MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

IRM MALAYSIAN INTEREST GROUP (RIG)

25th September 2025

DATO' TS. DR. HAJI AMIRUDIN ABDUL WAHAB FASc,
Chief Executive Officer
CyberSecurity Malaysia

SECURING OUR CYBERSPACE

1. What is the state of Cybersecurity in Malaysian space? What is the perception of Malaysian business to cyber security?
2. What areas are hackers currently going for, what are the bureau seeing (phishing, ransomware, insider threats?) What industries are being targeted? Are companies paying up?
3. Do you see Malaysian companies treating cyber security as a risk or just paying lip service?
4. What can companies do or where can they go to find out what is cyber security safe? How can companies do a test to find vulnerabilities'? Who do they talk to?
5. For an SME what can they do to protect themselves?
6. How do we compare in Malaysia for cyber security resilience to other ASEAN countries (excluding Singapore and Hong Kong)?
7. How much are we losing as an economy to cyber security risks?
8. What is the agency's purpose and mission?
9. How does Malaysia's Cyber Security Act (2024 draft/implementation status) and the Personal Data Protection Act (PDPA) impact organisations in terms of cybersecurity compliance?
10. How are Malaysian regulators (e.g., Bank Negara Malaysia, MCMC, CyberSecurity Malaysia) shaping the cybersecurity landscape for businesses?
11. What differences do you see between Malaysian compliance requirements and those in Singapore, Hong Kong, or the EU (e.g., GDPR)?
12. How significant is the threat from state-sponsored or regional cyber actors in Malaysia compared to APAC as a whole?
13. How do organisations here balance cost vs. risk when investing in cybersecurity?
14. What best practices would you recommend for improving cyber resilience in Malaysia?

WHAT IS THE STATE OF CYBERSECURITY IN MALAYSIAN SPACE?

WHAT IS THE PERCEPTION OF MALAYSIAN BUSINESS TO CYBERSECURITY?

THE INTERCONNECTED WORLD OF CYBERSPACE

5.41 BILLION

SOCIAL MEDIA USERS WORLDWIDE

5.65 BILLION

INDIVIDUAL USERS WORLDWIDE ARE USING THE INTERNET.

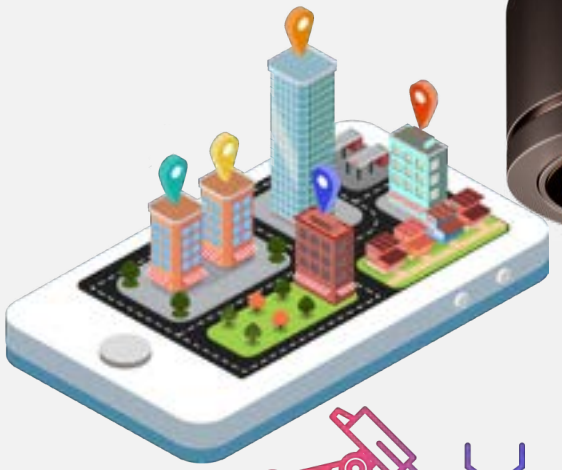
33.5 MILLION

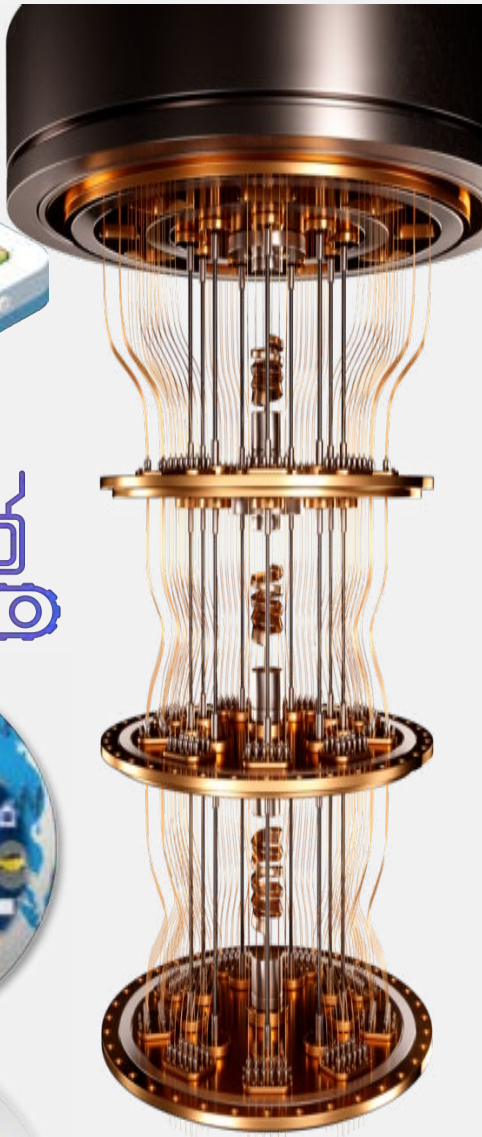
INDIVIDUAL USERS WORLDWIDE ARE USING THE INTERNET.

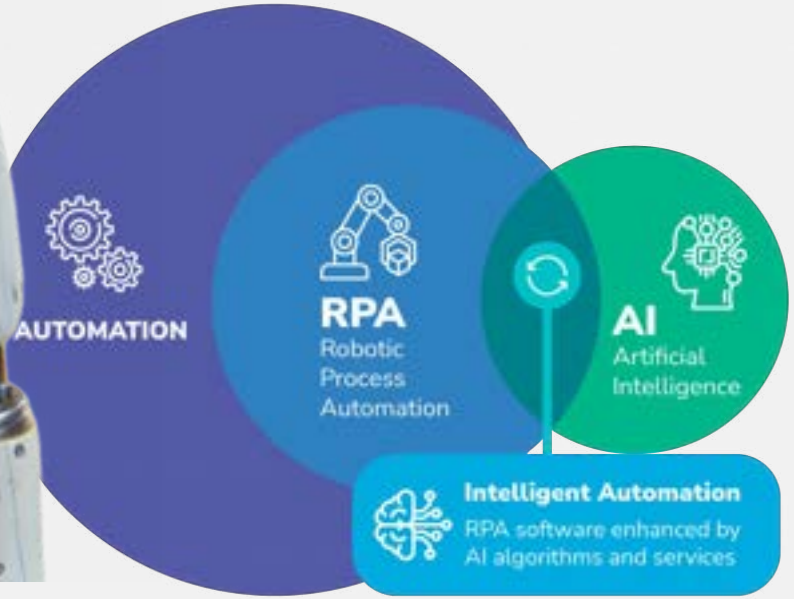
https://datareportal.com/reports/digital-2025-july-global-statshot

EMERGING TECHNOLOGIES: POWERING INNOVATION, RAISING THE STAKES

Driving Digital Transformation Amid Heightened Risks







WE HAVE TO BE AWARE THAT **EVERY CONVENIENCE** COMES WITH **RISKS.**

DIGITAL EVOLUTIONS OFFER BENEFITS BUT OPEN THE DOOR TO NEW VULNERABILITIES AND THREATS

1. Technology such as AI, has changed how we conduct business, offering workers constant access to business-critical applications and data.

2. While this flexibility is convenient and expands productivity, it **introduces complexity and security risk**. These new technologies and devices become **new targets for hackers** looking to infiltrate a corporate network.

