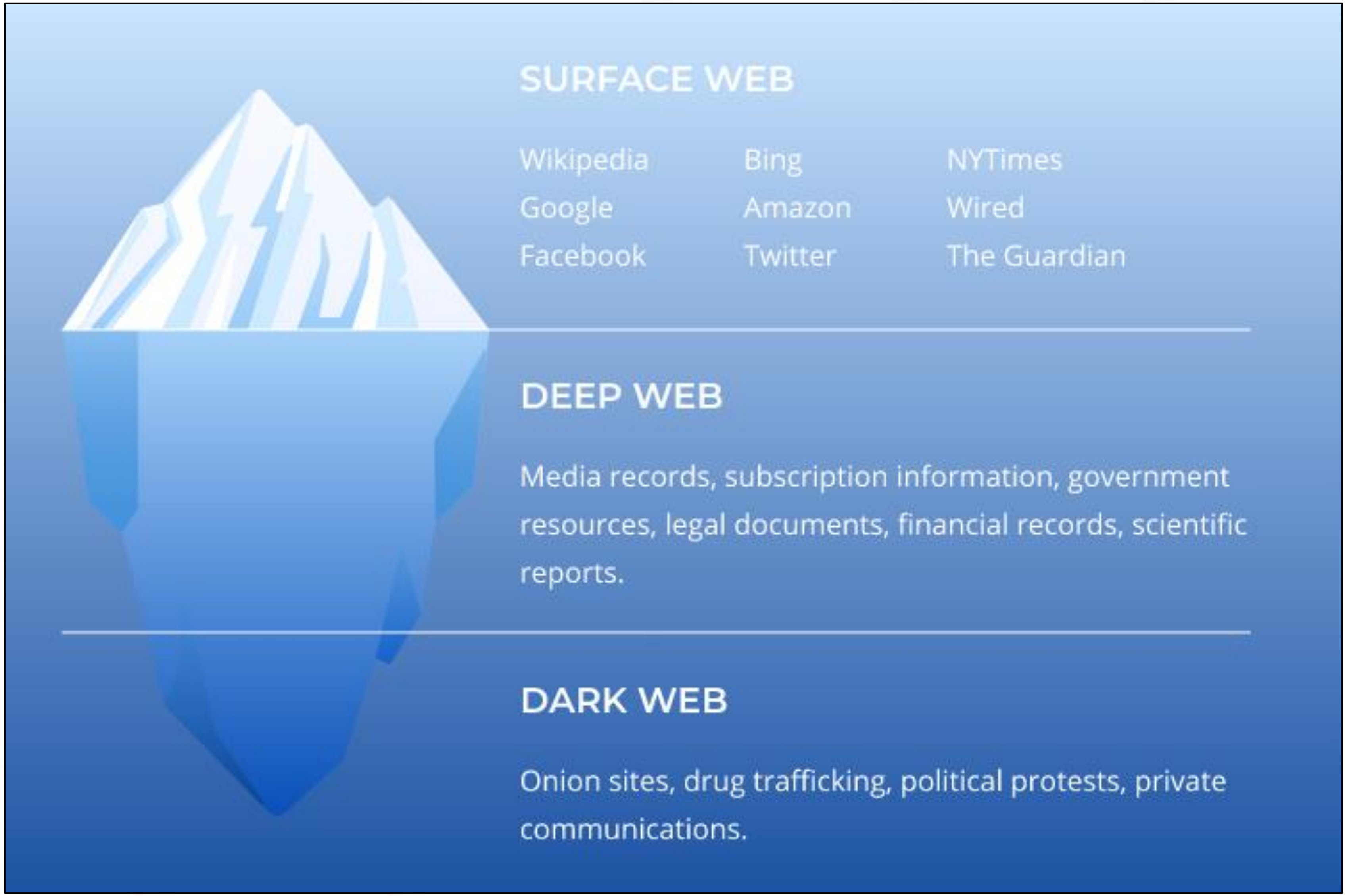
RISIKO GLOBAL 2023

	2 years		10 years
1	Cost-of-living crisis	1	Failure to mitigate climate change
2	Natural disasters and extreme weather events	2	Failure of climate-change adaptation
3	Geoeconomic confrontation	3	Natural disasters and extreme weather events
4	Failure to mitigate climate change	4	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	5	Large-scale involuntary migration
6	Large-scale environmental damage incidents	6	Natural resource crises
7	Failure of climate change adaptation	7	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	8	Widespread cybercrime and cyber insecurity
9	Natural resource crises	9	Geoeconomic confrontation
10	Large-scale involuntary migration	10	Large-scale environmental damage incidents

Source: WEF_Global_Risks_Report_2023.pdf (weforum.org)

Copyright © 2023 CyberSecurity Malaysia

…MAKLUMAT TERSEMBUNYI…



SURFACE WEB

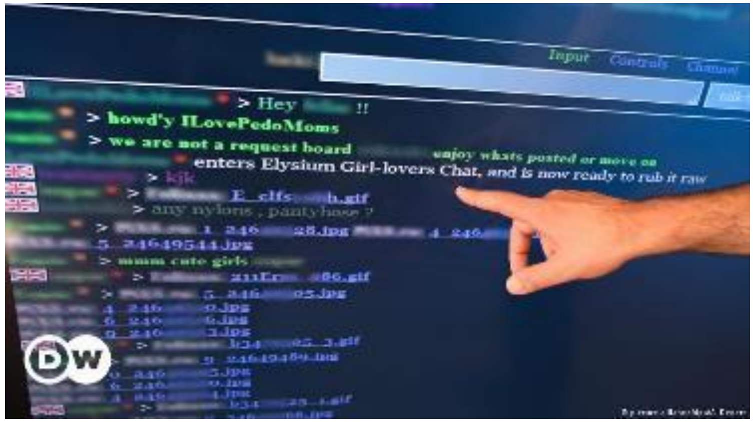
Wikipedia	Bing	NYTimes
Google	Amazon	Wired
Facebook	Twitter	The Guardian

DEEP WEB

Media records, subscription information, government resources, legal documents, financial records, scientific reports.

DARK WEB

Onion sites, drug trafficking, political protests, private communications.

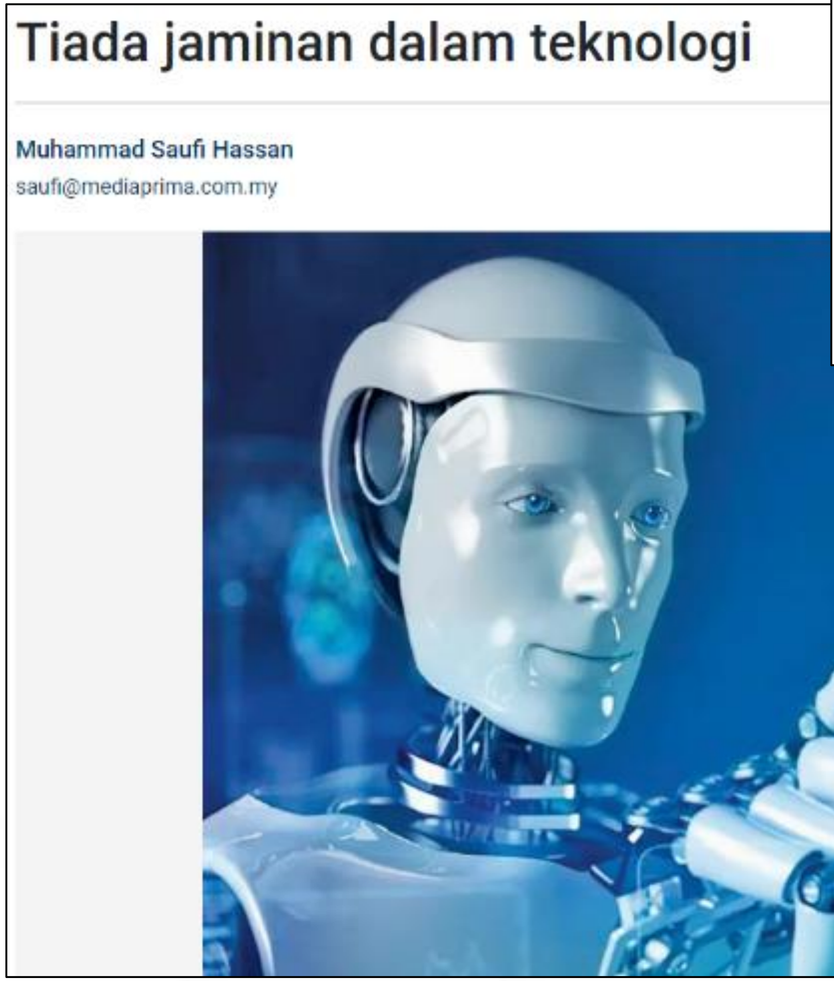


```
> Hey
> howd'y ILovePedoMoms
> we are not a request board     enjoy whats posted or move on
  enters Elysium Girl-lovers Chat, and is now ready to rub it raw
> kik
> any nylons , pantyhose ?
> mmm cute girls
```

…RISIKO TERSEMBUNYI…

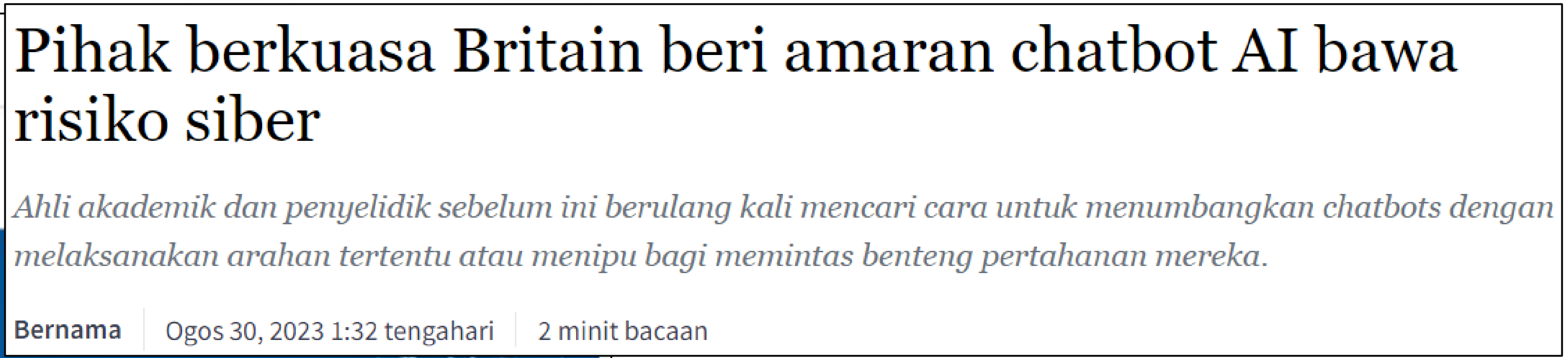
Copyright © 2023 CyberSecurity Malaysia

KEMAJUAN TEKNOLOGI MEMBAWA CABARAN BAHARU



Tiada jaminan dalam teknologi

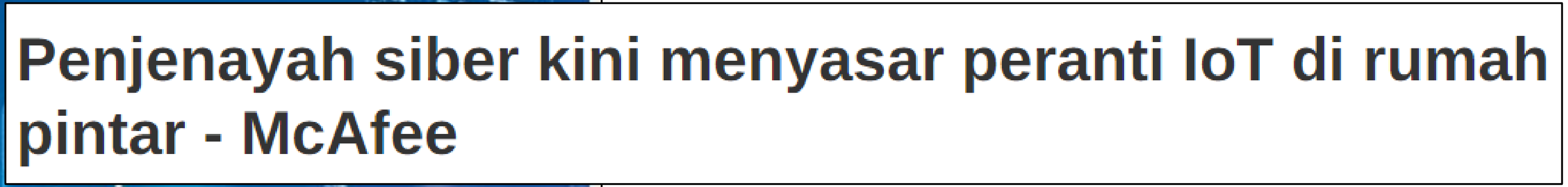
Muhammad Saufi Hassan
saufi@mediaprima.com.my



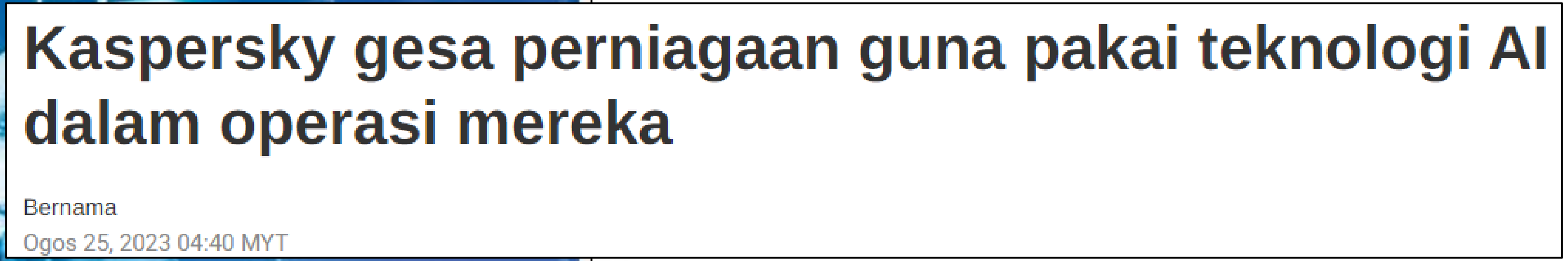
Pihak berkuasa Britain beri amaran chatbot AI bawa risiko siber

Ahli akademik dan penyelidik sebelum ini berulang kali mencari cara untuk menumbangkan chatbots dengan melaksanakan arahan tertentu atau menipu bagi memintas benteng pertahanan mereka.

Bernama | Ogos 30, 2023 1:32 tengahari | 2 minit bacaan

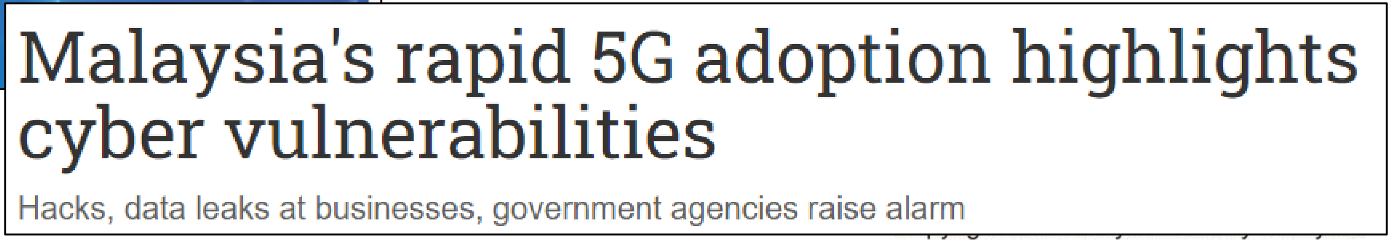


Penjenayah siber kini menyasar peranti IoT di rumah pintar - McAfee



Kaspersky gesa perniagaan guna pakai teknologi AI dalam operasi mereka

Bernama
Ogos 25, 2023 04:40 MYT

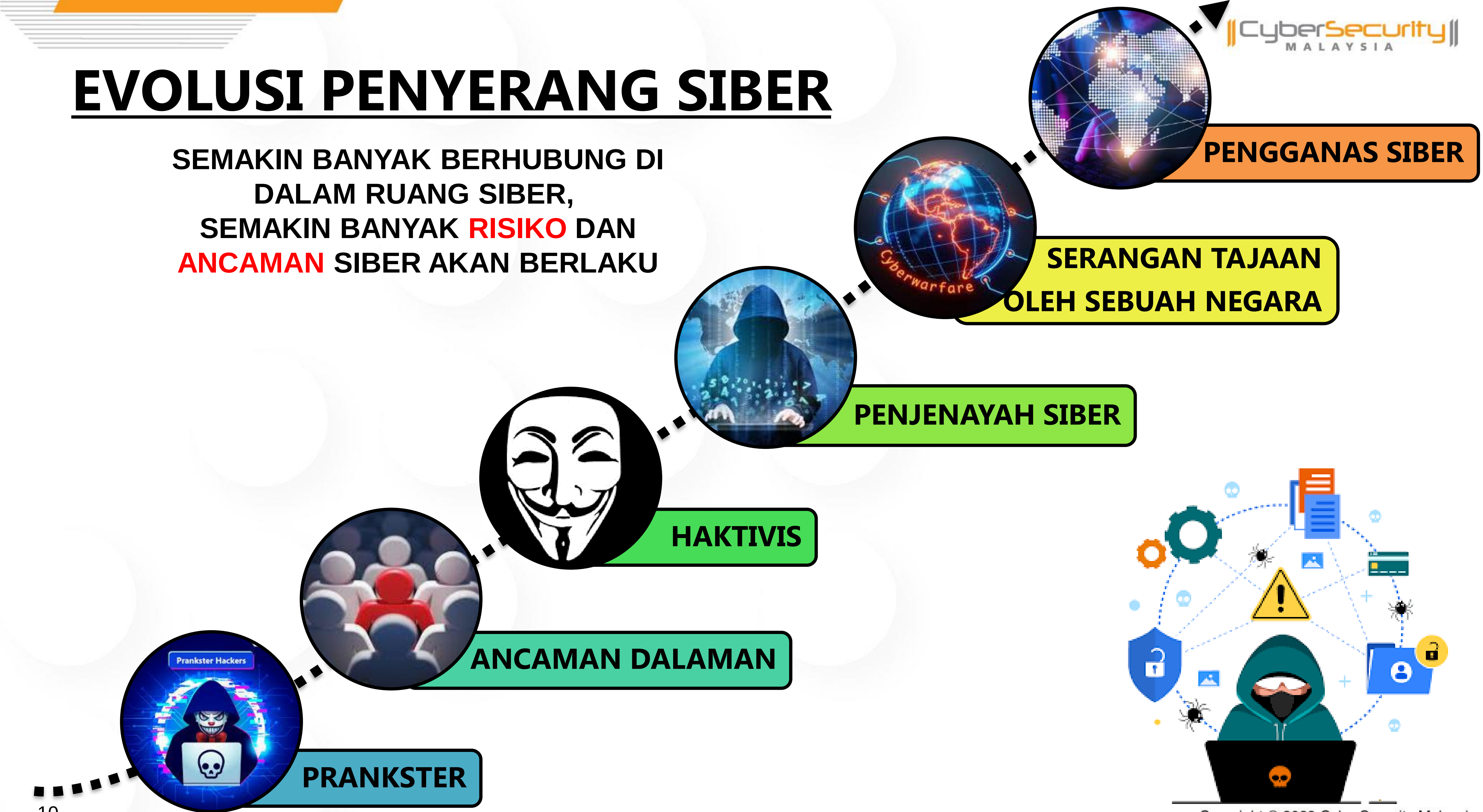


Malaysia's rapid 5G adoption highlights cyber vulnerabilities

Hacks, data leaks at businesses, government agencies raise alarm

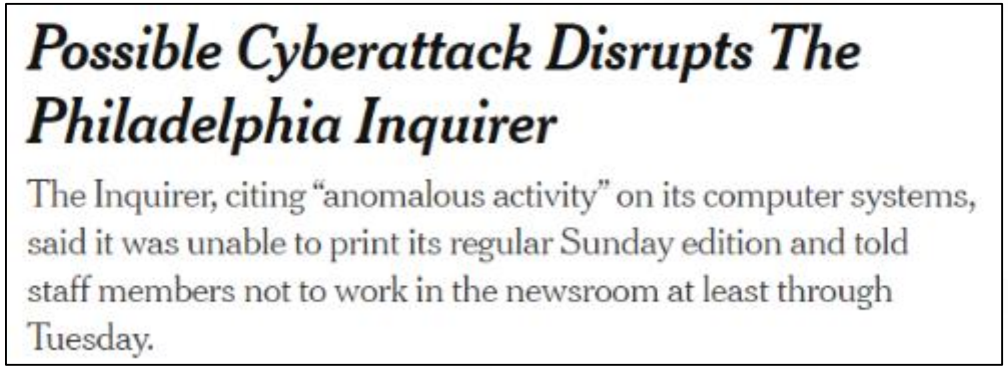
EVOLUSI PENYERANG SIBER

SEMAKIN BANYAK BERHUBUNG DI DALAM RUANG SIBER,
SEMAKIN BANYAK RISIKO DAN ANCAMAN SIBER AKAN BERLAKU



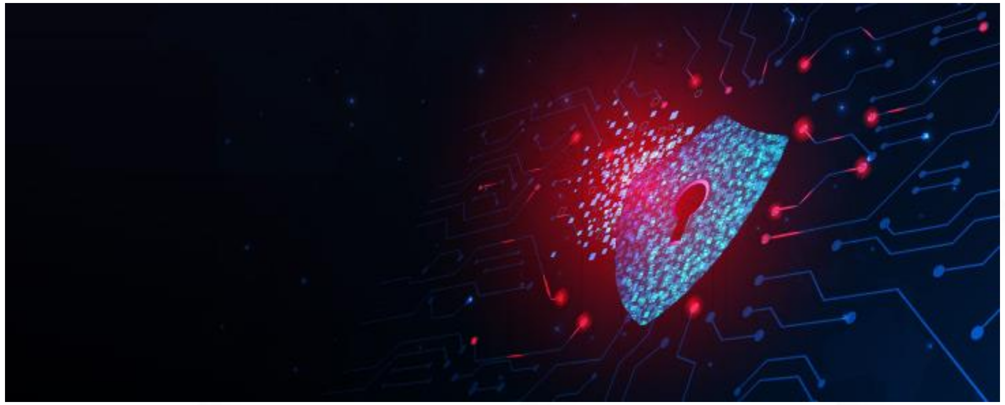
Copyright © 2023 CyberSecurity Malaysia

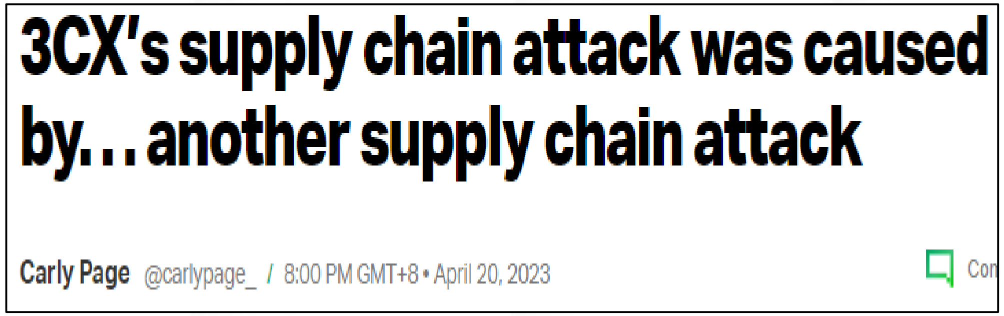
SERANGAN SIBER DI SELURUH DUNIA



Possible Cyberattack Disrupts The Philadelphia Inquirer

The Inquirer, citing "anomalous activity" on its computer systems, said it was unable to print its regular Sunday edition and told staff members not to work in the newsroom at least through Tuesday.

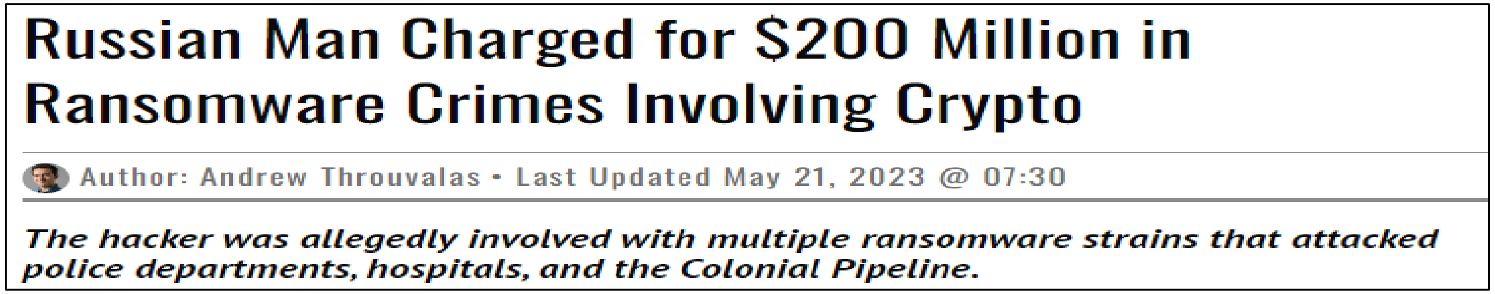




3CX's supply chain attack was caused by... another supply chain attack

Carly Page @carlypage_ / 8:00 PM GMT+8 • April 20, 2023

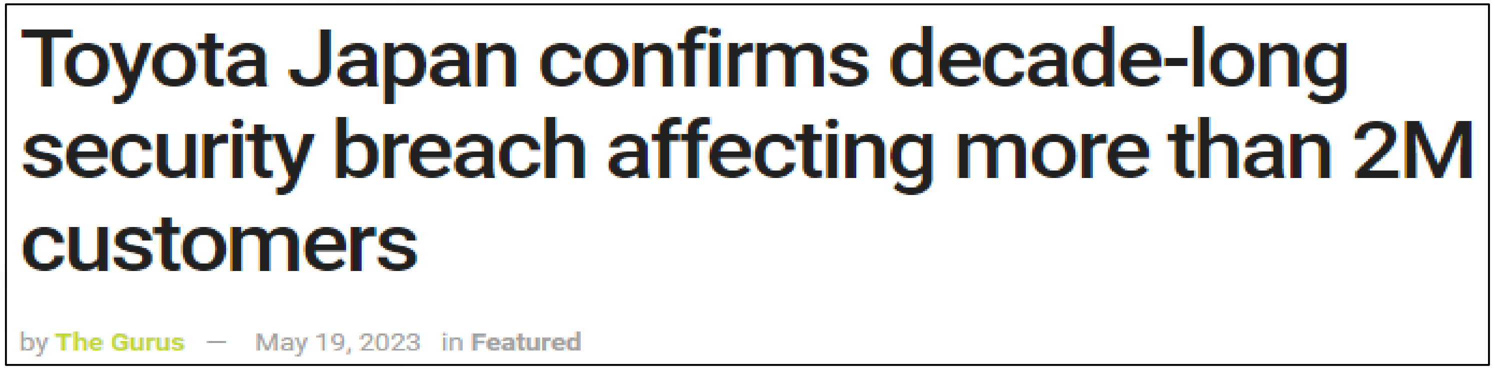
Con



Russian Man Charged for $200 Million in Ransomware Crimes Involving Crypto

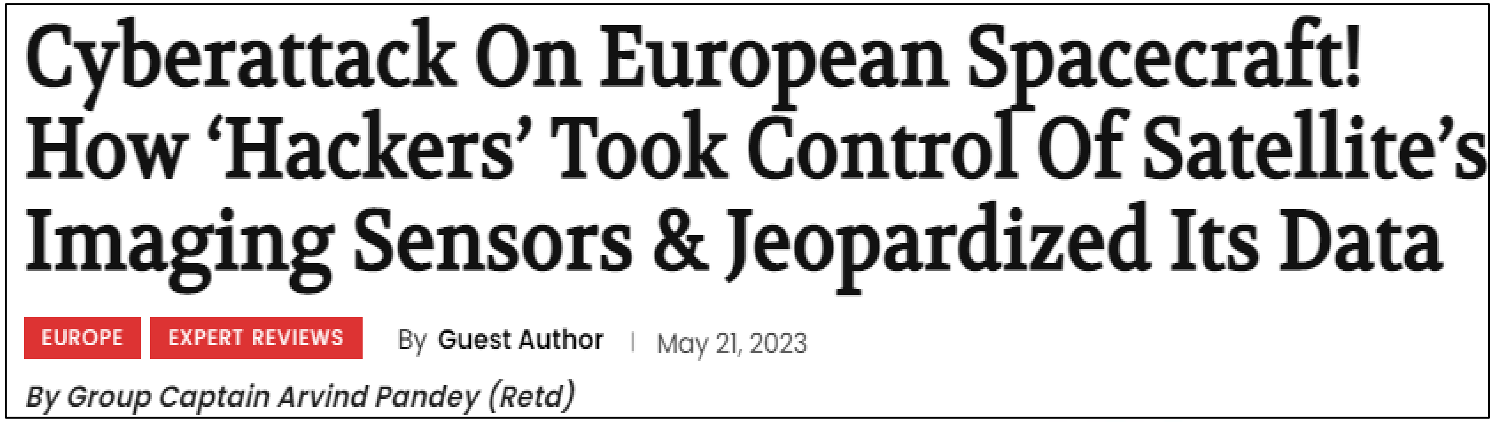
Author: Andrew Throuvalas • Last Updated May 21, 2023 @ 07:30

The hacker was allegedly involved with multiple ransomware strains that attacked police departments, hospitals, and the Colonial Pipeline.



Toyota Japan confirms decade-long security breach affecting more than 2M customers

by The Gurus — May 19, 2023 in Featured



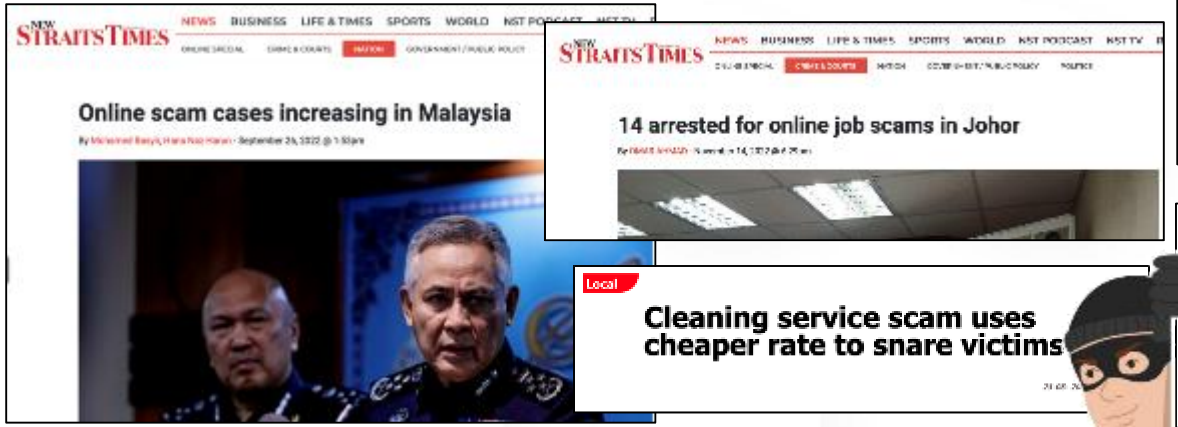
Cyberattack On European Spacecraft! How 'Hackers' Took Control Of Satellite's Imaging Sensors & Jeopardized Its Data

EUROPE EXPERT REVIEWS By Guest Author | May 21, 2023

By Group Captain Arvind Pandey (Retd)

Copyright © 2023 CyberSecurity Malaysia

SERANGAN SIBER DI MALAYSIA



NEW STRAITS TIMES

NEWS BUSINESS LIFE & TIMES SPORTS WORLD NST PODCAST

Online scam cases increasing in Malaysia

By Mohamed Basyir, Hana Naz Harun - September 26, 2022 @ 1:50pm

NEW STRAITS TIMES

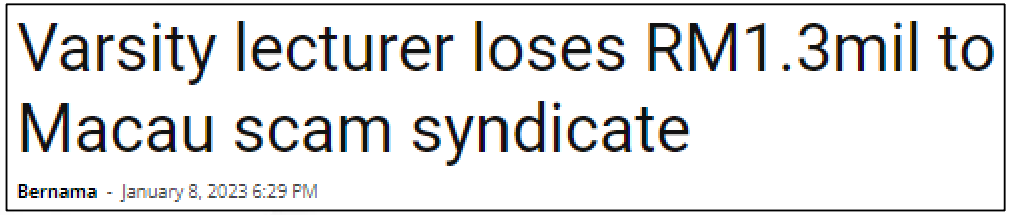
NEWS BUSINESS LIFE & TIMES SPORTS WORLD NST PODCAST NST TV

CRIME & COURTS NATION

14 arrested for online job scams in Johor

Local

Cleaning service scam uses cheaper rate to snare victims



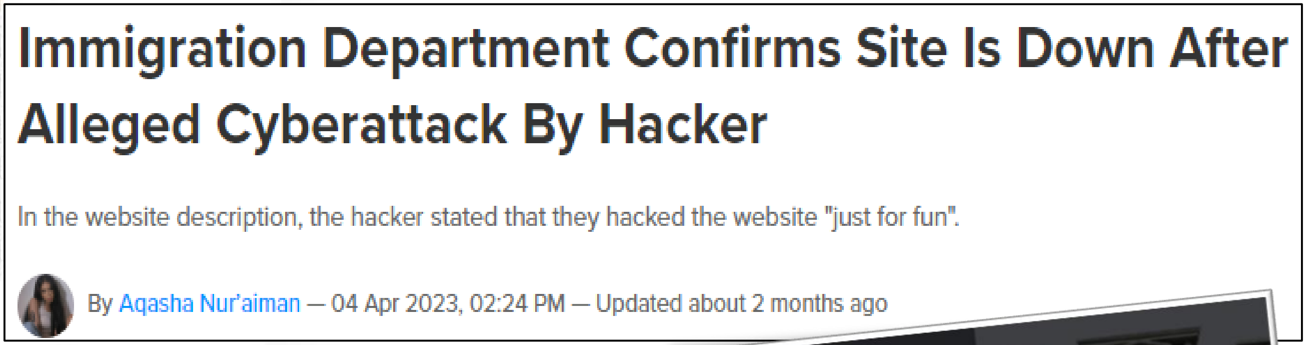
Varsity lecturer loses RM1.3mil to Macau scam syndicate

Bernama - January 8, 2023 6:29 PM

Fortinet: Malaysia recorded 84 million cyber attacks daily in fourth quarter last year

By Bernama - February 22, 2023 @ 10:16am

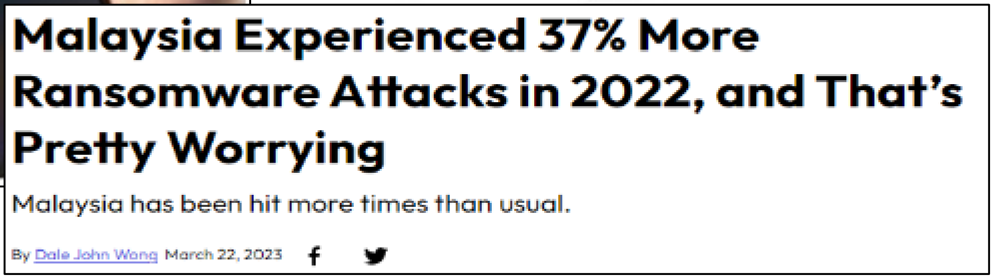
Most cell phone numbers in Malaysia are leaked and sold to scammers. Are telcos to be blamed?



Immigration Department Confirms Site Is Down After Alleged Cyberattack By Hacker

In the website description, the hacker stated that they hacked the website "just for fun".

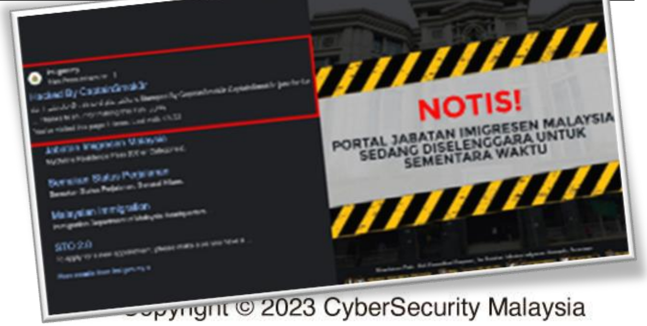
By Aqasha Nur'aiman — 04 Apr 2023, 02:24 PM — Updated about 2 months ago



Malaysia Experienced 37% More Ransomware Attacks in 2022, and That's Pretty Worrying

Malaysia has been hit more times than usual.