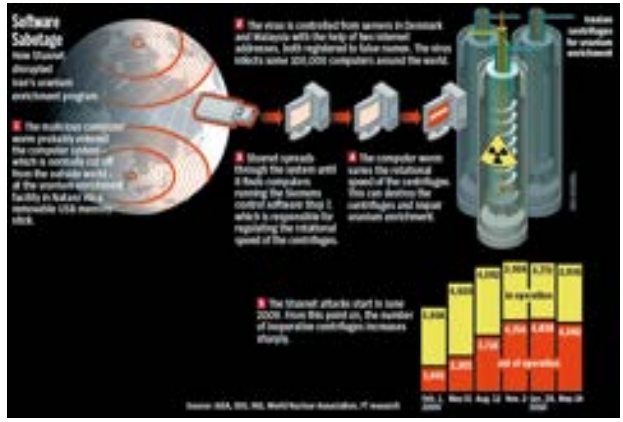
TECHNOLOGY EXECUTIVE COUNCIL

‘Cyber-physical attacks’ fueled by AI are a growing threat, experts say

PUBLISHED SUN, MAR 3 2024·10:05 AM EST

Kevin Williams

SHARE



THE RISE OF CYBER THREAT LEVEL

- As technology advances, so do cyber threats, rising with data breaches, ransomware attacks, and hacks becoming increasingly commonplace

PRANKSTER

- PASSWORD CRACKING
- PASSWORD GUESSING

INSIDER THREATS

- MALICIOUS INSIDER THREAT (DELIBERATE)
- NEGLIGENT INSIDER THREAT (CARELESS)

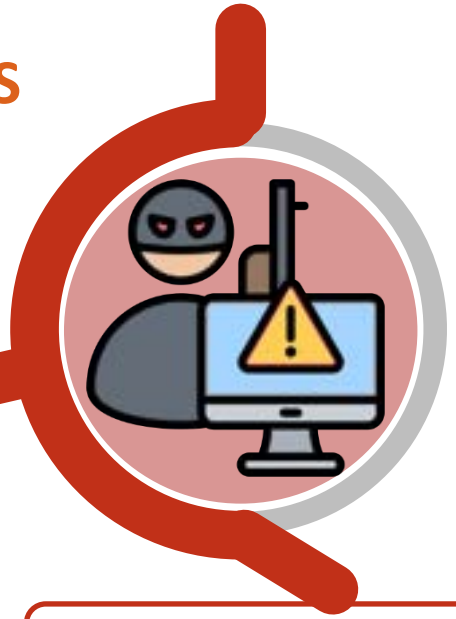
CYBER CRIMINALS

- SCAMMERS
- MALWARE
- RANSOMWARE
- PHISHING

NON-STATE ACTORS

- ESPIONAGE
- DISRUPTION/ DESTRUCTION
- POLITICAL MESSAGING

CYBER TERRORISM



- CAUSE MASS CHAOS
- DISRUPT CNII
- INFLICT PHYSICAL DAMAGE

LATEST TOP CYBERSECURITY THREATS

AI-Powered Phishing Attacks

- Hyper-personalized
- Mimic a real human
- Mimic real brands
- No more spelling or grammatical errors

Supply Chain Breaches

- 3rd parties' vulnerabilities

API Exploits

- Exposed endpoints
- Open the door to users' data

Cloud Mis-configurations

- Incorrect settings can lead to a breach.

Deepfake / Social Engineering

- Fake audios
- Fake faces
- Bypass identity checks
- Compromise trust
- Mis/disinformation

WHAT DO WE NEED TO LOOK OUT FOR...

ARTIFICIAL INTELLIGENCE

AI is rewriting the rules of the cyber battlefield. It empowers attackers to strike faster and smarter, while arming defenders with intelligent tools to detect patterns, expose anomalies, and automate countermeasures in real time

QUANTUM TECHNOLOGY

Quantum Computing is the new front there. It's still early, but when it hits, today's encryption could become obsolete. Forward-thinking organisations are already exploring quantum-safe algorithms.

PERIMETERLESS

With the rise of cloud adoption, remote work, and an increase in connected devices, security must follow where users and data are. Not just the office.

DATA INTEGRITY

Data integrity is under attack. It's no longer just about access. Tactics that alter, corrupt, or manipulate data are on the rise, and the damage can be severe.

SPEED IS THE NEW METRIC

The faster you detect and respond, the better your chances. Delayed action can turn a minor issue into a major incident.

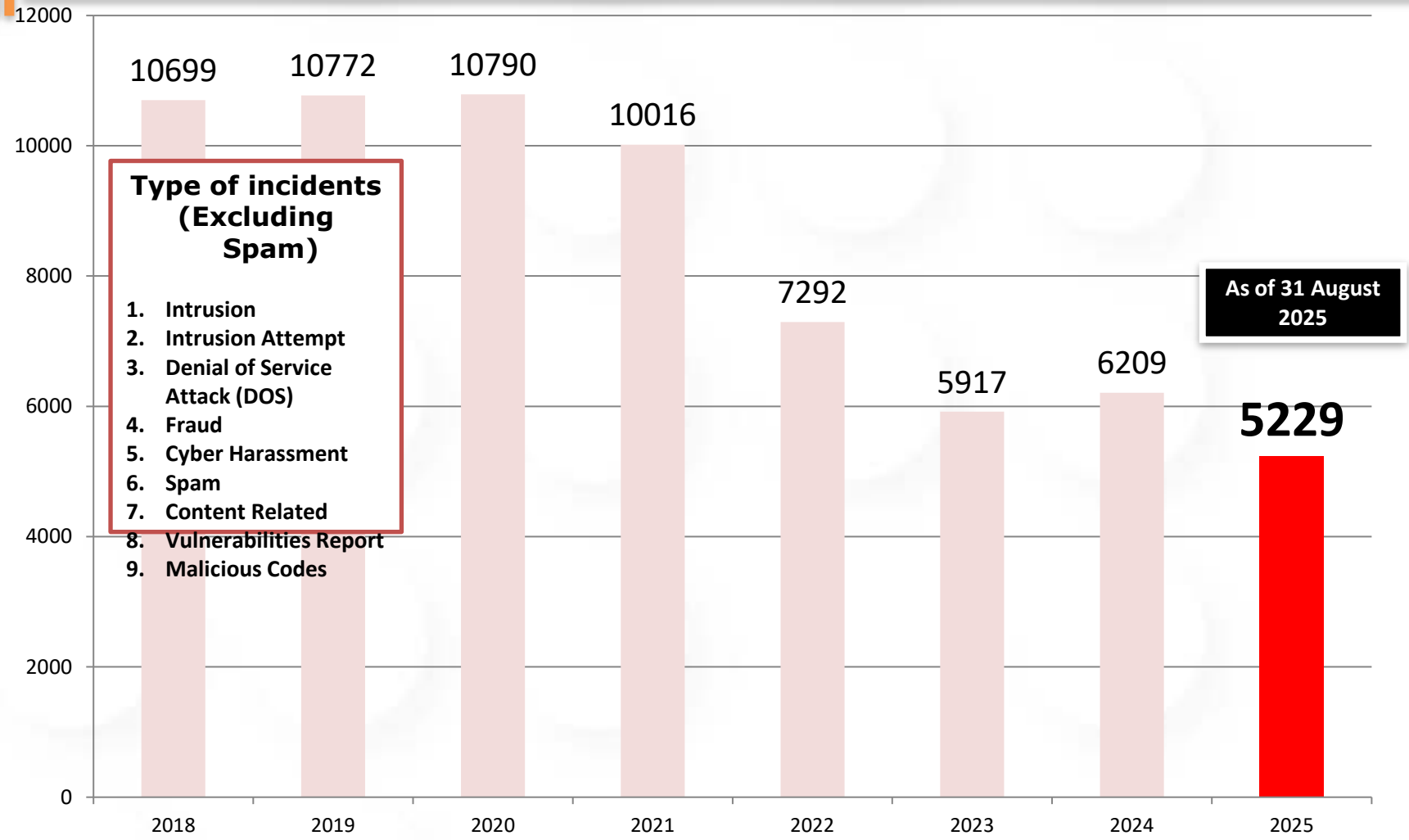
https://www.ibm.com/think/insights/cybersecurity-trends-ibm-predictions-2025

WHAT AREAS ARE HACKERS CURRENTLY GOING FOR, WHAT ARE THE BUREAU SEEING (PHISHING, RANSOMWARE, INSIDER THREATS)?