By Dale John Wong March 22, 2023



Hacked By CaptainGreak3r

Jabatan Imigresen Malaysia

Semakan Status Pas Perjalanan

Malaysian Immigration

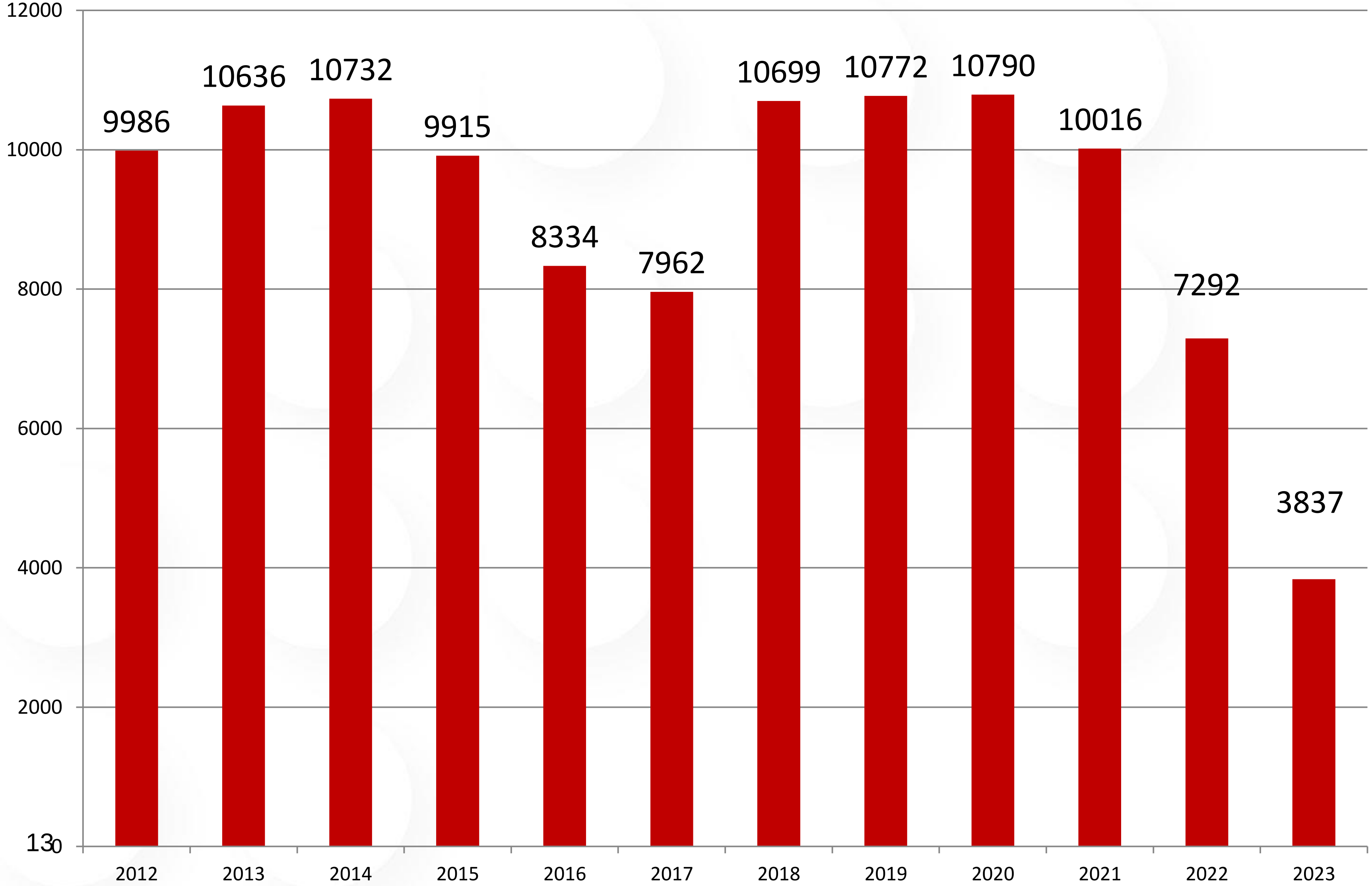
STO 2.0

NOTIS!

PORTAL JABATAN IMIGRESEN MALAYSIA SEDANG DISELENGGARA UNTUK SEMENTARA WAKTU

Copyright © 2023 CyberSecurity Malaysia

INSIDEN KESELAMATAN SIBER YANG DILAPORKAN KEPADA CYBERSECURITY MALAYSIA (2011 – 31 Ogos 2023)



MyCERT Incident Statistics

Security Alert

EMPAT INSIDEN SIBER TERTINGGI DI MALAYSIA (CYBER999)

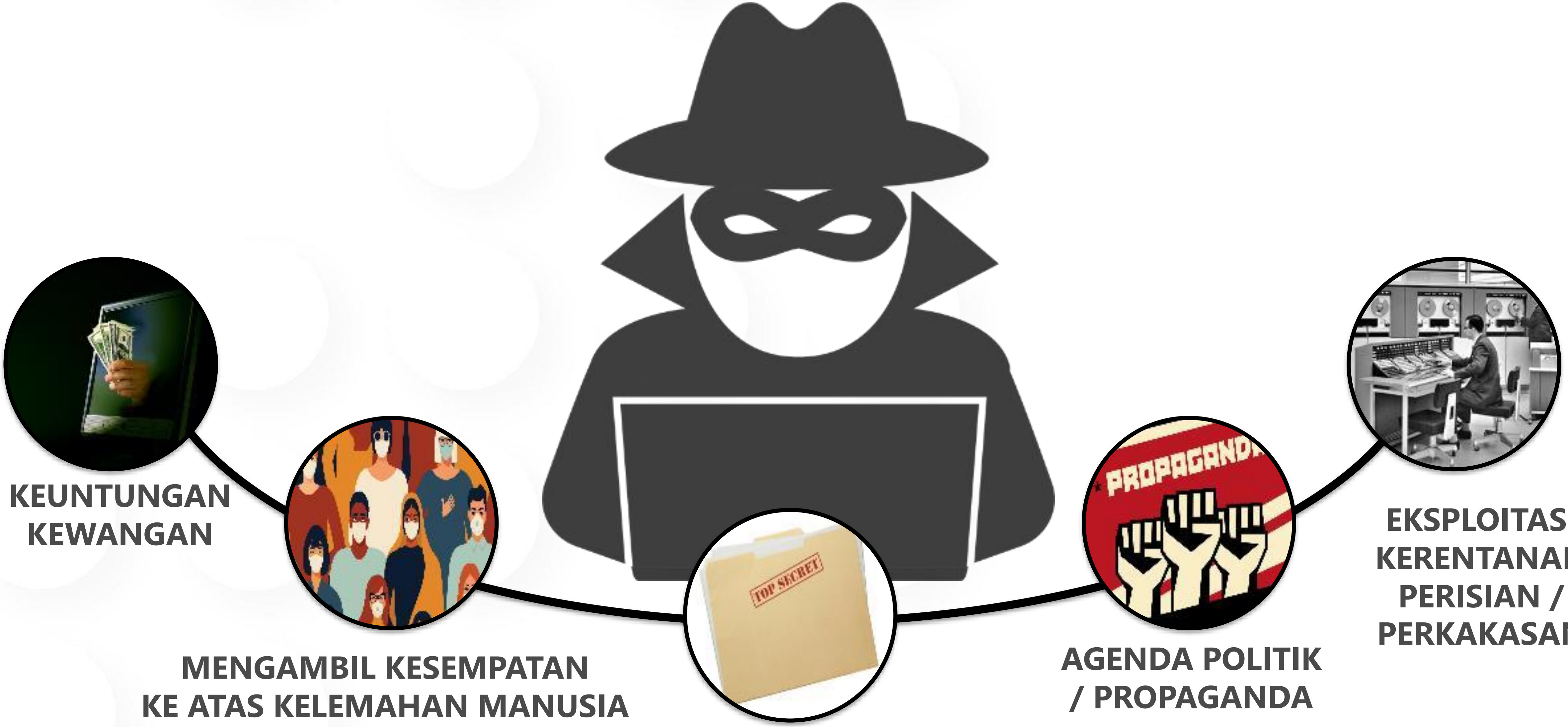
1. Penipuan
2. Kod Berbahaya
3. Pencerobohan
4. Berkaitan Kandungan

Jenis Insiden

1. Pencerobohan
2. Percubaan Pencerobohan
3. Denial of Service Attack (DOS)
4. Penipuan
5. Spam
6. Kandungan Berkaitan
7. Laporan Kerentanan
8. Malicious Codes

Copyright © 2023 CyberSecurity Malaysia

KENAPA IANYA MASIH LAGI BERLAKU?



KEUNTUNGAN KEWANGAN

MENGAMBIL KESEMPATAN KE ATAS KELEMAHAN MANUSIA

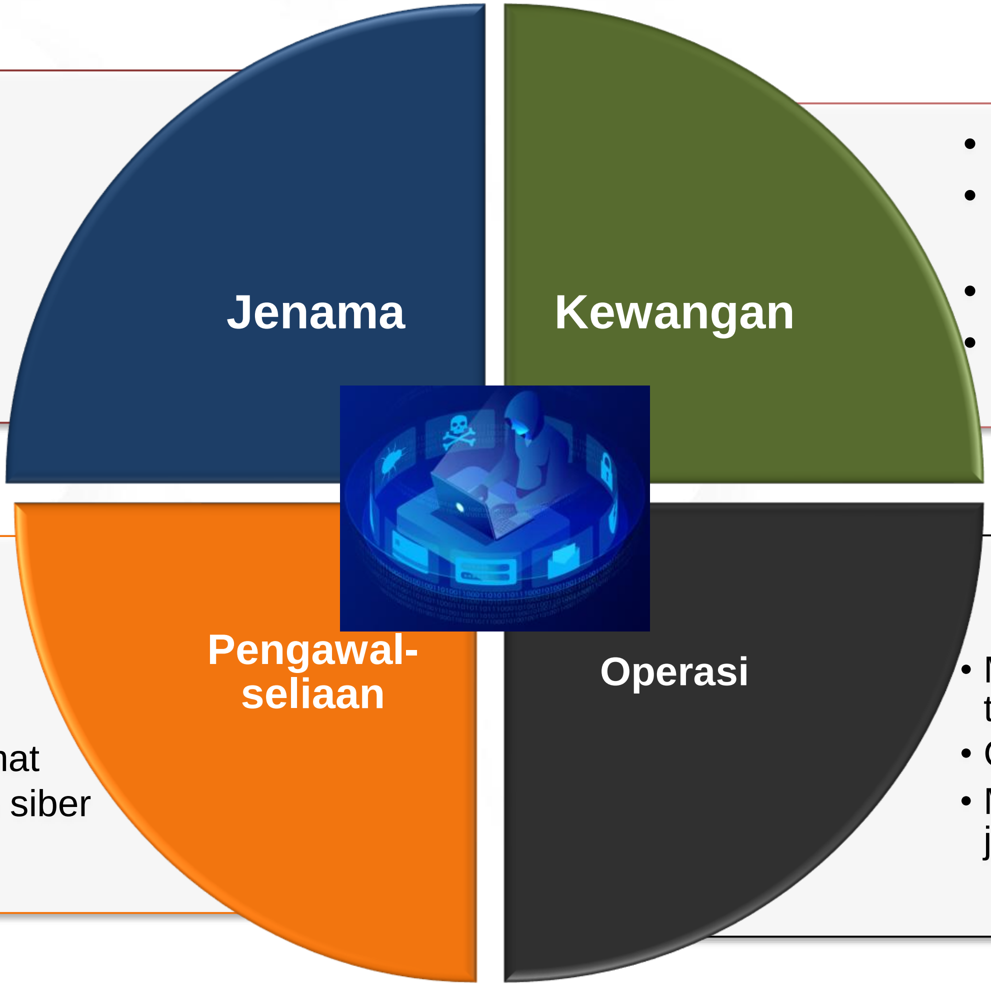
PENGINTIPAN SIBER

AGENDA POLITIK / PROPAGANDA

EKSPLOITASI KERENTANAN PERISIAN / PERKAKASAN

Copyright © 2023 CyberSecurity Malaysia

RISIKO DAN IMPAK SERANGAN SIBER



Jenama

- Kritikan dari media dan orang awam
- Perhubungan Awam terjejas
- Kehilangan harta intelek /aset

Kewangan

- Peningkatan kos
- Kehilangan perniagaan / kontrak
- Hilang persaingan
- Kos pemulihan

Kos kepada insuran premium

Pengawal-seliaan

- Audit bebas
- Tindakan Undang-undang
- Sekatan dalam perkongsian maklumat
- Membangunkan solusi keselamatan siber yang komprehensif

Operasi

- Mengalih perhatian kakitangan kepada tugas pemulihan
- Gangguan kepada operasi
- Melakukan pengawalan kerosakan dan juga pemulihan organisasi

Copyright © 2023 CyberSecurity Malaysia

This Photo by Unknown author is licensed under CC BY-NC-ND.

KESELAMATAN SIBER ADALAH TANGGUNGJAWAB BERSAMA

SEMUA ORANG BERTANGGUNGJAWAB

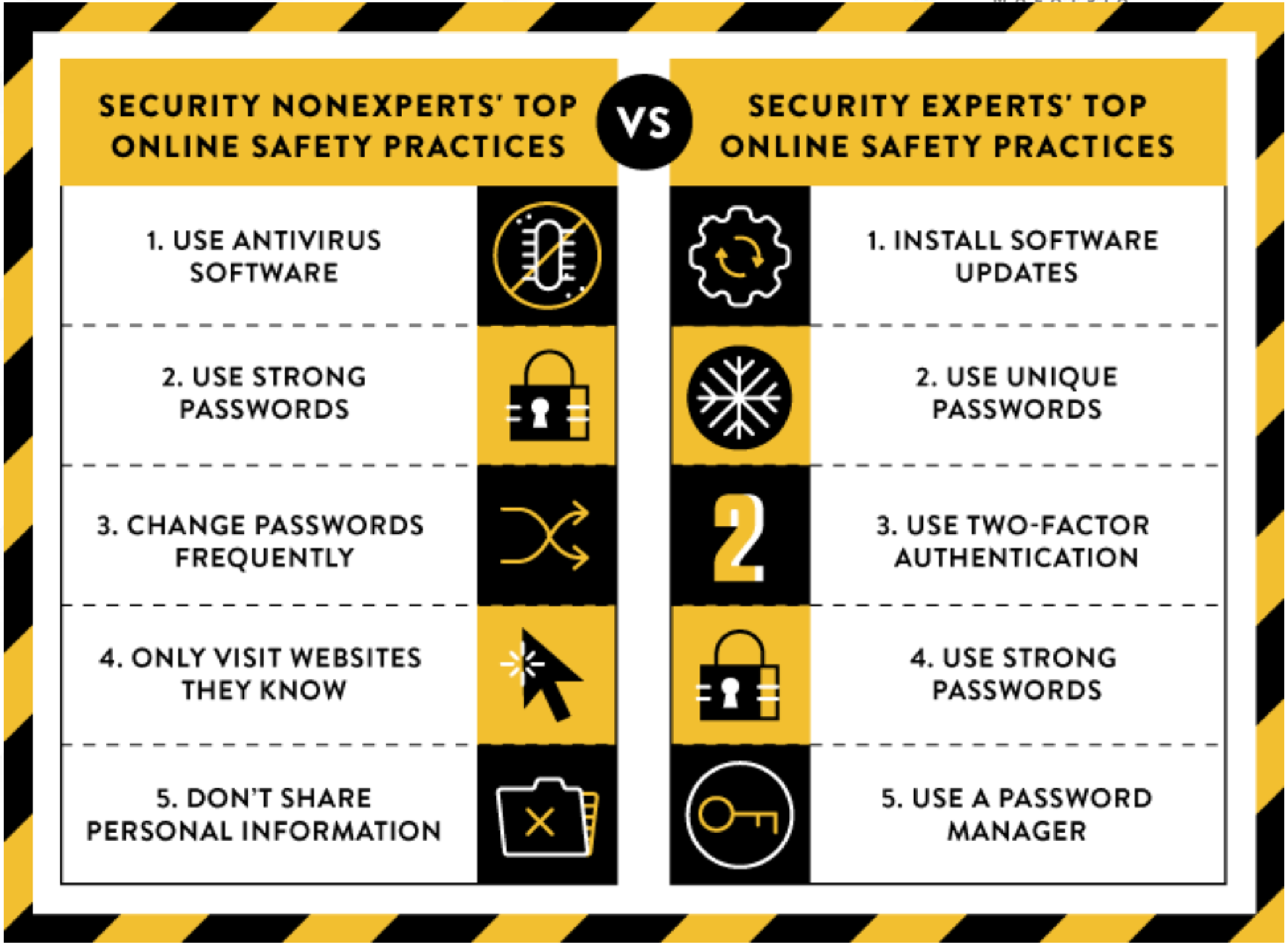
KESELAMATAN SIBER **TIDAK** BERFUNGSI SECARA **SILO**

PIHAK PENGURUSAN PERLU MEMIMPIN DENGAN CONTOH, MENINGKATKAN KEMAMPUAN KESELAMATAN SIBER ORGANISASI

Copyright © 2023 CyberSecurity Malaysia

CYBER HYGIENE

Merujuk kepada asas amalan terbaik keselamatan siber yang boleh dilakukan oleh pengamal dan pengguna keselamatan organisasi.



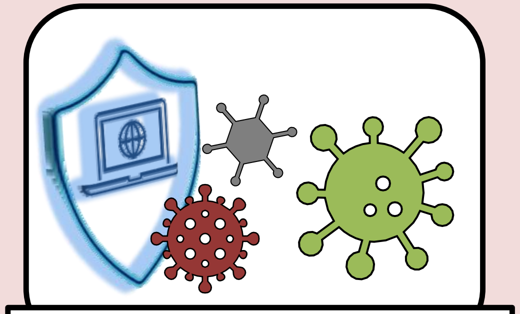
SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

Practice Great Cyber Hygiene - Cyber Risk Opportunities

Copyright © 2023 CyberSecurity Malaysia

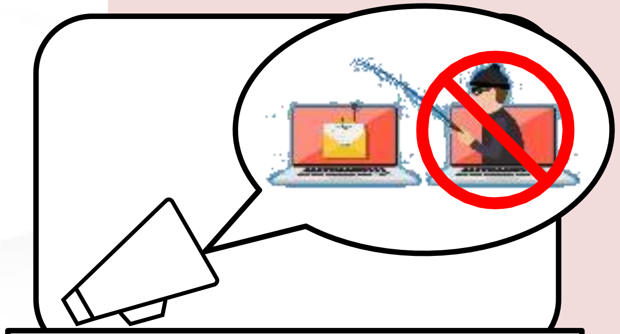
ASAS KESELAMATAN SIBER

KATA LALUAN YANG KOMPLEKS

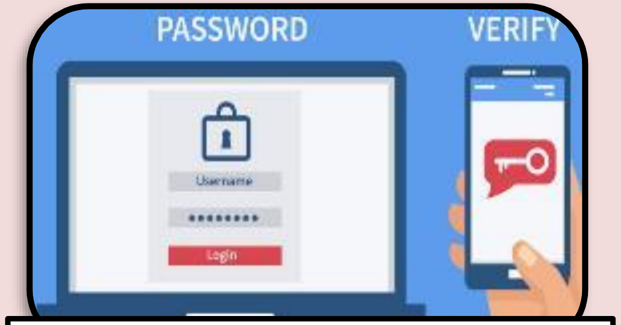


PERISIAN ANTIVIRUS

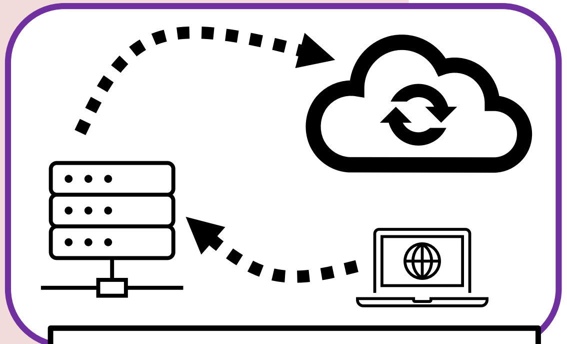
KEMASKINI SISTEM BERKALA



KEMPEN KESEDARAN BERTERUSAN



2-FAKTOR PENGESAHAN



SANDARAN BERJADUAL

Copyright © 2023 CyberSecurity Malaysia

CyberSecurity
MALAYSIA

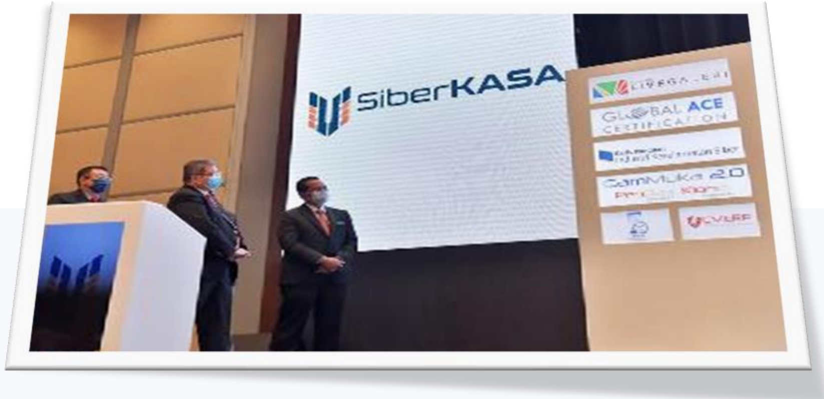
INISIATIF
CYBERSECURITY MALAYSIA

SiberKASA

SiberKASA

DILANCARKAN SECARA RASMI PADA
23 MAC 2021

SiberKASA merupakan inisiatif kerajaan yang bertujuan untuk membangun, memperkasa, mengukuh dan melestarikan prasarana serta ekosistem keselamatan siber negara agar sentiasa mampan, terpelihara dan berdaya tahan

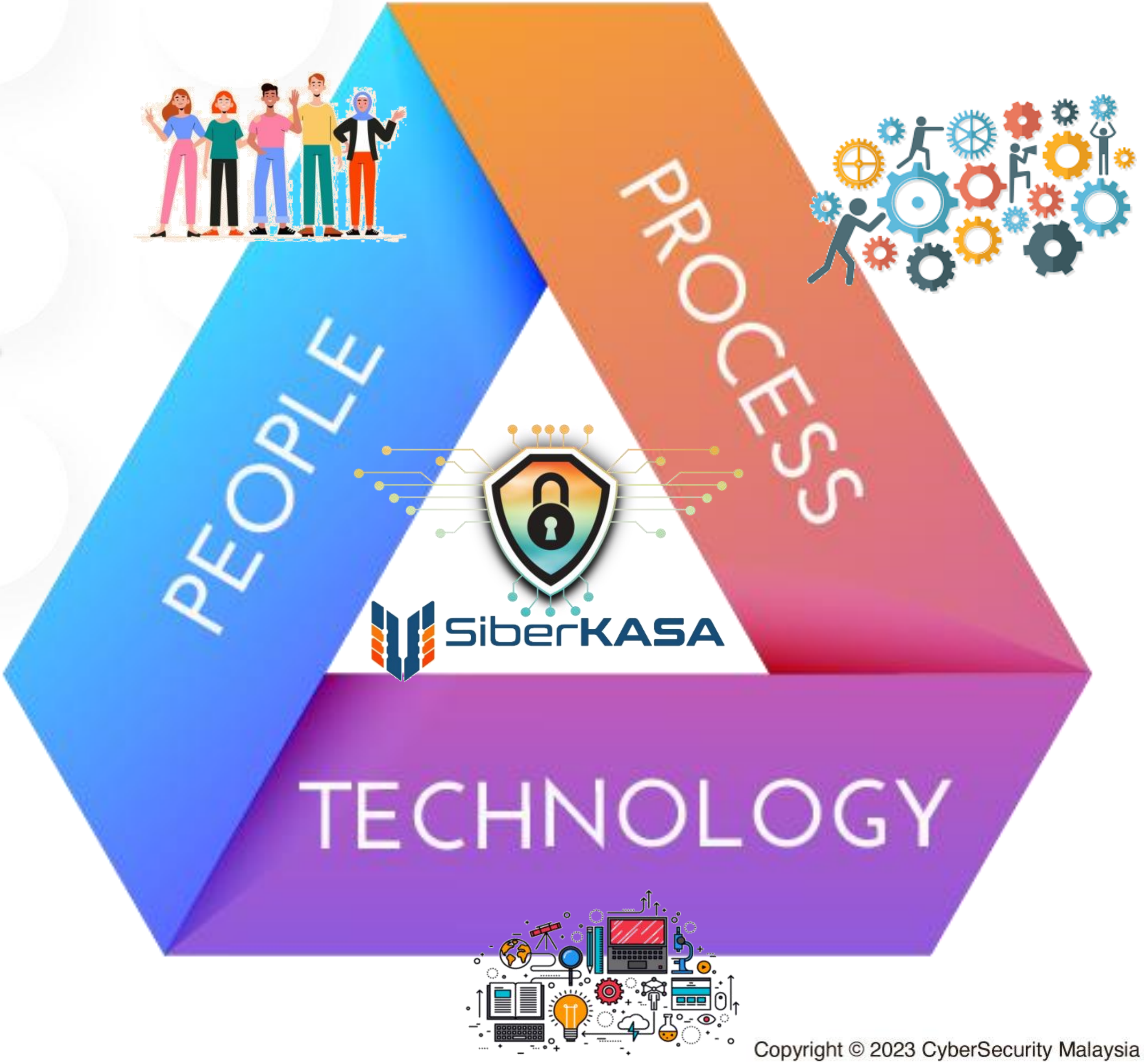


INISIATIF CYBERSECURITY MALAYSIA

PENDEKATAN HOLISTIK

- **Penerapan pendekatan holistik yang** mengenalpasti potensi ancaman kepada organisasi dan impak kepada keselamatan negara dan kesejahteraan awam

- Membangunkan keupayaan negara untuk mempunyai daya tahan siber **yang kukuh dan mempunyai** keupayaan untuk melindungi **pihak berkepentingan, reputasi dan aktiviti-aktiviti yang utama**



Copyright © 2023 CyberSecurity Malaysia

SiberKASA

(Program PemerKASAan Keselamatan Siber)

Objektif: Untuk membangun, memperkasa, mengukuh dan melestarikan prasarana serta ekosistem keselamatan siber negara agar sentiasa mampan, terpelihara dan berdaya tahan.

	HUMAN	PROCESS	TECHNOLOGY
	Covers aspects of skills, knowledge, ethics, behavior and talent	Covers aspects of policy development, strategy, Standard Operating Procedure (SOP), recognition of international standards	Involves technology in particular matters related to minimizing vulnerabilities, digital forensic analysis, malicious code (malware) and data
	PRODUCTS AND SERVICES		
PRODUCT	1. Global Accredited Cybersecurity Education (ACE)Scheme 2. CyberSAFE L.I.V.E Gallery	1. Information Security Governance, Risk & Compliance Health Check Assessment (ISGRiC) 2. ISMS Guidance Series 3. Information Security Management System(ISMS)	1. USB Secure Suite 2. Crypto Random test tool 3. X- Forensics Tools 4. Coordinated Malware Eradication and Remediation Platform (CMERP) 5. Lebahnet
SERVICE	1. CyberDrill Exercise 2. Behavioral Competency Assessment (BCA) 3. Cyber Safety Awareness for Everyone (CyberSAFE) 4. CyberSecurity Malaysia Awards, Conference & Exhibition (CSM-ACE) 5. Cyber Security Professional Development	1. Business Continuity Management System(BCMS) 2. MyCyberSecurity Clinic (MyCSC) - Data Recovery Service 3. DF Case Management System 4. Cyber Discovery 5. Mobile Incident Analysis (CyberDEF) 6. MyTrustSEAL 7. Technology Security Assurance (TSA) 8. ICT Product Security Assessment (IPSA) 9. Security Posture Assessment (SPA) 10. SCADA Security Assessment (SSA) 11. PHP Secure Code Assessment (PSCA) 12. Malaysian Common Criteria (MyCC)	1. MyCyberSecurity Clinic (MyCSC) - Data Sanitization Service 2. DF Lab Quality Management 3. Penetration Testing Service Provider (PTSP) 4. CyberSecurity Malaysia Crptographic Evaluation Lab (MyCEL) 5. CCTV Forensic readiness 6. Commercial Incident Respond Handling / Investigation (CyberDEF) 7. Backdoor Scanning 8. Cloud Security Compliance Audit 9. Cloud Security Assessment Audit 10. Cloud Security Audit for ISMS

Copyright © 2023 CyberSecurity Malaysia

Product security and ICT systems guarantee

Common Criteria

CyberDEF
Uncovering Future Threats

Teknologi

Proses

LAWS OF MALAYSIA

ACT 709
PERSONAL DATA PROTECTION ACT 2010

ISMS
Information Security Management System

Manusia

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

GLOBAL ACE
Global Accredited Cybersecurity Education (ACE) Scheme

CyberSAFE
Cyber Security Awareness For Everyone

SIBERKASA

PERTAHANAN BERLAPIS

Copyright © 2023 CyberSecurity Malaysia

RANGKA KERJA PEMBANGUNAN KAPASITI KESELAMATAN SIBER

GLOBAL ACE

Global Accredited Cybersecurity Education (ACE) Scheme

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

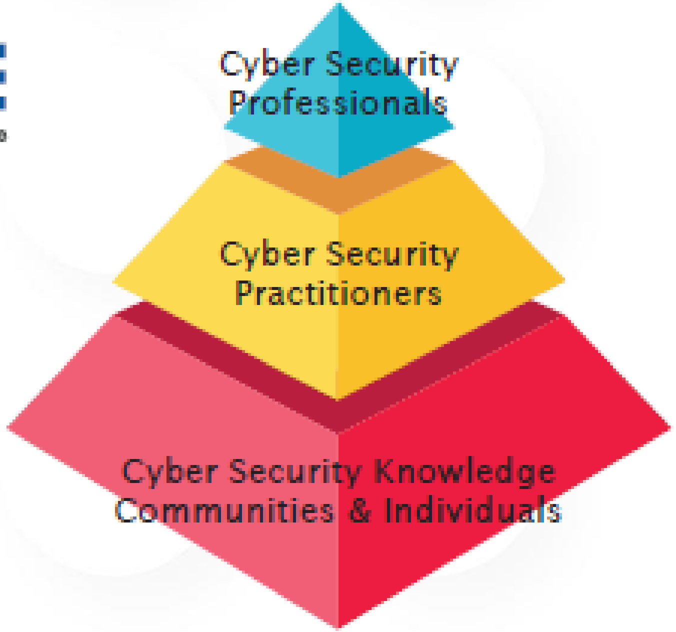
CyberGuru

CYBER SECURITY PROFESSIONAL DEVELOPMENT

Cyberguru
https://www.cyberguru.my

CyberSAFE™

Cybersafe
https://www.cybersafe.my



Cyber Security Professionals
Cyber Security Practitioners
Cyber Security Knowledge Communities & 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

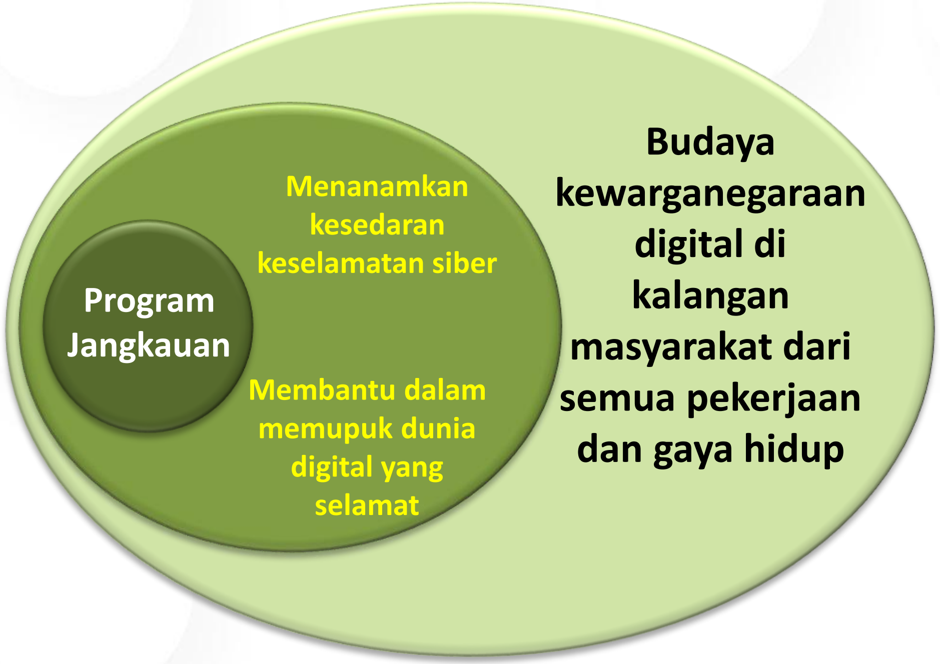
To nurture cyber security professionals that are capable in strategizing, planning and executing cyber security initiatives

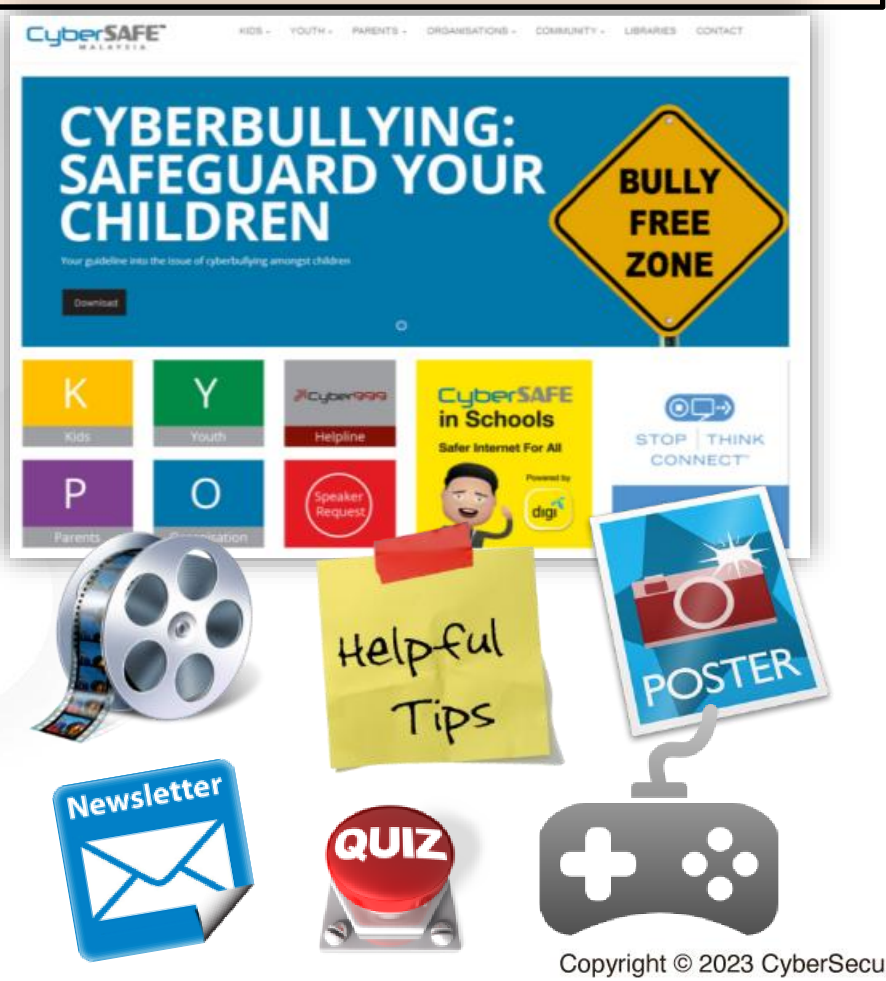
Copyright © 2023 CyberSecurity Malaysia

KESEDARAN KESELAMATAN SIBER MELALUI *CYBERSECURITY AWARENESS FOR EVERYONE* (CyberSAFE)

- **CyberSAFE** dilancarkan oleh **YAB Timbalan Perdana Menteri**
- Telah melibatkan **34,000** pelajar, pihak pengajar, para belia, dewasa dan lebih daripada **190** sekolah / organisasi.
- Program kesedaran yang dirujuk oleh **Australian Communications** dan **Media Authority**

Menjadi keutamaan untuk menyediakan maklumat, peralatan dan sumber-sumber yang relevan untuk meningkatkan tahap kesedaran nasional berkenaan kepentingan keselamatan siber


Program Jangkauan
Menanamkan kesedaran keselamatan siber
Membantu dalam memupuk dunia digital yang selamat
Budaya kewarganegaraan digital di kalangan masyarakat dari semua pekerjaan dan gaya hidup



Copyright © 2023 CyberSecurity Malaysia

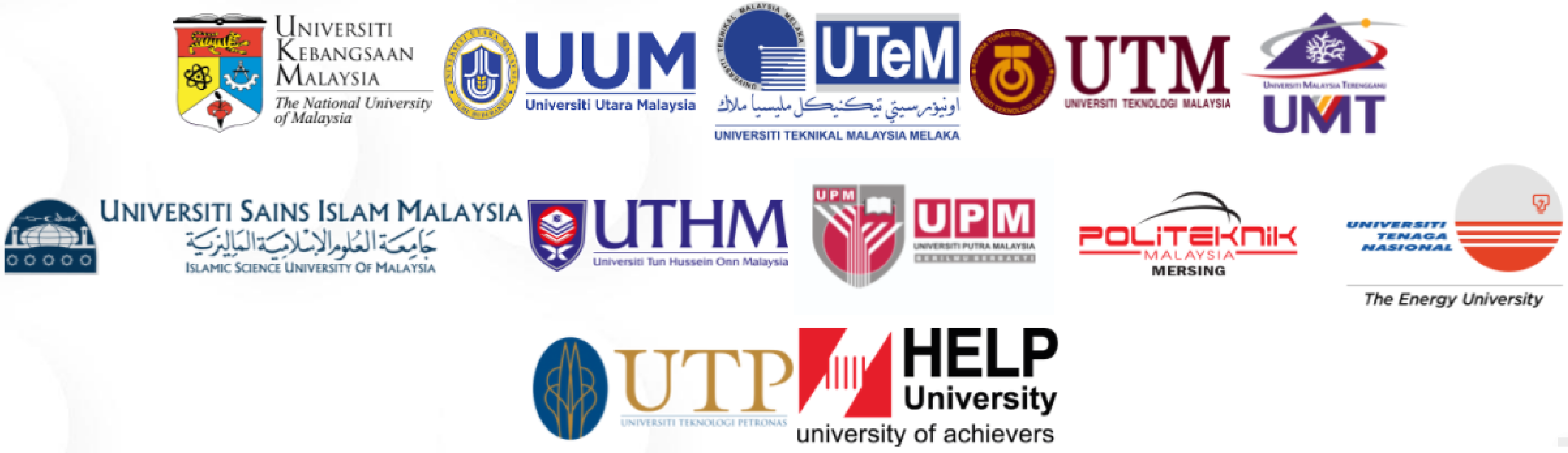
CyberGuru

CYBER SECURITY PROFESSIONAL DEVELOPMENT

Kerjasama Dalam Pembangunan Kapasiti Keselamatan Siber

CyberSecurity Malaysia menggabungkan program latihannya ke dalam program latihan tempatan dan antarabangsa terpilih serta bekerjasama rapat dengan rakan usaha sama industri untuk menambahbaik, menyampaikan dan memasarkan perkhidmatan ini dengan berkesan dan cekap.