WHAT INDUSTRIES ARE BEING TARGETED?

ARE COMPANIES PAYING UP?

CYBER INCIDENTS REFERRED TO CYBERSECURITY MALAYSIA (2018 – 31 August 2025)



https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=23495156-c6ec-48fa-89e2-c73bc081e157

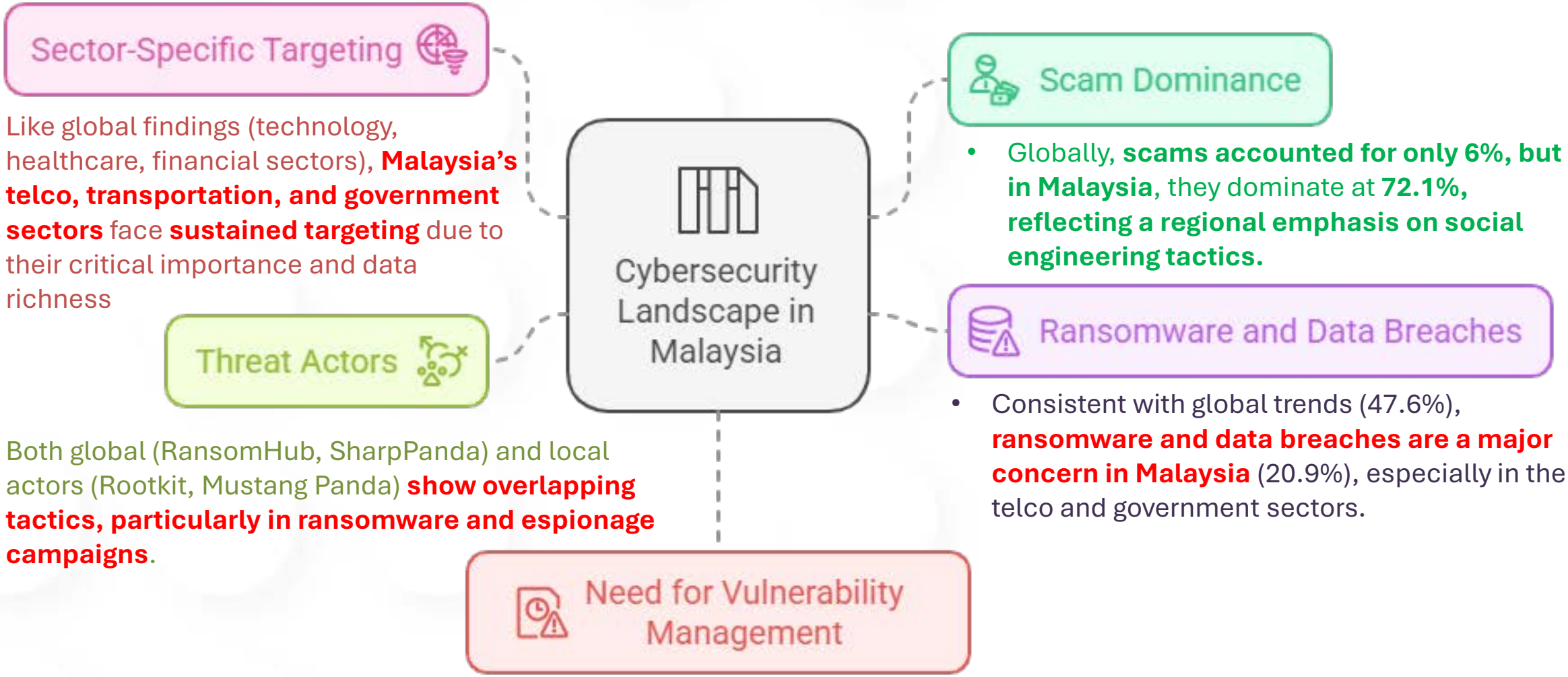
MyCERT Incident Statistics

Security Alert

TOP FOUR CYBER INCIDENTS IN MALAYSIA (CYBER999)

1. Fraud
2. Malicious Code
3. Intrusion
4. Content Related

Malaysia CyberSecurity Landscape Correlation with Global Insights



- Like global findings (technology, healthcare, financial sectors), **Malaysia's telco, transportation, and government sectors** face **sustained targeting** due to their critical importance and data richness

- Globally, **scams accounted for only 6%, but in Malaysia**, they dominate at **72.1%, reflecting a regional emphasis on social engineering tactics.**

- Both global (RansomHub, SharpPanda) and local actors (Rootkit, Mustang Panda) **show overlapping tactics, particularly in ransomware and espionage campaigns**.

- Consistent with global trends (47.6%), **ransomware and data breaches are a major concern in Malaysia** (20.9%), especially in the telco and government sectors.

- The global emphasis on CVEs (e.g., CVE-2024-3400, CVE-2023-41724) aligns with the need for Malaysia to prioritise timely patching in high-risk sectors.

THE COST OF A CYBERSECURITY RISK, THREATS, OR AN ATTACK

CyberSecurity MALAYSIA

Cyber attacks may cost Malaysia RM49.15 billion in economic losses

Cyber attacks may cost Malaysia billion in economic losses | Chubb

06/2022

2022 - Expectation

Cybercrime costs Malaysia RM1.22 billion in ten months - IGP

Mohd Khalid warns of alarming rise in cyber threats, including data breaches and online fraud, as authorities turn to artificial intelligence to counter escalating digital crimes

Updated 3 weeks ago · Published on 26 Aug 2025 1:33PM

2025 - Realities

Cyber Crime Modus Operandi	Case	Loses (RM)
Telecommunication Fraud	14,687	497,342,125.12
E-Financial Fraud – BEC/Phishing	1,814	65,519,370.80
Love Scam	771	45,877,765.84
E-Commerce Fraud	7,665	70,880,019.93
Non-Existent Loan	10,250	182,277,157
Non-Existent Loan Investment	4,102	46,254,080.37
Total	6,343	851,057,755.27

Source: PDRM Commercial Crime Intelligence System 6 Jan 2025

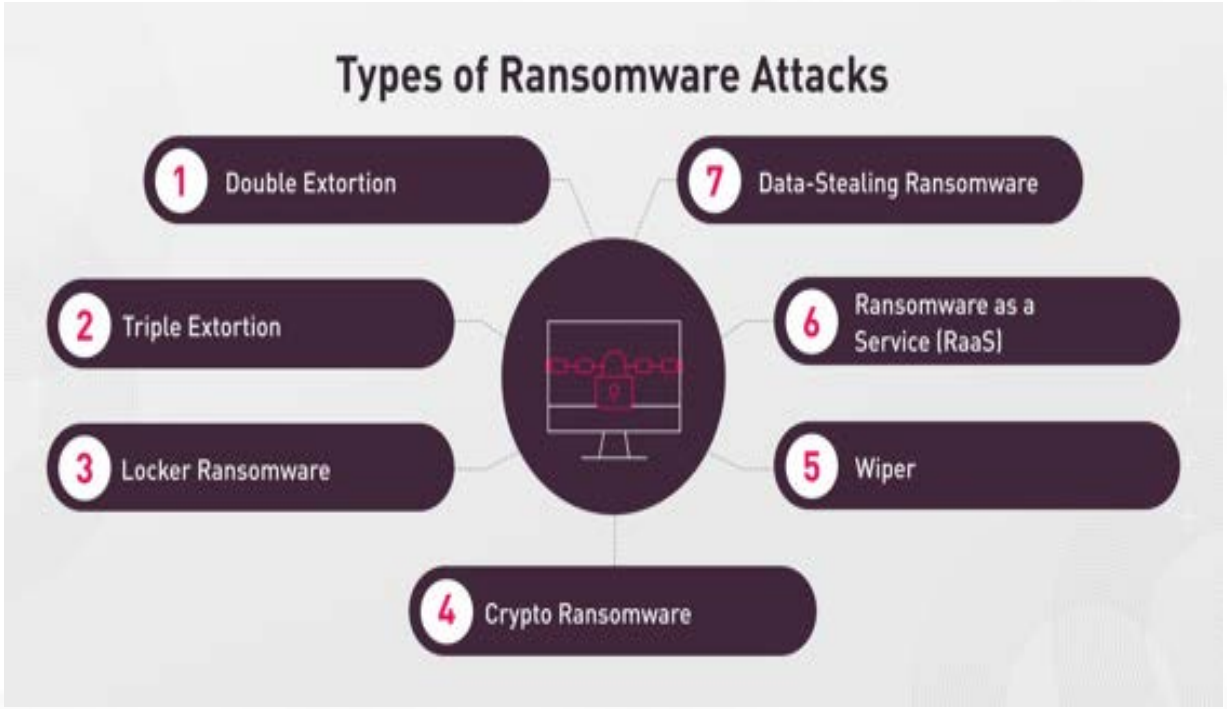
ARE COMPANIES PAYING UP?