Kerjasama Akademik Keselamatan Siber


Universiti Kebangsaan Malaysia
The National University of Malaysia
UUM
Universiti Utara Malaysia
UTeM
Universiti Teknikal Malaysia Melaka
UTM
Universiti Teknologi Malaysia
UMT
Universiti Malaysia Terengganu
Universiti Sains Islam Malaysia
Islamic Science University of Malaysia
UTHM
Universiti Tun Hussein Onn Malaysia
UPM
Universiti Putra Malaysia
Politeknik Malaysia Mersing
Universiti Tenaga Nasional
The Energy University
UTP
Universiti Teknologi Petronas
HELP University
university of achievers

Copyright © 2023 CyberSecurity Malaysia

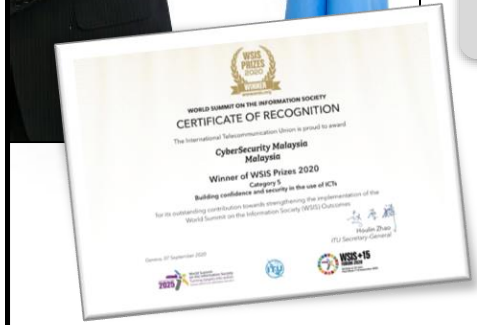
GLOBAL ACE CERTIFICATION

MATLAMAT & OBJEKTIF

MATLAMAT

Mewujudkan tenaga kerja kompeten bertaraf dunia dalam bidang keselamatan siber dan menggalakkan pembangunan program profesional keselamatan siber di rantau ini

Pensijilan Global ACE telah dipilih sebagai salah satu Projek Juara di bawah Kategori 5: Membina Keyakinan dan Keselamatan dalam Penggunaan ICT di WSIS Prizes 2020



WSIS PRIZES 2020 WINNER

WORLD SUMMIT ON THE INFORMATION SOCIETY

CERTIFICATE OF RECOGNITION

The International Telecommunication Union is proud to award

CyberSecurity Malaysia
Malaysia

Winner of WSIS Prizes 2020
Category 5
Building confidence and security in the use of ICTs

for its outstanding contribution towards strengthening the implementation of the World Summit on the Information Society (WSIS) Outcomes

Houlin Zhao
ITU Secretary-General

Geneva, 07 September 2020

OBJEKTIF

1 Mewujudkan program pensijilan profesional yang diiktiraf di peringkat global

2 Menyediakan profesional keselamatan siber dengan pengetahuan, kemahiran, sikap (KSA) dan pengalaman yang betul

3 Menggalakkan pembangunan program profesional keselamatan siber di peringkat global

4 Memastikan kakitangan bertauliah telah dinilai secara bebas dan komited kepada tahap perkhidmatan yang konsisten dan berkualiti tinggi

Copyright © 2023 CyberSecurity Malaysia

PROGRAM LATIHAN PENSIJILAN GLOBAL ACE

A. Currently running Global ACE Certification Programmes

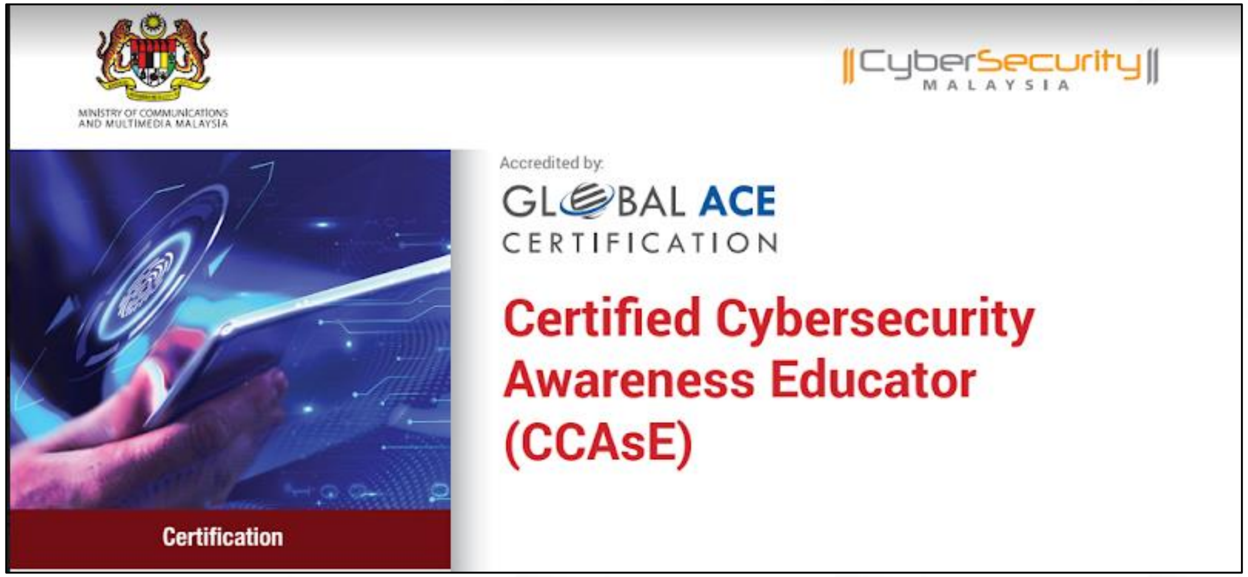
1. Certified Digital Forensics First Responder
2. Certified Information Security Management System Auditor
3. Certified Penetration Tester
4. Certified Secured Applications Practitioner
5. Certified Information Security Awareness Manager
6. Certified MyCC Evaluator
7. Certified Data Security Analyst
8. Certified IoT Security Analyst
9. Certified Cybersecurity Awareness Educator
10. Certified Security Operations Centre Analyst
11. Certified Incident Handling and Network Security Analyst
12. Certified IP Associate
13. Certified IT Associate
14. Certified Cybersecurity Data Science Analyst
15. Certified Mobile Security Analyst
16. Certified Cyber Law Practitioner
17. Certified Cybersecurity Risk Manager

B. Ready by 2023/2024

1. Certified Industrial Control System Security Analyst
2. Certified Secure Web Application (PHP) Developer
3. Certified Smart Card Reader Analyst
4. Certified Cloud Security Auditor
5. Certified IoT Blockchain Practitioner
6. Certified Cyber Forensics Analyst
7. Certified Web Application Penetration Tester
8. Certified Data Privacy Officer
9. Certified Data Privacy Specialist
10. Certified Chief Data Privacy Officer
11. Certified Cryptocurrency Seizing Officer

Copyright © 2023 CyberSecurity Malaysia

Brosur Pensijilan Global ACE AND CyberGURU



MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

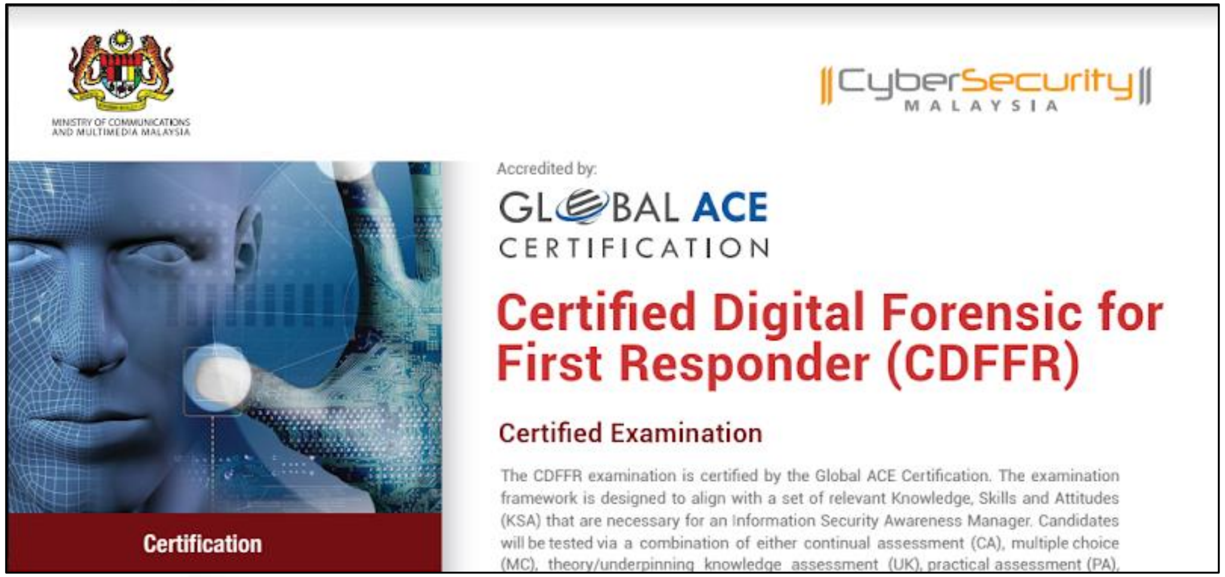
CyberSecurity MALAYSIA

Accredited by:

GLOBAL ACE CERTIFICATION

Certified Cybersecurity Awareness Educator (CCAsE)

Certification



MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

Accredited by:

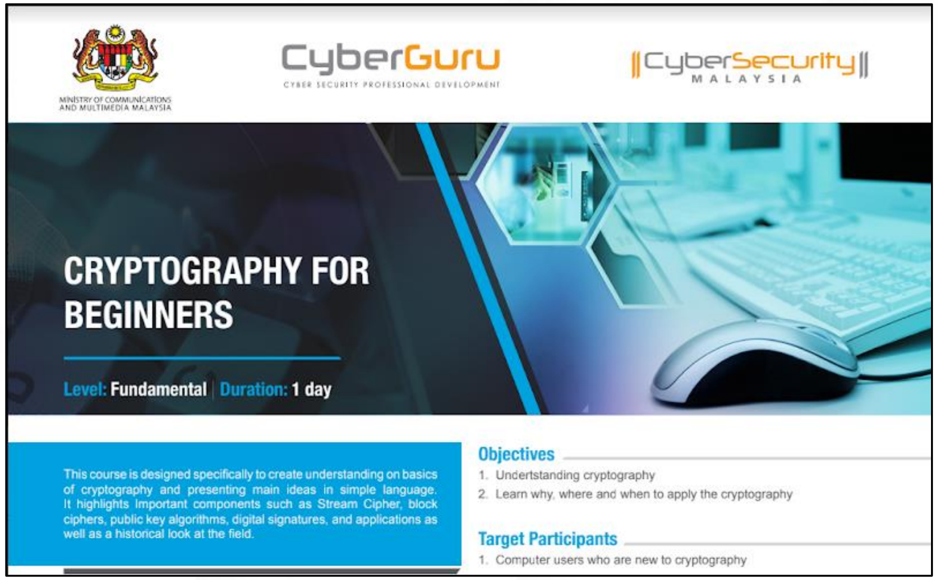
GLOBAL ACE CERTIFICATION

Certified Digital Forensic for First Responder (CDFFR)

Certification

Certified Examination

The CDFFR examination is certified by the Global ACE Certification. The examination framework is designed to align with a set of relevant Knowledge, Skills and Attitudes (KSA) that are necessary for an Information Security Awareness Manager. Candidates will be tested via a combination of either continual assessment (CA), multiple choice (MC), theory/underpinning knowledge assessment (UK), practical assessment (PA),



MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberGuru CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

CRYPTOGRAPHY FOR BEGINNERS

Level: Fundamental | Duration: 1 day

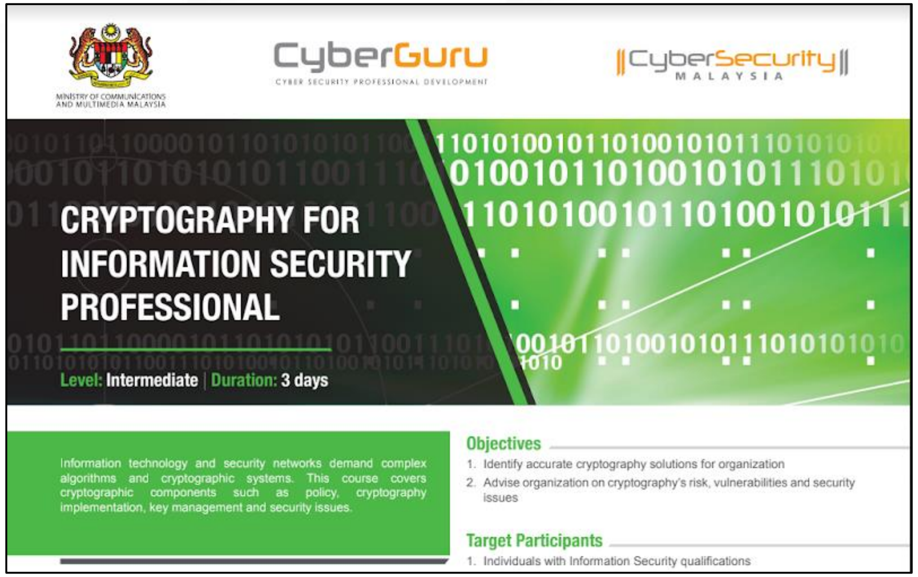
This course is designed specifically to create understanding on basics of cryptography and presenting main ideas in simple language. It highlights Important components such as Stream Cipher, block ciphers, public key algorithms, digital signatures, and applications as well as a historical look at the field.

Objectives

1. Undertstanding cryptography
2. Learn why, where and when to apply the cryptography

Target Participants

1. Computer users who are new to cryptography



MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberGuru CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

CRYPTOGRAPHY FOR INFORMATION SECURITY PROFESSIONAL

Level: Intermediate | Duration: 3 days

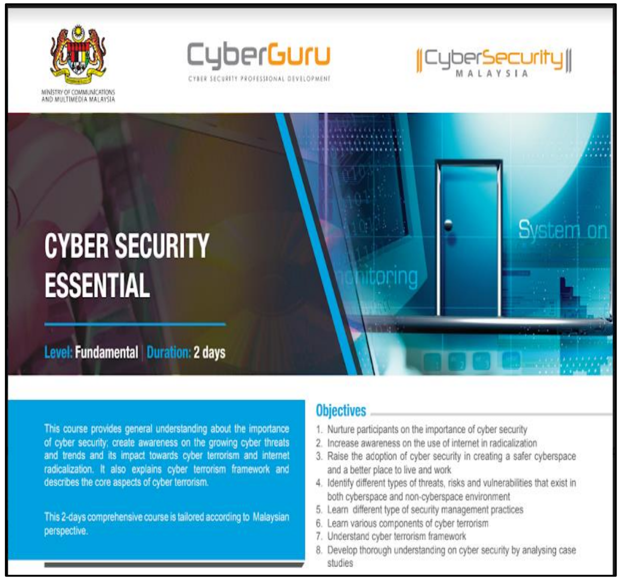
Information technology and security networks demand complex algorithms and cryptographic systems. This course covers cryptographic components such as policy, cryptography implementation, key management and security issues.

Objectives

1. Identify accurate cryptography solutions for organization
2. Advise organization on cryptography's risk, vulnerabilities and security issues

Target Participants

1. Individuals with Information Security qualifications



MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberGuru CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

CYBER SECURITY ESSENTIAL

Level: Fundamental | Duration: 2 days

This course provides general understanding about the importance of cyber security; create awareness on the growing cyber threats and trends and its impact towards cyber terrorism and internet radicalization. It also explains cyber terrorism framework and describes the core aspects of cyber terrorism.

This 2-days comprehensive course is tailored according to Malaysian perspective.

Objectives

1. Nurture participants on the importance of cyber security
2. Increase awareness on the use of internet in radicalization
3. Raise the adoption of cyber security in creating a safer cyberspace and a better place to live and work
4. Identify different types of threats, risks and vulnerabilities that exist in both cyberspace and non-cyberspace environment
5. Learn different type of security management practices
6. Learn various components of cyber terrorism
7. Understand cyber terrorism framework
8. Develop thorough understanding on cyber security by analysing case studies

CYBER SECURITY MODULAR CERTIFICATION

MODULAR PROFESSIONAL CERTIFICATION

CyberSecurity Malaysia bersama Jabatan Pembangunan Kemahiran Malaysia (JPK) dan Lembaga Teknologis Malaysia (MBOT) telah memulakan projek untuk mengintegrasikan Global ACE Certification dan latihan TVET ke dalam projek sulung yang dikenali sebagai Pensijilan Profesional Modular Keselamatan Siber melalui National Occupational Skills Standard (NOSS).

JABATAN PEMBANGUNAN KEMAHIRAN (JPK)
KEMENTERIAN SUMBER MANUSIA

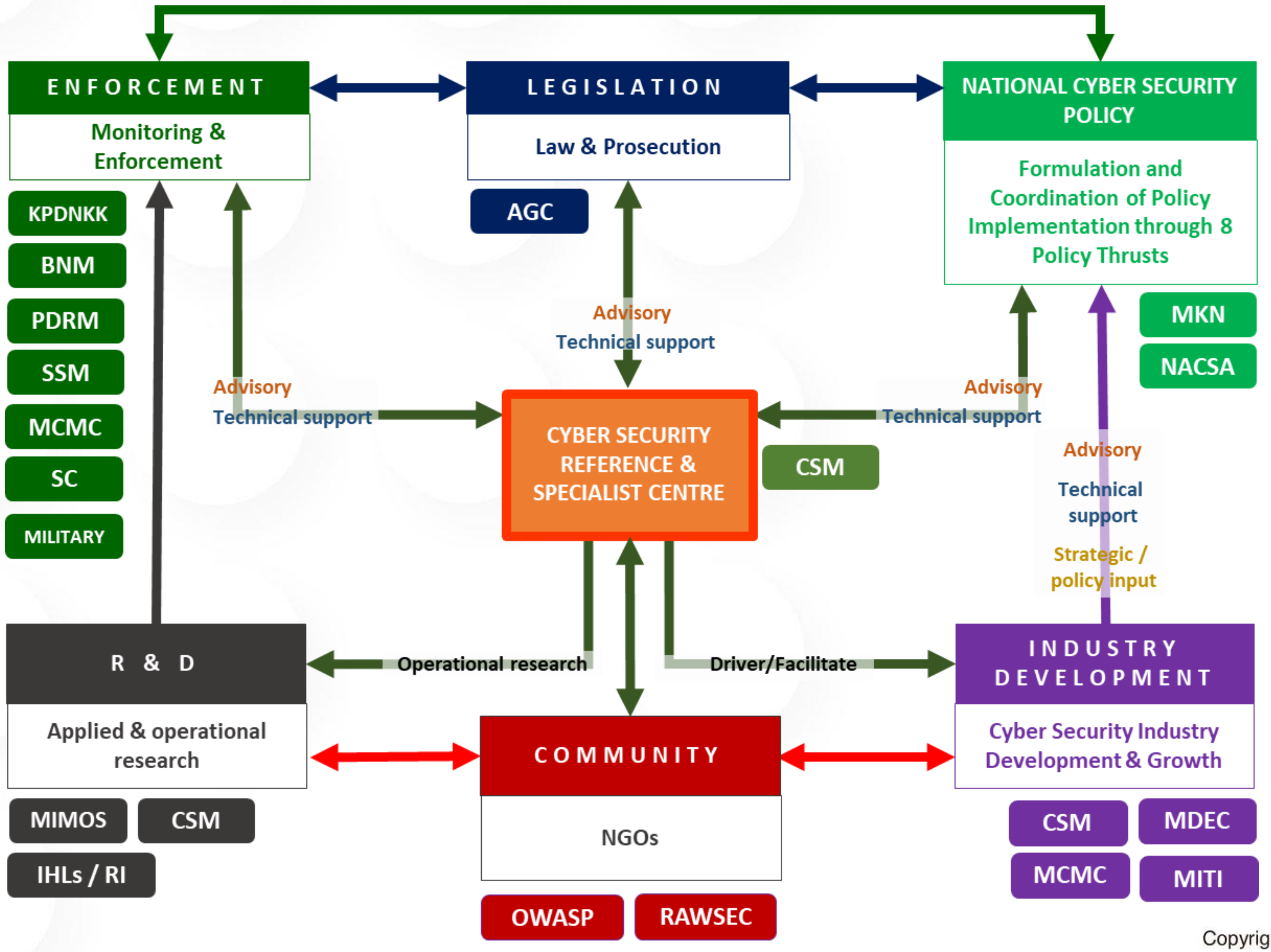
MBOT
LEMBAGA TEKNOLOGIS MALAYSIA
MALAYSIA BOARD OF TECHNOLOGY

Copyright © 2023 CyberSecurity Malaysia

PROSES

SiberKASA

EKOSISTEM CYBERSECURITY MALAYSIA



ENFORCEMENT

Monitoring & Enforcement

KPDNKK

BNM

PDRM

SSM

MCMC

SC

MILITARY

LEGISLATION

Law & Prosecution

AGC

NATIONAL CYBER SECURITY POLICY

Formulation and Coordination of Policy Implementation through 8 Policy Thrusts

MKN

NACSA

Advisory

Technical support

Advisory

Technical support

Advisory

Technical support

CYBER SECURITY REFERENCE & SPECIALIST CENTRE

CSM

Advisory

Technical support

Strategic / policy input

R & D

Applied & operational research

MIMOS

CSM

IHLs / RI

Operational research

Driver/Facilitate

COMMUNITY

NGOs

OWASP

RAWSEC

INDUSTRY DEVELOPMENT

Cyber Security Industry Development & Growth

CSM

MDEC

MCMC

MITI

Copyright © 2023 CyberSecurity Malaysia

Ministries of Communication and Multimedia Strategic Framework

Strategic Thrust 2:
Driving the Digital Economy and IT Towards Developed Countries

Strategic Thrust 3:
Strengthen the regulation of a reliable and stable communications and multimedia ecosystem

12TH Malaysia Plan (RMK-12)

Pillar 1: Source of Growth

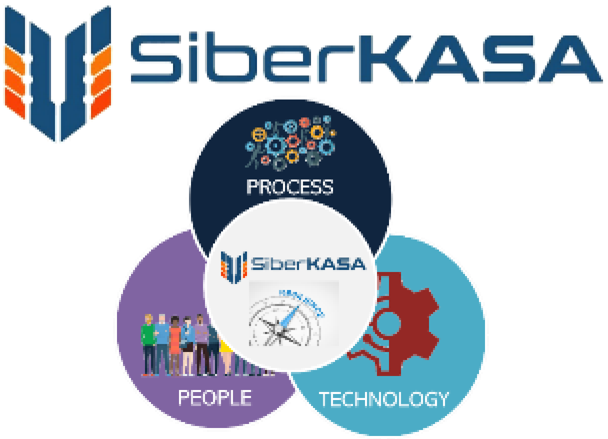
Pillar 4: Human Capital Transformation and Market Strengthening Labor:

Pillar 5: Inclusivity and People's Well being

Pillar 6: Institutional Reform

Pillar 7: Social Capital

Peranan CSM dalam **Menyokong** Polisi & Pelan Strategik Berkaitan Keselamatan Siber Negara



Agensi Keselamatan Siber Teknikal Kebangsaan bertanggungjawab untuk **menasihati & melaksanakan** program berkaitan keselamatan siber

Malaysia Digital Economy Blueprint

Thrust 1: Drive digital transformation in the public sector

Thrust 4: Build agile and competent digital talent

Thrust 6: Build trusted, secure and ethical digital environment

Malaysia Cyber Security Strategy

Pillar 1: Effective Governance and Management

Pillar 2: Strengthening Legislative Framework and Enforcement

Pillar 3: Catalysing World Class Innovation, Technology, R&D and Industry

Pillar 4: Enhancing Capacity and Capability Building, Awareness and Education

Pillar 5: Strengthening Global Collaboration

National 4th Industrial Revolution Policy (N4IR)

Thrust 1:
Equip the Rakyat with 4IR knowledge and skill sets

Thrust 3:
Future-proof regulations to be agile with technological changes

MENANGANI KESELAMATAN SIBER MELALUI POLISI

STRATEGI KESELAMATAN SIBER MALAYSIA

CYBER SECURITY STRATEGY

5 TONGGAK

12 Strategi

CyberSecurity MALAYSIA

1

Effective Governance and Management

- Enhancing National Cyber Security Governance and Ecosystem
- Improving Organization Management and Business Operation (Government, CNII and Business)
- Strengthening Cyber Security Incident Management and Active Cyber Defence

2

Strengthening Legislative Framework and Enforcement

- Enhancing Malaysia's Cyber Laws to Address Current and Emerging Threats
- Enhancing the Capacity and Capability of Cybercrime Enforcement

3

Catalyzing World Class Innovation, Technology, R&D and Industry

- Spurring National Cyber Security R&D Programmed
- Promoting a Competitive Local Industry and Technology

4

Enhancing Capacity & Capability Building, Awareness and Education

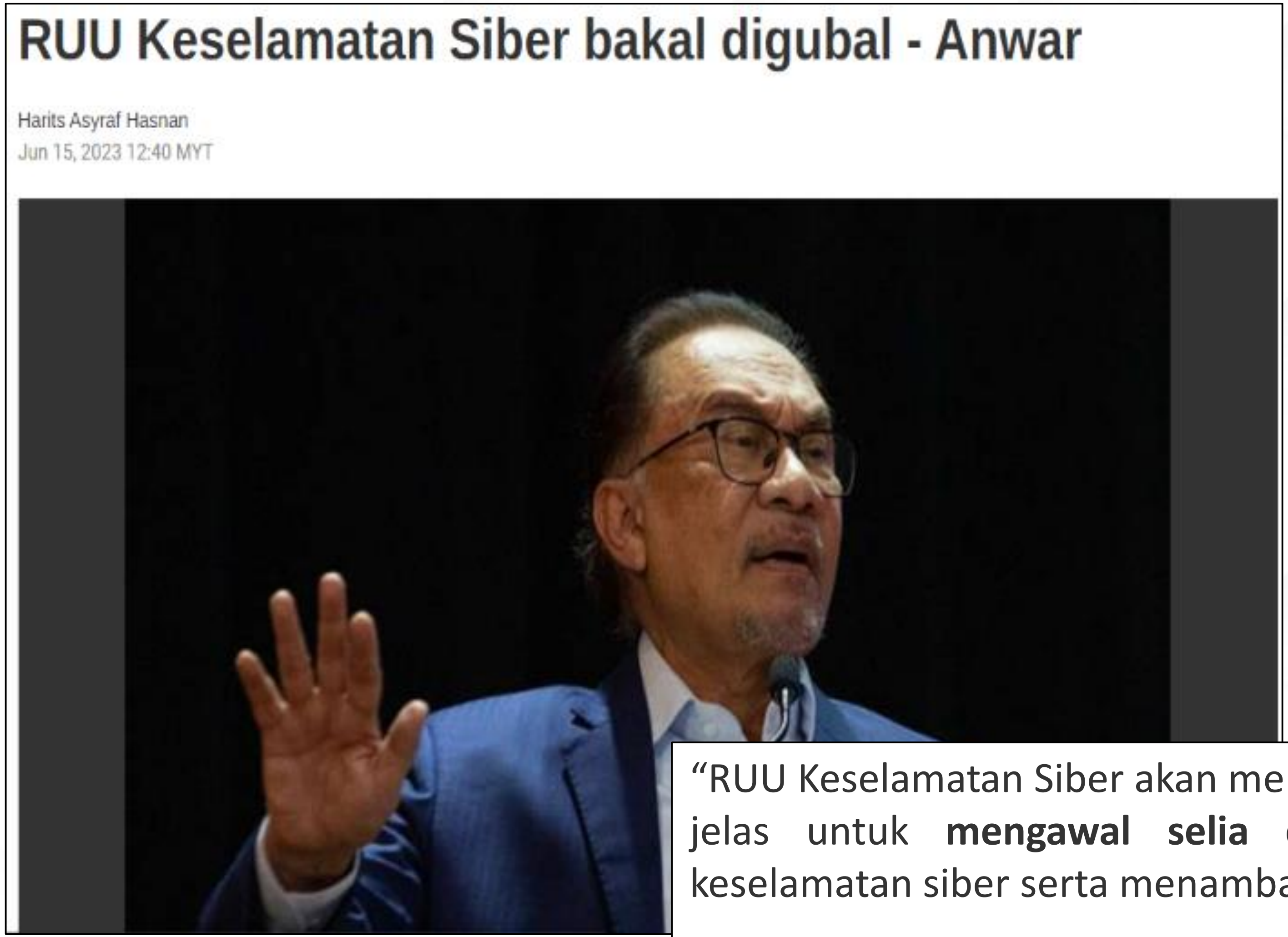
- Enhancing National Cyber Security Capacity and Capability Building
- Enhancing Cyber Security Awareness
- Nourishing Cyber Security Knowledge Through Education

5

Strengthening Global Collaboration

- Strengthening International Collaboration and Cooperation in Cyber Security Affairs
- Demonstrating Malaysia's Commitment in Promoting Secure, Stable and Peaceful Cyberspace to Uphold International Security

RANG UNDANG-UNDANG KESELAMATAN SIBER



RUU Keselamatan Siber bakal digubal - Anwar

Harits Asyraf Hasnan
Jun 15, 2023 12:40 MYT

Memperkukuhkan perundangan dan penguatkuasaan berkaitan keselamatan dan jenayah siber

- Mempertingkatkan Undang-undang Siber Malaysia untuk Menangani Ancaman Semasa dan Ancaman Muncul
- Meningkatkan Kapasiti dan Keupayaan Penguatkuasaan Jenayah Siber

“RUU Keselamatan Siber akan memberi NACSA, MKN punca kuasa undang-undang yang jelas untuk **mengawal selia dan menguatkuasakan undang-undang** berkaitan keselamatan siber serta menambah baik **keberkesanan fungsi-fungsi NACSA, MKN**

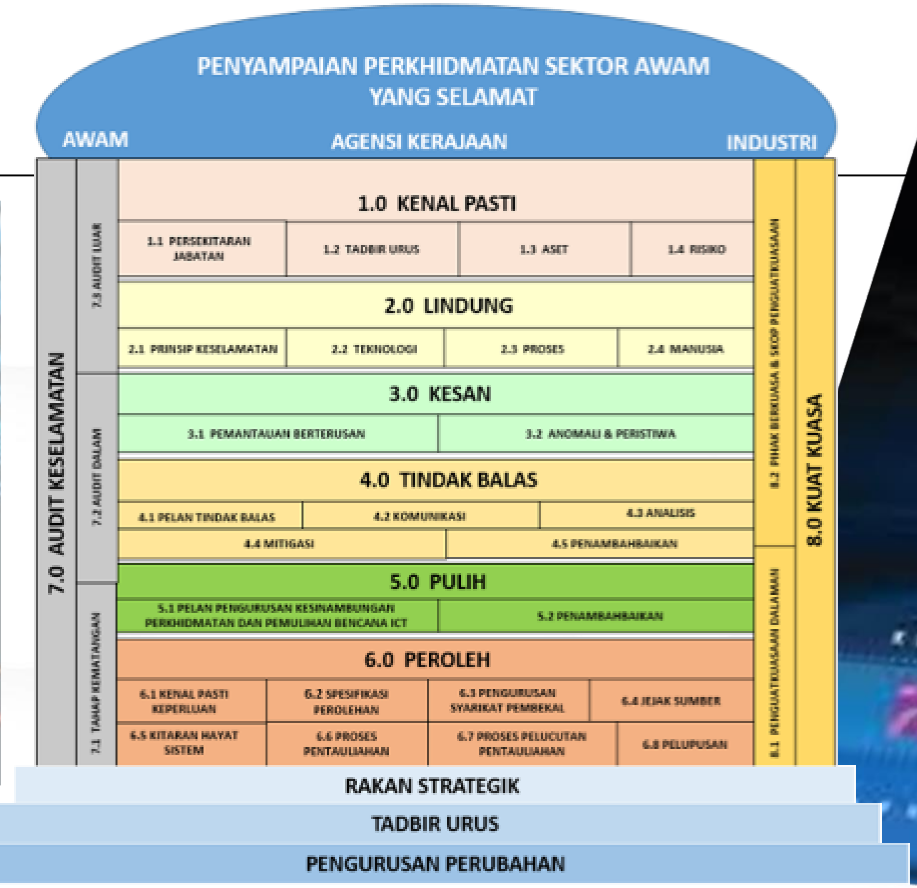
Sejajar dengan hasrat yang termaktub dalam **Arahan MKN No. 26 Pengurusan Keselamatan Siber Negara dan Strategi Keselamatan Siber Malaysia (Malaysia Cyber Security Strategy, MCSS)**” – Perdana Menteri Malaysia ke-10

Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)

MAMPU komited usaha digitalisasi sektor awam melalui data raya

Ehsan A Marisah

November 10, 2021 15:07 MYT



PENYAMPAIAN PERKHIDMATAN SEKTOR AWAM YANG SELAMAT

AWAM | AGENSI KERAJAAN | INDUSTRI

7.0 AUDIT KESELAMATAN

7.3 AUDIT LUAR

7.2 AUDIT DALAM

7.1 TAHAP KEMATANGAN

1.0 KENAL PASTI

1.1 PERSEKITARAN JABATAN | 1.2 TADBIR URUS | 1.3 ASET | 1.4 RISIKO

2.0 LINDUNG

2.1 PRINSIP KESELAMATAN | 2.2 TEKNOLOGI | 2.3 PROSES | 2.4 MANUSIA

3.0 KESAN

3.1 PEMANTAUAN BERTERUSAN | 3.2 ANOMALI & PERISTIWA

4.0 TINDAK BALAS

4.1 PELAN TINDAK BALAS | 4.2 KOMUNIKASI | 4.3 ANALISIS

4.4 MITIGASI | 4.5 PENAMBAHBAIKAN

5.0 PULIH

5.1 PELAN PENGURUSAN KESINAMBUNGAN PERKHIDMATAN DAN PEMULIHAN BENCANA ICT | 5.2 PENAMBAHBAIKAN

6.0 PEROLEH

6.1 KENAL PASTI KEPERLUAN | 6.2 SPESIFIKASI PEROLEHAN | 6.3 PENGURUSAN SYARIKAT PEMBEKAL | 6.4 JEJAK SUMBER

6.5 KITARAN HAYAT SISTEM | 6.6 PROSES PENTAULIAHAN | 6.7 PROSES PELUCUTAN PENTAULIAHAN | 6.8 PELUPUSAN

8.0 KUAT KUASA

8.2 PIHAK BERKUASA & SKOP PENGUATKUASAAN

8.1 PENGUATKUASAAN DALAMAN

RAKAN STRATEGIK

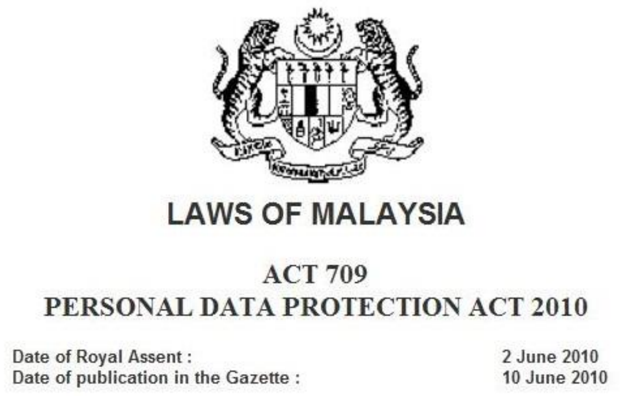
TADBIR URUS

PENGURUSAN PERUBAHAN

RAKKSSA
RANGKA KERJA KESELAMATAN SIBER SEKTOR AWAM
KERJASAMA RAKAN STRATEGIK
APRIL 2016, VERSI 1.0

Security Malaysia

AKTA PERLINDUNGAN DATA PERIBADI 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