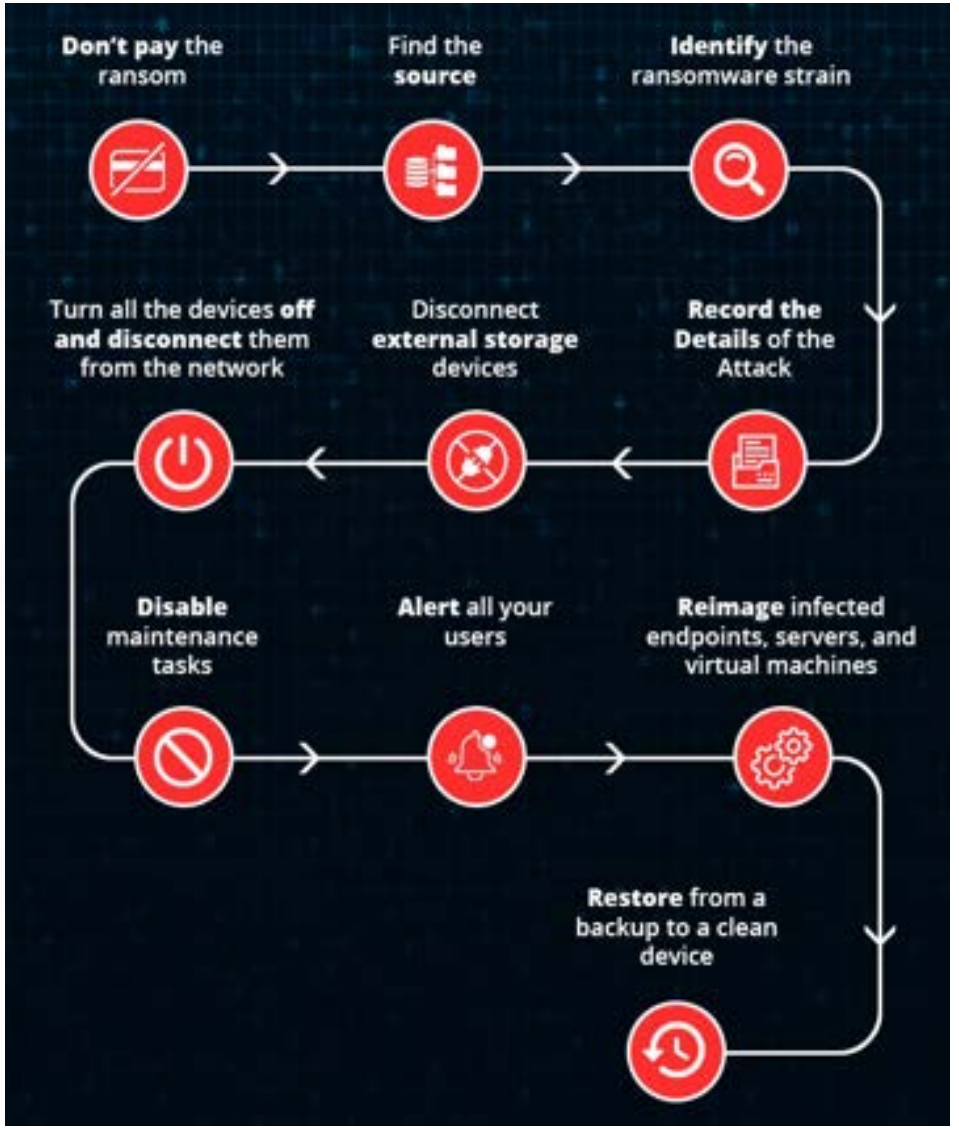
Malaysia PM Refuses to Pay $10M Ransomware Demand

The attack hit the Kuala Lumpur airport over the weekend, and it remains unclear who the threat actors are and what kind of information they may have stolen.

- **There is no guarantee that you will get your money back.**
- **You might be also targeted in future attacks.**
- **They money you paid might go and finance criminal activities and groups.**
- **Your system might still be infected.**