01 **Memudahkan urusniaga perniagaan / e-dagang / ekonomi digital**

02 **Merangsang dan meningkatan kepercayaan – berintegriti dalam mengendalikan data peribadi**

03 **Mengelakkan penyalahgunaan data peribadi dan data peribadi sensitif**

04 **Memposisikan Malaysia sebagai sebuah negara di dunia yang menguatkuasakan perundangan perlindungan data peribadi yang kukuh**

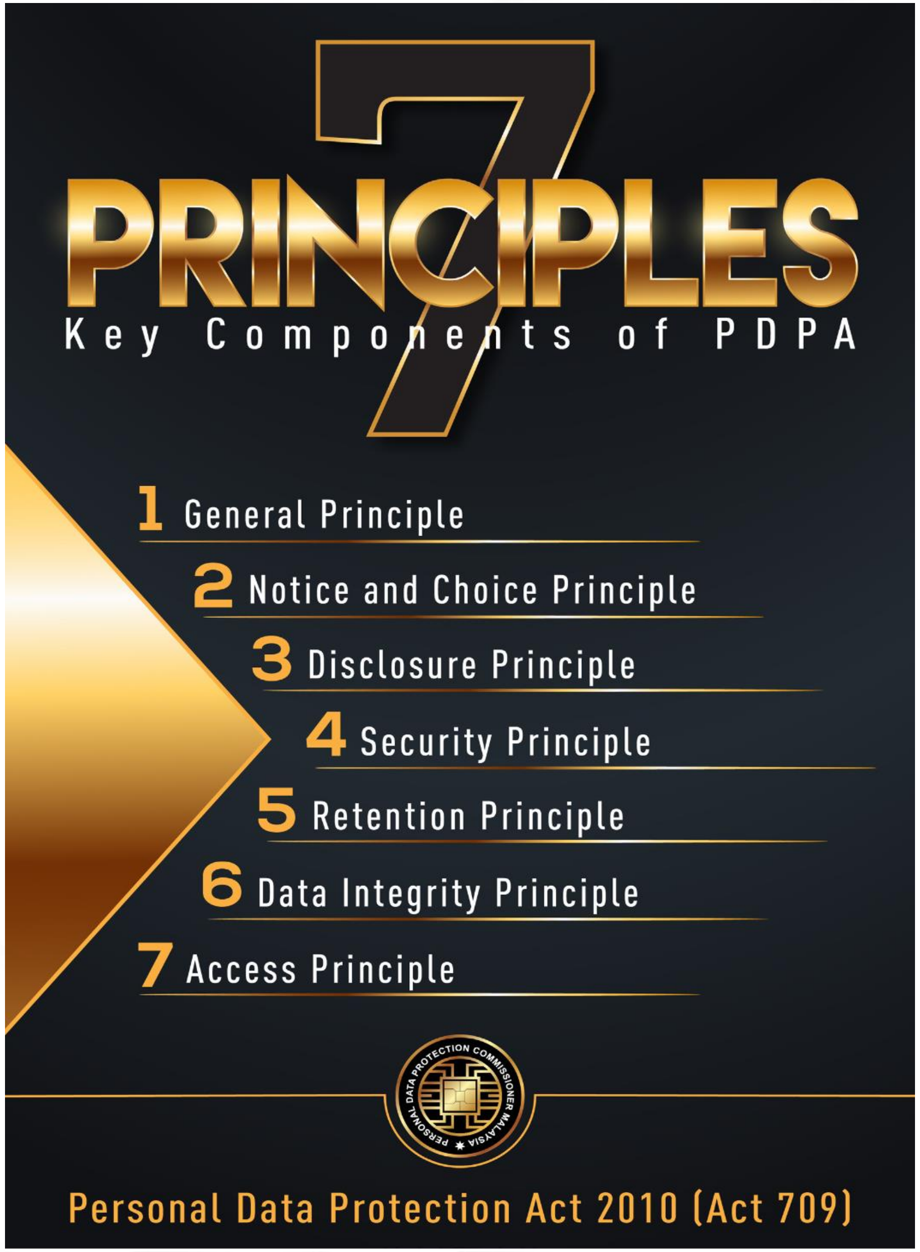
Isu dan cabaran berkaitan Akta Perlindungan Data Peribadi (PDPA) 2010

- Hanya melindungi daripada salah guna penggunaan data peribadi untuk tujuan komersial sahaja.
- Tidak mempunyai peruntukan yang khusus menangani isu dalam talian, yang termasuk data seperti geolokasi dan cookies.
- Tidak boleh digunakan jika data peribadi diproses di luar Malaysia.
- Ketinggalan di belakang perlindungan data dan inisiatif pengawalseliaan yang serupa di tempat lain seperti GDPR.

Usaha Untuk Pindaan Akta PDPA 2010 Sedang Dilaksanakan Oleh JPDP/KKD

Copyright © 2023 CyberSecurity Malaysia

AKTA PERLINDUNGAN DATA PERIBADI 2010(PDPA)



7 PRINCIPLES

Key Components of PDPA

1 General Principle

2 Notice and Choice Principle

3 Disclosure Principle

4 Security Principle

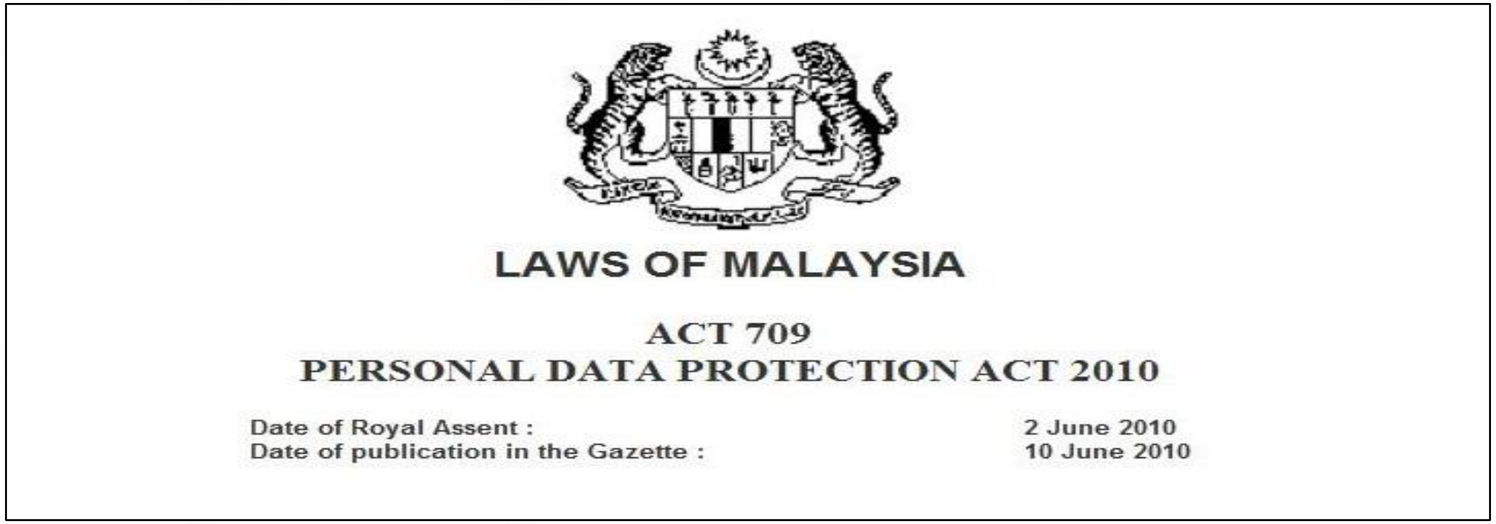
5 Retention Principle

6 Data Integrity Principle

7 Access Principle

PERSONAL DATA PROTECTION COMMISSIONER MALAYSIA

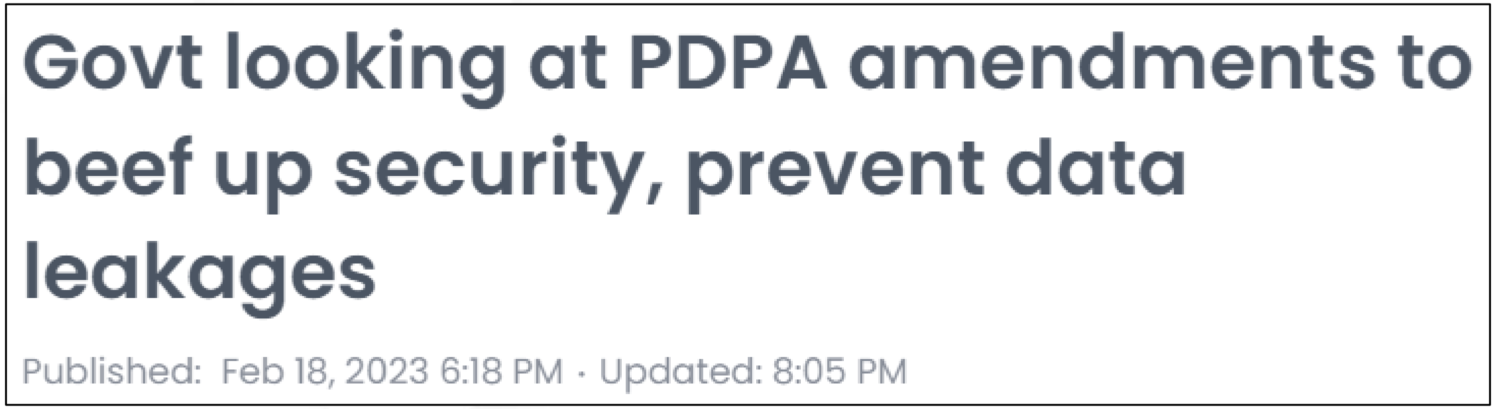
Personal Data Protection Act 2010 (Act 709)



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



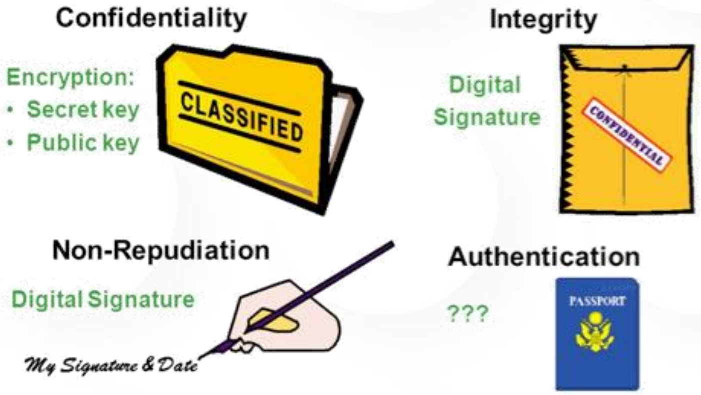
Govt looking at PDPA amendments to beef up security, prevent data leakages

Published: Feb 18, 2023 6:18 PM · Updated: 8:05 PM

CyberSecurity Malaysia Turut Bekerjasama Dengan Jabatan Perlindungan Data Peribadi (PDPD) Untuk Memperkasakan Perlindungan Data

Copyright © 2023 CyberSecurity Malaysia

MENGATASI PERLINDUNGAN DATA DAN KETAHANAN SIBER MELALUI TEKNOLOGI ENKRIPSI



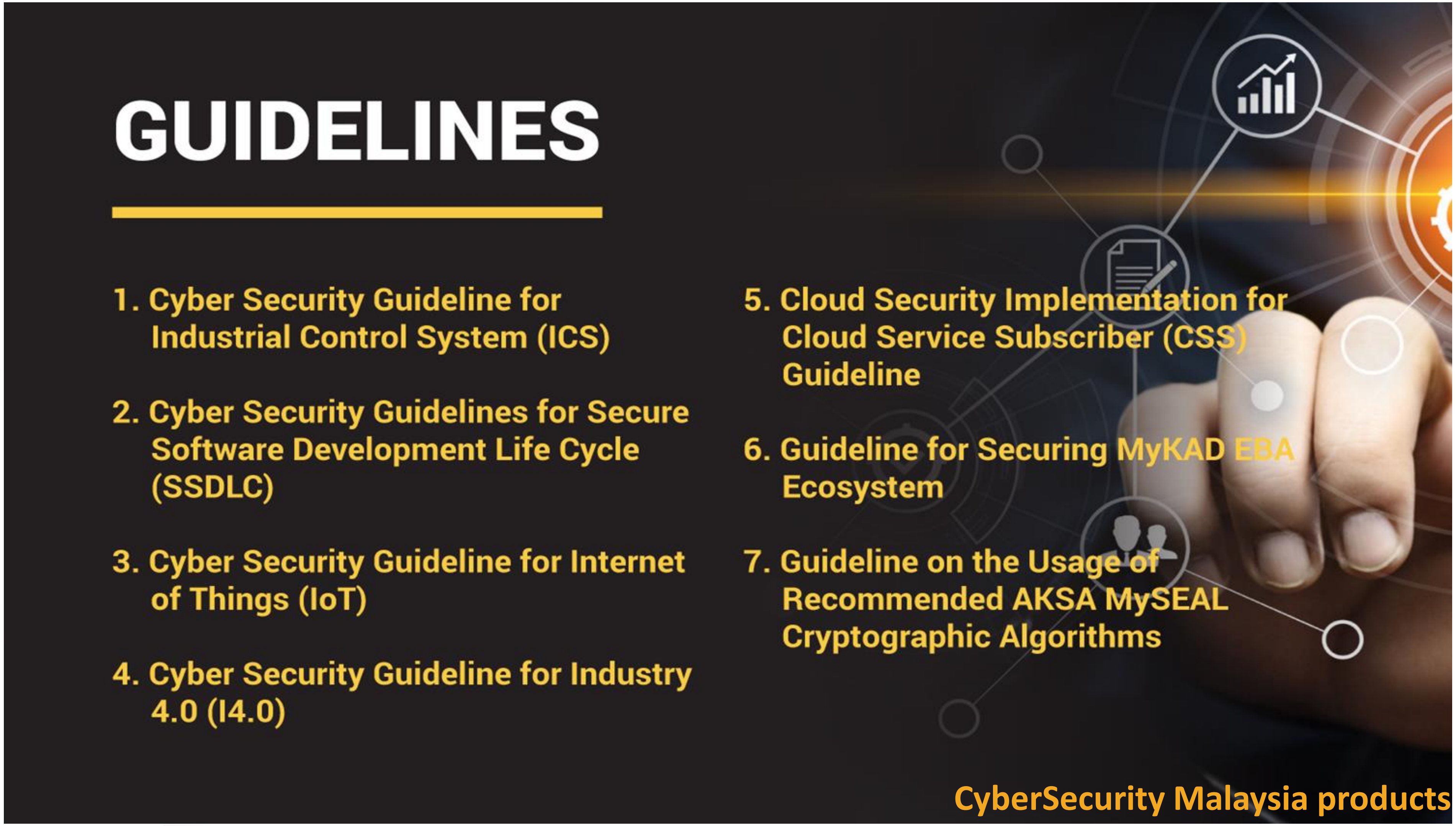
- **Dasar Kriptografi Negara** telah diluluskan oleh pihak Kerajaan pada Januari 2013

- Terdapat aplikasi kriptografi yang komprehensif dalam Kerajaan ke Kerajaan (G2G), Kerajaan ke Warganegara (G2C), Kerajaan ke Perniagaan (G2B) dan Perniagaan ke Perniagaan (B2B) ke arah memastikan persekitaran siber yang selamat dan dipercayai

- Kriptografi juga menyokong Ekonomi Digital Nasional dan merealisasikan Agenda Transformasi Nasional untuk mengubah Malaysia menjadi negara maju dan berpendapatan tinggi

Copyright © 2023 CyberSecurity Malaysia

MENANGANI PERLINDUNGAN DATA MELALUI GARIS PANDUAN KESELAMATAN SIBER



GUIDELINES

1. Cyber Security Guideline for Industrial Control System (ICS)
2. Cyber Security Guidelines for Secure Software Development Life Cycle (SSDLC)
3. Cyber Security Guideline for Internet of Things (IoT)
4. Cyber Security Guideline for Industry 4.0 (I4.0)
5. Cloud Security Implementation for Cloud Service Subscriber (CSS) Guideline
6. Guideline for Securing MyKAD EBA Ecosystem
7. Guideline on the Usage of Recommended AKSA MySEAL Cryptographic Algorithms

CyberSecurity Malaysia products

Copyright © 2023 CyberSecurity Malaysia

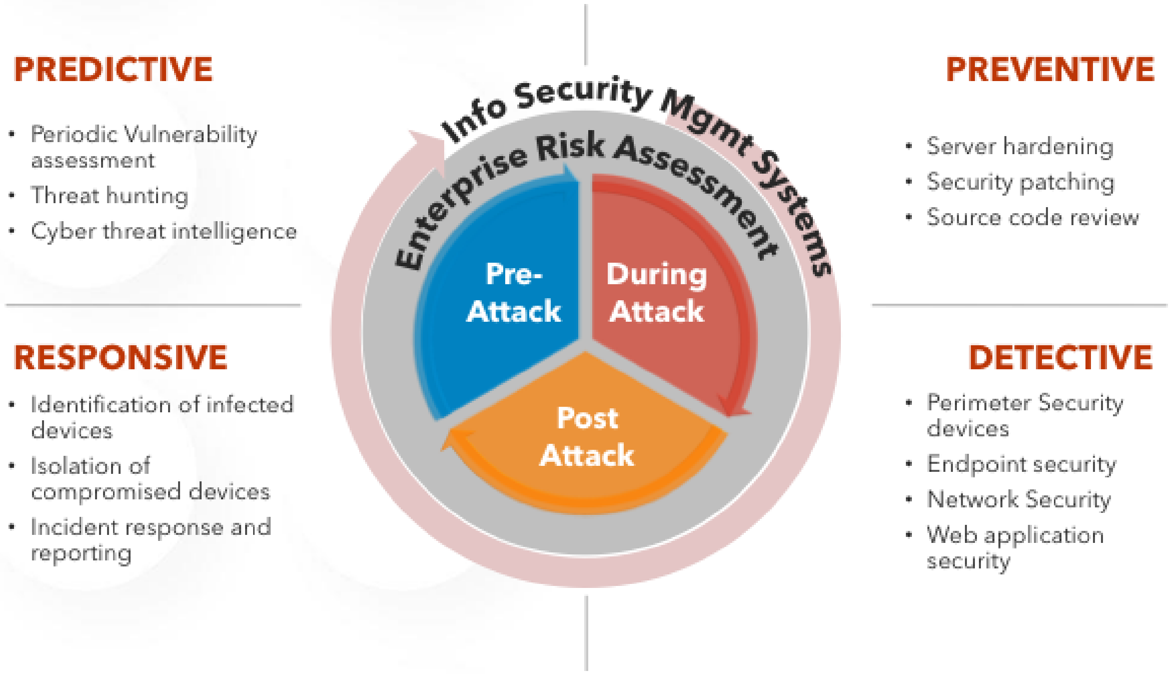
TEKNOLOGI

SiberKASA

KETAHANAN SIBER MELALUI **KESELAMATAN ADAPTIF**

Menjadi lebih proaktif, dinamik and pendekatan keselamatan siber yang lebih bersepadu

Keselamatan adaptif adalah keselamatan siber yang **menganalisis tingkah laku dan insiden** untuk melindungi dan menyesuaikan diri dengan ancaman sebelum ia berlaku. Dengan Senibina Keselamatan Adaptif, sebuah organisasi perlu **terus menilai risiko dan secara automatik memberikan penguatkuasaan**



PREDICTIVE

- Periodic Vulnerability assessment
- Threat hunting
- Cyber threat intelligence

PREVENTIVE

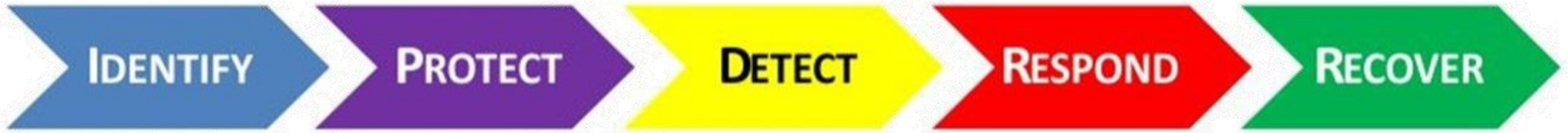
- Server hardening
- Security patching
- Source code review

RESPONSIVE

- Identification of infected devices
- Isolation of compromised devices
- Incident response and reporting

DETECTIVE

- Perimeter Security devices
- Endpoint security
- Network Security
- Web application security



Kos organisasi ada pada setiap tahap dalam kitaran insiden tindak balas — **pengesanan, notifikasi, tindak balas, pasca insiden**, dan kos kerugian perniagaan.