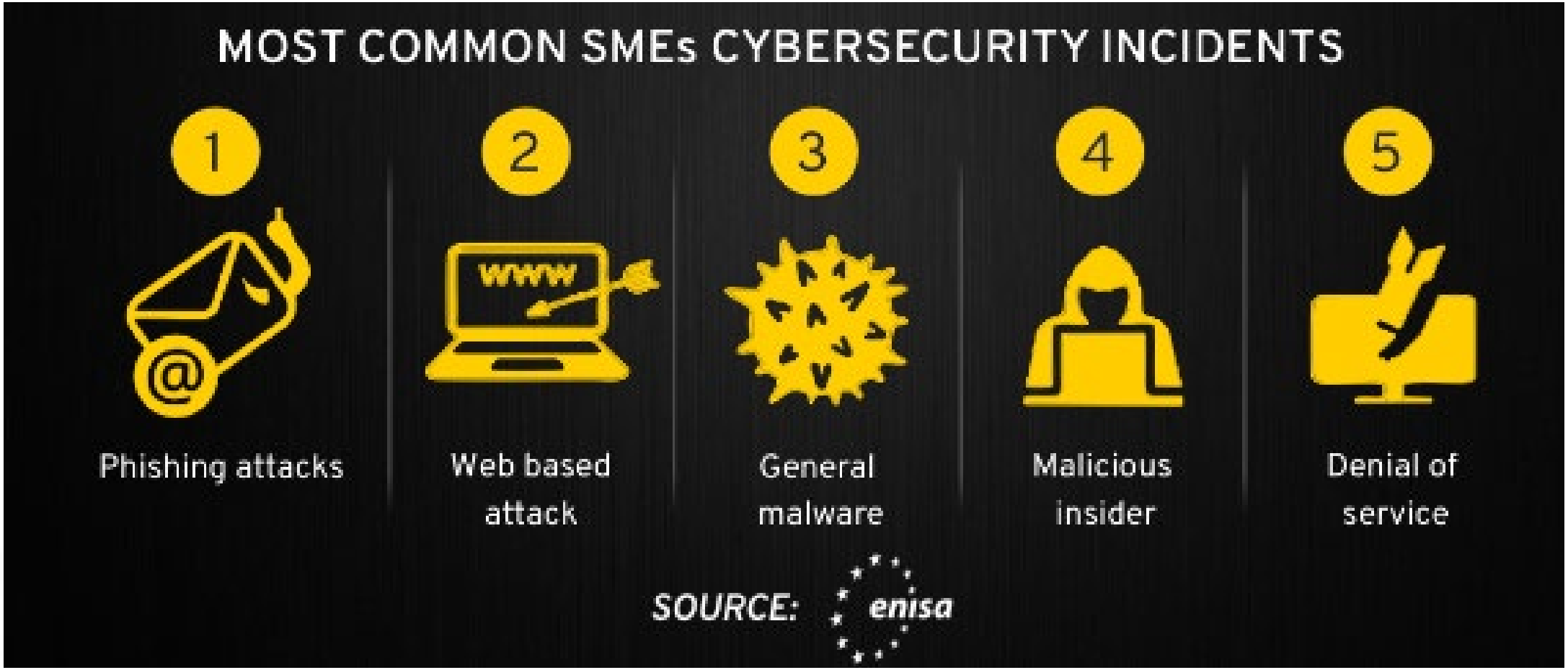
STEPS TO TACKLE RANSOMWARE ATTACK





https://www.lepide.com/blog/how-to-recover-from-a-ransomware-attack/

SME ARE ALSO PRONE TO CYBER-ATTACKS



SME’s CYBER SECURITY CHECKLIST

HOW SIGNIFICANT IS THE THREAT FROM STATE-SPONSORED OR REGIONAL CYBER ACTORS IN MALAYSIA COMPARED TO APAC AS A WHOLE?

- There is an increase in nation-state-sponsored cyber activities, including cyber espionage and information warfare. This poses significant geopolitical and security concerns for the Asia Pacific region.

- Close to 40% of cybercrime activity in the region has been attributed to state-sponsored threat groups.

Source: Ensign InfoSecurity Sdn Bhd - Cyber Threat Landscape Report 2025

WHY MALAYSIA BECOME TARGET OF STATE SPONSORED ATTACKS?

Intelligence Value

Central role in ASEAN, offering insights on security, migration, and counterterrorism.

Critical infrastructure

Expanding energy, telecom, and transport systems are prime targets for disruption or espionage.

Regional Influence

Opportunities to sway politics, public opinion, and policy directions.

Geopolitical Position

A strategic location in Southeast Asia, useful for monitoring and influencing the region.

Economic Importance

A hub for trade, finance and key industries like electronics, automotive, palm oil, and petroleum.

Cyber-attacks on Malaysian organizations not only do financial and reputational damage but also have a negative impact on attracting investments from potential global investors.

Threat groups are becoming more strategic

They are able to bypassing traditional defences by exploiting trust, vendor relationships and weak access points within systems.

Organizations can no longer assume that their defences are adequate. They must continuously adapt, verify, validate their security measures and address vulnerabilities to ensure their cyber posture is aligned with today's threat landscape.

DO YOU SEE MALAYSIAN COMPANIES TREATING CYBER SECURITY SERIOUSLY OR JUST PAYING LIP SERVICE?

Malaysia is serious about cybersecurity, says DPM Zahid at the opening of CYDES 2025

By Mc

PwC

Cyber Security Act 2024: A new era for cybersecurity in Malaysia

The Cyber Security Act 2024 is a crucial and timely legislation that strengthens Malaysia's cyber defense capabilities, reinforcing our position in an...

7 Nov 2024

Malaysia ramps up cyber security defense to stem rising fraud and ransomware attacks

Strengthens digital resilience with global partnerships.

By **Abbinaya Kuzhanthaivel** on Oct 15, 2024 12:48PM

In the face of escalating cyber threats, Malaysia is intensifying its cybersecurity strategy, focusing on a significant rise in fraud incidents and the alarming trend of double extortion ransomware attacks.

Malaysia

Malaysia

GCI 5th Edition Country Profile

Country Score
out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
20	20	18.82	20	20

Areas of Relative Strength
Legal Measures
Technical Measures
Capacity Development Measures
Cooperation Measures

Area of Potential Growth
Organizational Measures

Tier Performance
T1: Role modelling

BUT IS IT ENOUGH?

Alleged MyKad Data Leak Raises Concerns Over Financial Fraud in Malaysia

A reported leak of 17 million MyKad records has shaken Malaysia has its citizens flagging serious concerns regarding identity theft and financial fraud.

Izzat Najmi Abdullah — December 4, 2024 — 5 Mins Read

bernama

- 16 Billion Passwords Leaked: Why Malaysians Should Take Digital Security Seriously

By Nur Farah Ilyana Idros. In June 2025, researchers uncovered what is believed to be the largest data breach in history.

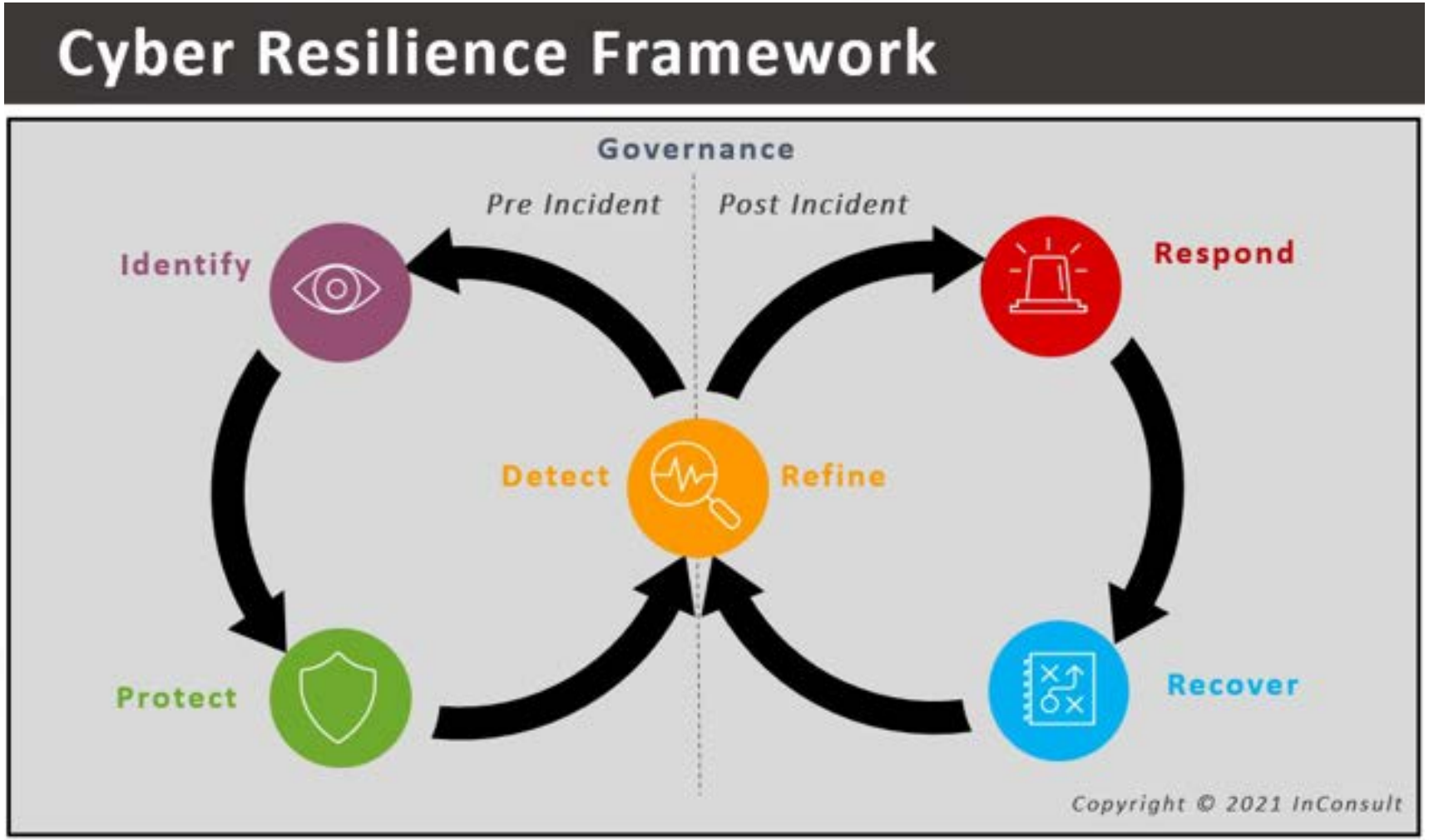
1 month ago

Ransomware Strike On MAHB Highlights Need For Stronger Cyber Defenses – Experts

26/03/2025 05:57 PM

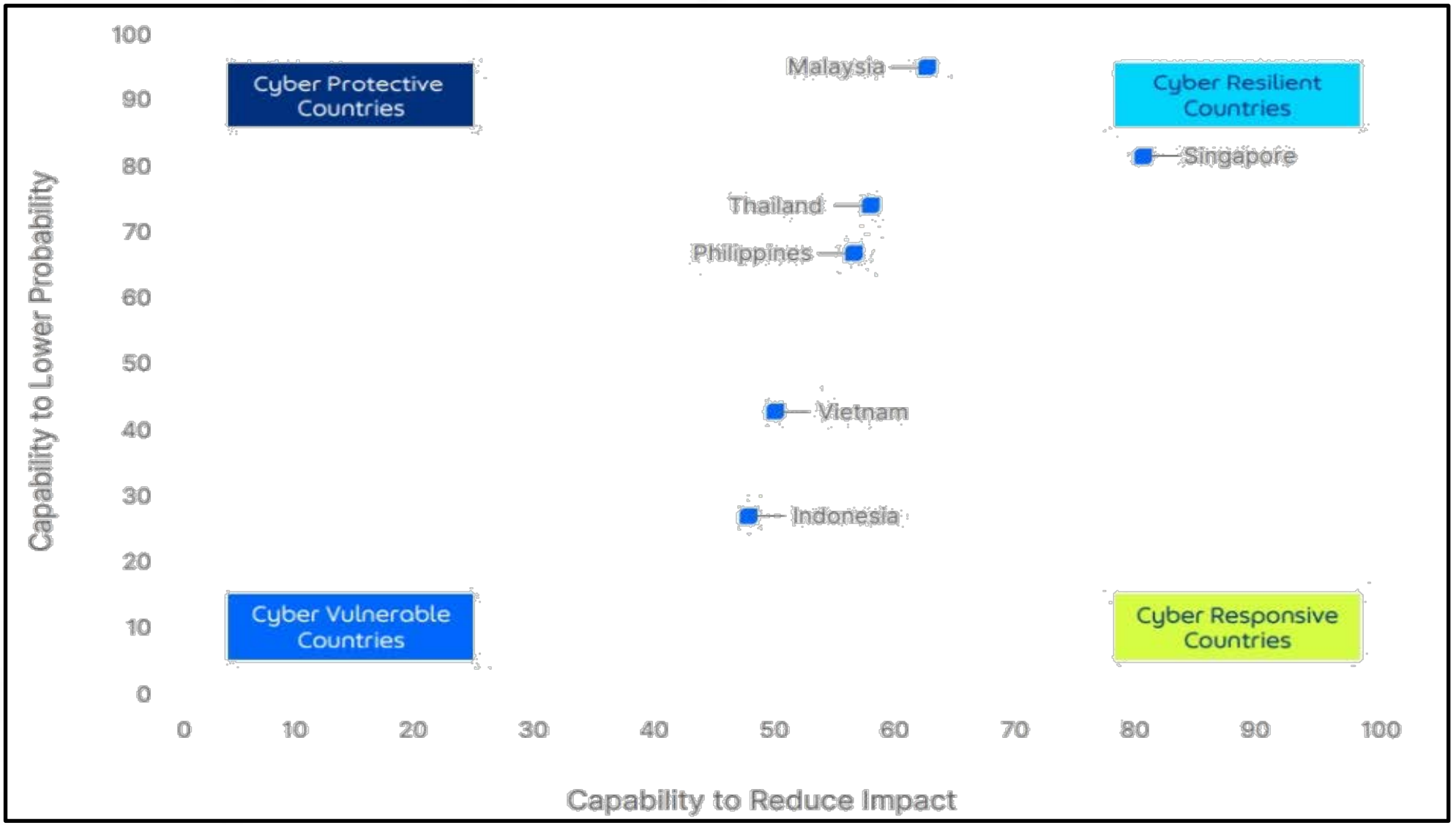
Experts call for urgent reform in cyber security priorities

THAT IS WHY CYBER RESILIENCE IMPORTANT (NOT ONLY CYBERSECURITY)



How do we compare in Malaysia for cyber security resilience to other ASEAN countries ?

Figure A. The State of Cyber Resilience in Southeast Asia



Source: Tech For Good Institute (TFGI)
Towards a Resilient Cyberspace in Southeast Asia Report

https://techforgoodinstitute.org/wp-content/uploads/2023/05/TFGI-Towards-a-Resilient-Cyberspace-in-Southeast-Asia-Report.pdf

Some ASEAN Initiatives on Cyber Resilience

Asean Cybersecurity Cooperation Strategy 2026-2030

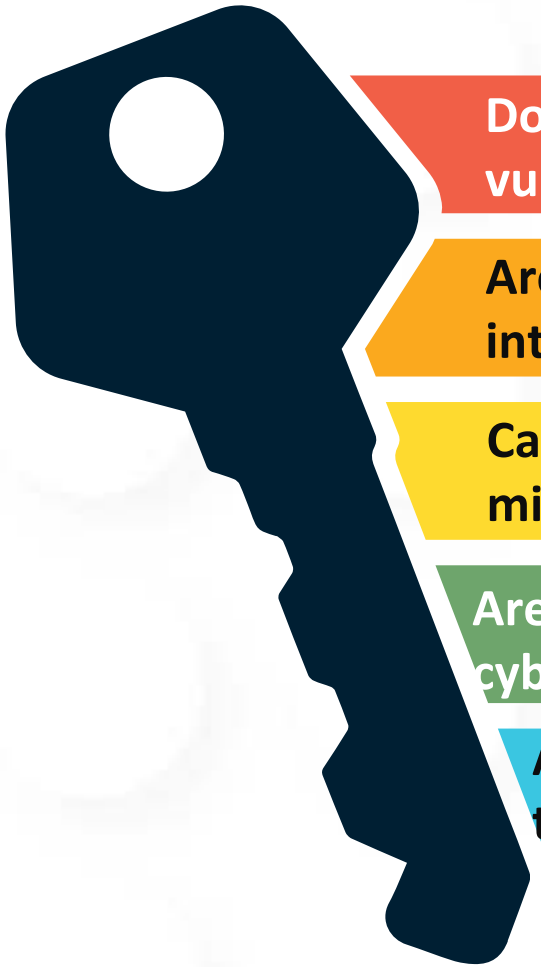
Focusing on information sharing, joint technology development, and human capital growth.

ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP)

ASEAN MALAYSIA 2025
INCLUSIVITY AND SUSTAINABILITY

WHAT BEST PRACTICES WOULD YOU RECOMMEND FOR IMPROVING CYBER RESILIENCE IN MALAYSIA?

TOP MANAGEMENT / LEADER NEED TO ASK THEMSELVES THESE KEY QUESTION



1. Do we know our most critical assets and vulnerabilities?
2. Are we investing enough in cybersecurity talents and intelligence?
3. Can we detect and respond to an attack within minutes, not days?
4. Are we setting the right tone at the top in terms of cyber hygiene, cybersecurity culture and responsibility?
5. Are we adopting an adapting and holistics approach that covers people, process and technology?

BEST PRACTICES IN IMPROVING CYBER RESILIENCE

NO 100% SECURE

Need to recognise there is no such thing as 100% secure. We need to act like we are going to be attacked soon or already has been attacked.