Copyright © 2023 CyberSecurity Malaysia

MENANGANI DAYA TAHAN SIBER MELALUI TEKNOLOGI DAN PERKHIDMATAN RESPONSIF CYBERSECURITY MALAYSIA

MyCERT

Malaysia Computer Emergency Response Team

Cyber999

Cyber999 Help Centre

Cyber Threat Research Centre (CTRC)

CMERP

Detection | Eradication | Remediation

Coordinated Malware Eradication & Remediation Project (CMERP)

MyCERT

MASSA

LebahNET.MY

CyberSecurity Honeynet Project

Lebahnet (Honeynet Project)

Computer Security Incident Response Team (CSIRT) Consultancy

DIGITAL FORENSIC (DF)

CyberDiscovery

CyberCSI

crime scene investigation

CyberDEF

Uncovering Future Threats

Cyber Detect, Eradicate and Forensics (CyberDEF)

X-Forensics Tools

PenDua

x-Forensik 2.0

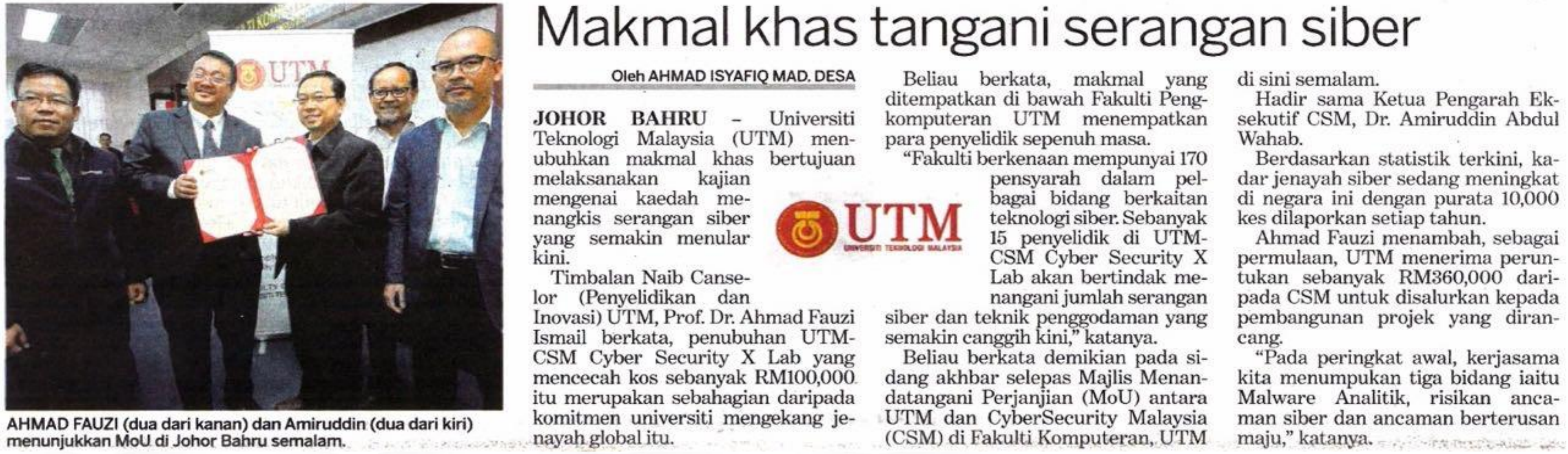
Kloner

x-Forensik 2.0

CamMuka V2.0

Copyright © 2023 CyberSecurity Malaysia

MENGUATKAN PERLINDUNGAN DATA MELALUI KECERDASAN ANCAMAN SIBER PREDIKTIF



Makmal khas tangani serangan siber

Oleh AHMAD ISYAFIQ MAD. DESA

JOHOR BAHRU – Universiti Teknologi Malaysia (UTM) menubuhkan makmal khas bertujuan melaksanakan kajian mengenai kaedah menangkis serangan siber yang semakin menular kini.

Timbalan Naib Canselor (Penyelidikan dan Inovasi) UTM, Prof. Dr. Ahmad Fauzi Ismail berkata, penubuhan UTM-CSM Cyber Security X Lab yang mencecah kos sebanyak RM100,000 itu merupakan sebahagian daripada komitmen universiti mengekang jenayah global itu.

Beliau berkata, makmal yang ditempatkan di bawah Fakulti Pengkomputeran UTM menempatkan para penyelidik sepenuh masa.

"Fakulti berkenaan mempunyai 170 pensyarah dalam pelbagai bidang berkaitan teknologi siber. Sebanyak 15 penyelidik di UTM-CSM Cyber Security X Lab akan bertindak menangani jumlah serangan siber dan teknik penggodaman yang semakin canggih kini," katanya.

Beliau berkata demikian pada sidang akhbar selepas Majlis Menandatangani Perjanjian (MoU) antara UTM dan CyberSecurity Malaysia (CSM) di Fakulti Komputeran, UTM di sini semalam.

Hadir sama Ketua Pengarah Eksekutif CSM, Dr. Amiruddin Abdul Wahab.

Berdasarkan statistik terkini, kadar jenayah siber sedang meningkat di negara ini dengan purata 10,000 kes dilaporkan setiap tahun.

Ahmad Fauzi menambah, sebagai permulaan, UTM menerima peruntukan sebanyak RM360,000 daripada CSM untuk disalurkan kepada pembangunan projek yang dirancang.

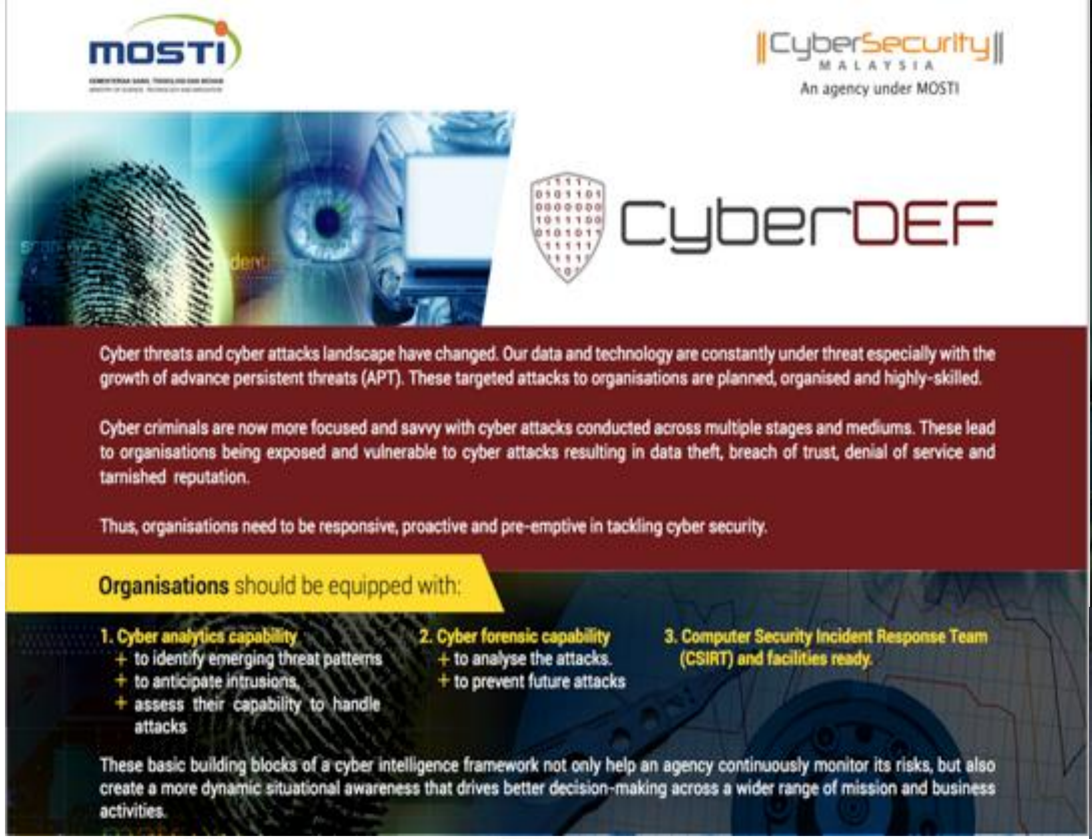
"Pada peringkat awal, kerjasama kita menumpukan tiga bidang iaitu Malware Analitik, risikan ancaman siber dan ancaman berterusan maju," katanya.

AHMAD FAUZI (dua dari kanan) dan Amiruddin (dua dari kiri) menunjukkan MoU di Johor Bahru semalam.

Copyright © 2023 CyberSecurity Malaysia

MEMPERKUKUHKAN KEUPAYAAN DETEKTIF MELALUI

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**

Copyright © 2015 CyberSecurity Malaysia

MENGUKUHKAN PENCEGAHAN KESELAMATAN CYBER MELALUI PENILAIAN TEKNOLOGI

Secure Software Development Lifecycle (SSDLC) Lab & Services

Internet of Things (IOT) Lab

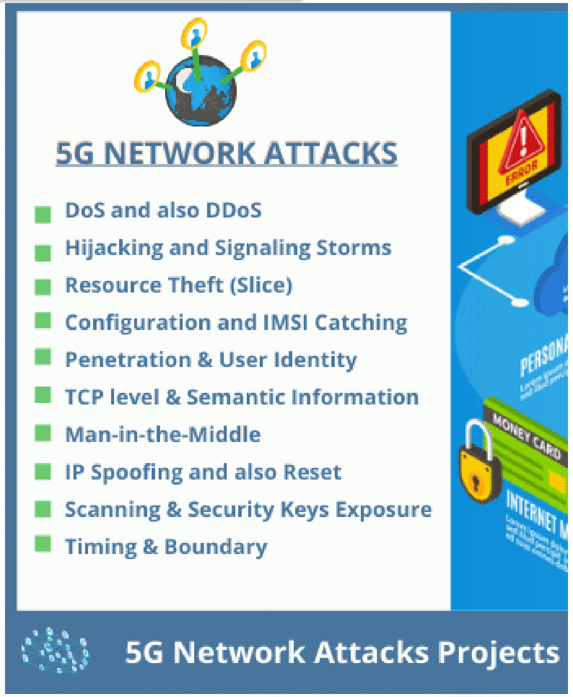
Robotic Lab (4th Industry Revolution)

Copyright © 2023 CyberSecurity Malaysia

Threat actors value zero-day exploits because most security defenses are designed to handle known flaws, so attacks that use them can go unnoticed for a long time.

CYBERSECURITY 2023 OUTLOOK

Copyright © 2023 CyberSecurity Malaysia

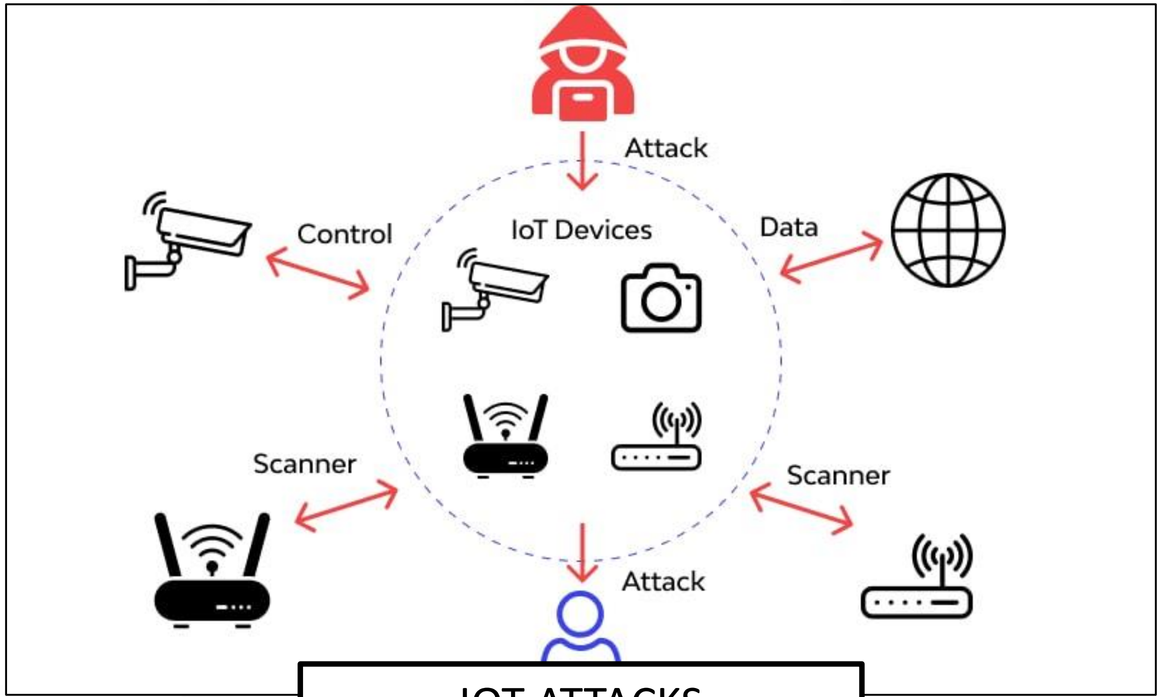


5G NETWORK ATTACKS

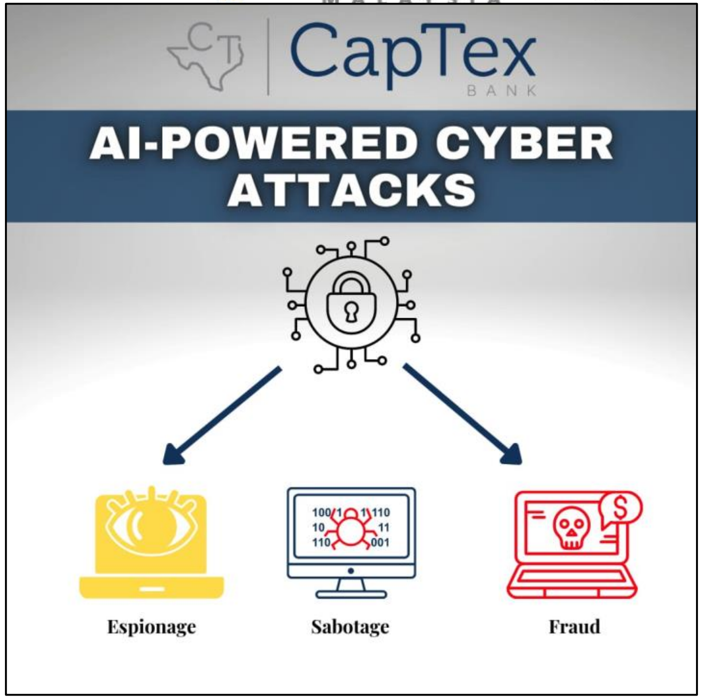
- DoS and also DDoS
- Hijacking and Signaling Storms
- Resource Theft (Slice)
- Configuration and IMSI Catching
- Penetration & User Identity
- TCP level & Semantic Information
- Man-in-the-Middle
- IP Spoofing and also Reset
- Scanning & Security Keys Exposure
- Timing & Boundary

5G Network Attacks Projects

ERROR
PERSONAL
MONEY CARD
INTERNET



IOT ATTACKS



CapTex BANK

AI-POWERED CYBER ATTACKS

CYBERSECURITY 2023 OUTLOOK

KESIMPULAN DAN HALA TUJU

Keselamatan siber penting untuk sesebuah organisasi beroperasi dengan lebih efisien dan kritikal untuk melindungi data mereka;

Semasa organisasi membina prosedur keselamatan siber, organisasi tersebut perlu menggunakan model keselamatan yang berperingkat;

Mempunyai perlindungan keselamatan siber yang dinamik, holistik, inovatif dan adaptif untuk menangani serangan siber yang canggih;

Menguatkan keselamatan siber tempatan dan global melalui kerjasama antara agensi dan *Public-Private Partnership;* dan

Persediaan lengkap adalah kunci untuk menangani ancaman-ancaman siber terkini.

Copyright © 2023 CyberSecurity Malaysia

KEMENTERIAN
KOMUNIKASI DAN DIGITAL

TERIMA KASIH

CyberSecurity Malaysia
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

CyberSecurityMalaysia   cybersecuritymy   cybersecuritymy   CyberSecurity Malaysia   cybersecurity_my

JUBLI PERAK
1997 - 2022

SIBER MALAYSIA MADANI

Copyright © 2023 CyberSecurity Malaysia