PLAN AND ANTICIPATE

We must plan and anticipate for disruptions and incidents.

BY DESIGN

Security and resilience by design (embedded).

PROACTIVE

Don't only focus on responsive cybersecurity measures, its now imperative to have pre-emptive and proactive measures.

CIA TRAID

Confidentiality, Integrity, Availability (+Non-repudiation and Authorization)

LEARN AND ADAPT

Recover, learn from past incidents and adapt. Eg: AI: by continuously updationg ones skills, understanding the risk and benefits, learn from past experience and be more resilient.

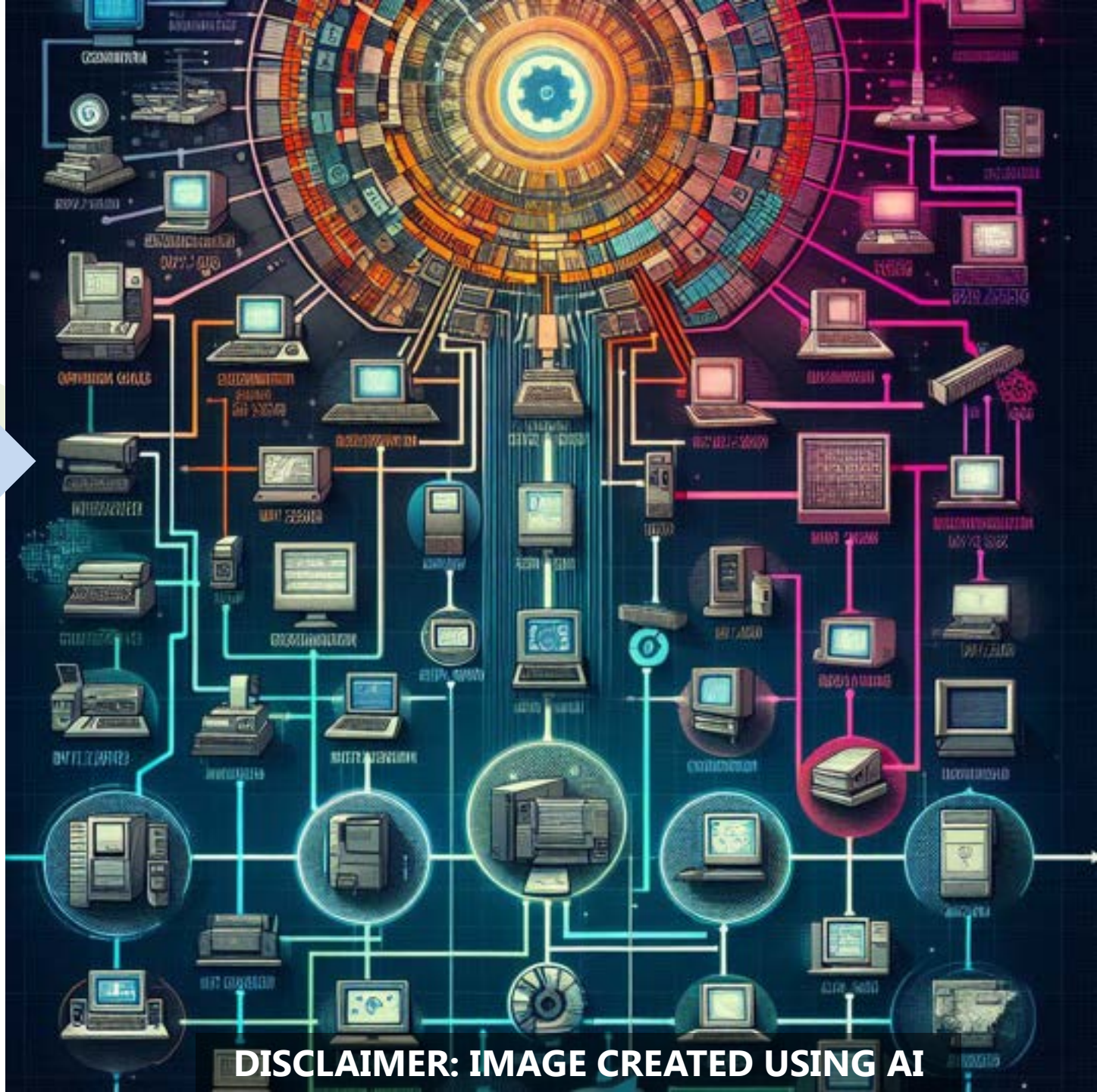
CREATE A CYBERSECURITY CULTURE

CYBERSECURITY REQUIRE GOOD CAPACITY BUILDING AND CYBER RESILIENCE PRACTICES

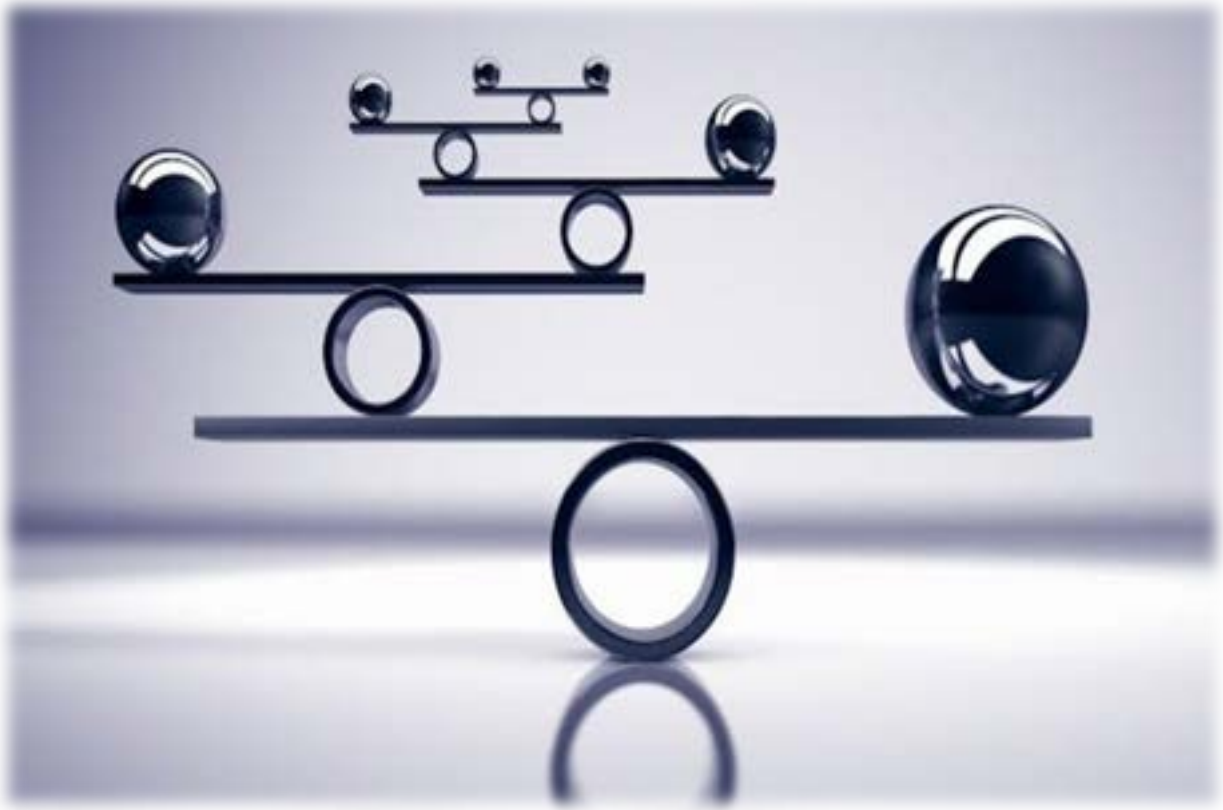
Collaborate with their counterparts, government agencies, the industry, non-governmental organisations, academia, etc to share knowledge, skills, to solve problems and have in-house training regarding the industries' best practices

TECHNOLOGY IS DEVELOPING AT SUCH A FAST PACE

POLICIES AND LEGISLATION NEED TO BE IN LINE WITH NEW TECHNOLOGY



DISCLAIMER: IMAGE CREATED USING AI



HOW DO ORGANISATIONS HERE BALANCE COST VS. RISK WHEN INVESTING IN CYBERSECURITY?

BALANCING COST AND RISK IN CYBERSECURITY

To weigh the spending on cybersecurity vs. the risk of big losses.

Cyber-attacks can be damaging in terms of cost (hundreds/thousands/millions) and reputation.

Convenience vs Security.

Need to strike a balance where systems are easy enough for users to access and use, but still strong enough to protect against threats and risks.

What To Do With The Risks

Decide whether to accept, avoid, transfer, reduce / mitigate the risk

Decision - making

To weigh the spending on cybersecurity vs. the risk of big losses.

Cost

Cyber-attacks can be damaging in terms of cost (hundreds/thousands/millions) and also reputation.

BALANCING COST AND RISK IN CYBERSECURITY

Hence it is important that:

- Use advance technologies such as automation, AI, bloackchain, and etc in order to help cut cost, be productive and also boost protection.
- Hire external parties (Managed Security Service Providers - MSSPs) that provide cost saving packages while staying safe and secure.
- Guided by proper policies, rules and regulation such as Cyber Security Act 2024.

MALAYSIA EFFORTS FOR CYBERSECURITY

POLICY & STRATEGIES	LEGISLATION	GUIDELINE & BEST PRACTICES
1. Digital Economy Blueprint (MyDIGITAL) 2. National Policy on Industry 4.0 3. Malaysia Cybersecurity Strategy 2020-2024 4. National Cyber Security Policy (NCSP) 2006	1. CyberSecurity Act 2024 2. Personal Data Protection Act 2024 (PDPA Amendment) 3. Data Sharing Act 2024 4. Online Safety Bill 5. Communications and Multimedia Act 1998 (CMA) 6. Computer Crimes Act 1997 (CCA) (To be amended) 7. Digital Signature Act 1997 (DSA) 8. Electronic Government Activities Act 2007 (EGAA) 9. Penal Code (Amendments related to cybercrimes)	1. Bank Negara Malaysia's Risk Management in Technology (RMiT) 2. Cybersecurity Best Practices and Guidelines by CSM 3. MCMC Guidelines 4. Cyber Security Framework For Public Sector (RAKKSSA) 5. Artificial Intelligence Governance and Ethics (AIGE)

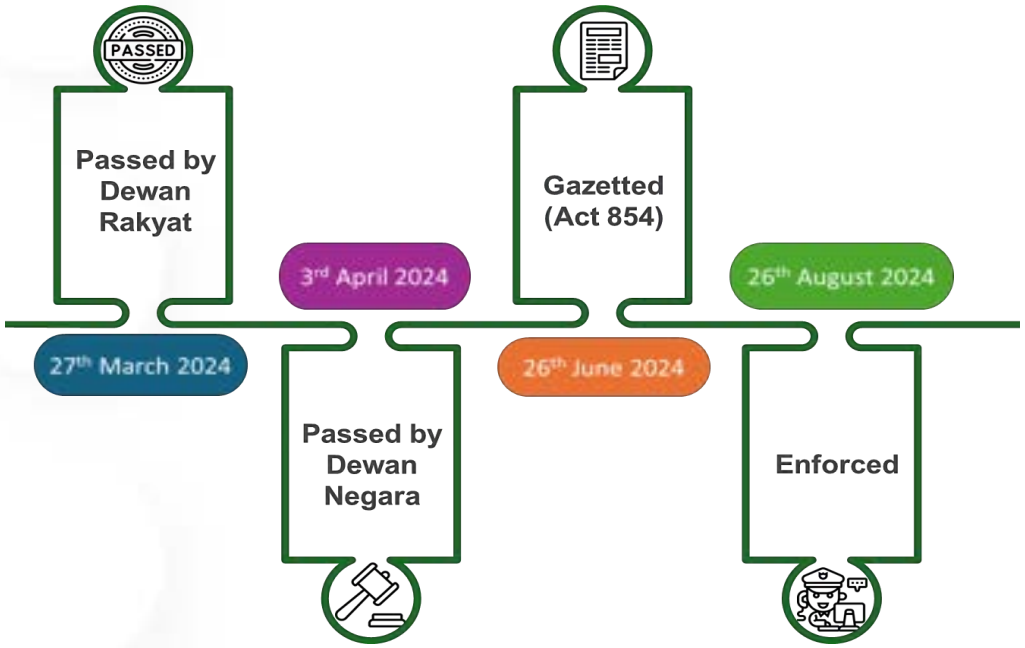
CURRENTLY ONGOING / IN PROGRESS

1. Freedom Of Information Act
2. Malaysia Cyber Security Strategy 2025-2030 – Launched July 2025
3. MyDigital ID
4. Malaysia Technology and Cryptology Centre
5. Cybercrime Initiatives

KEY ELEMENTS OF CYBER SECURITY ACT (ACT 854)

The Cyber Security Act 2024 has been officially gazetted by the Attorney General's Chambers on 26 June 2024. This legislation is a major milestone in strengthening Malaysia's cyber defences and enhancing our resilience against emerging threats.

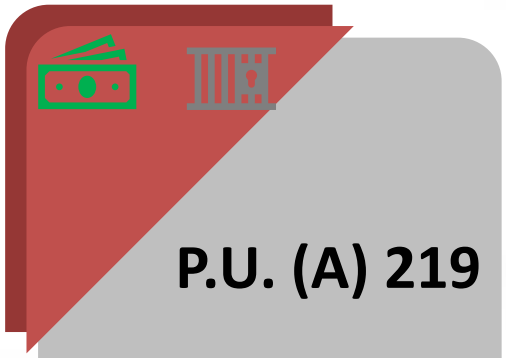
Addresses the management of cyber security threats and incidents related to National Critical Information Infrastructure (NCII).



First Set of Regulations | **26th August: Act started to be enforced**

Non-Compliance
Compounding of Offences

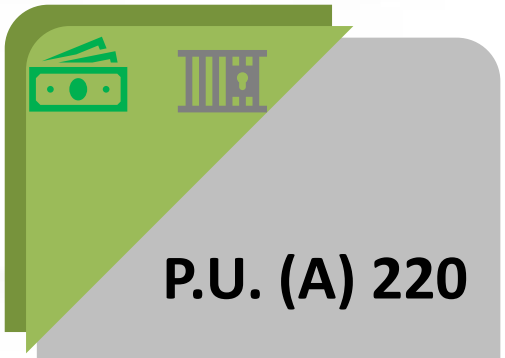
CYBER SECURITY ACT 2024
CYBER SECURITY (COMPOUNDING OF OFFENCES) REGULATIONS 2024



P.U. (A) 219

Failure to conduct Risk Assessment

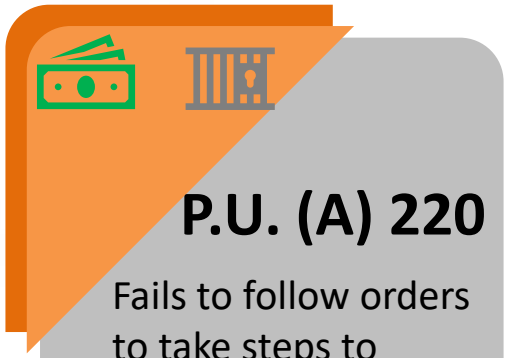
- **RM 200,000**
- **3 years jail**
- **Or both**



P.U. (A) 220

Fail to notify that cyber incident has occurred

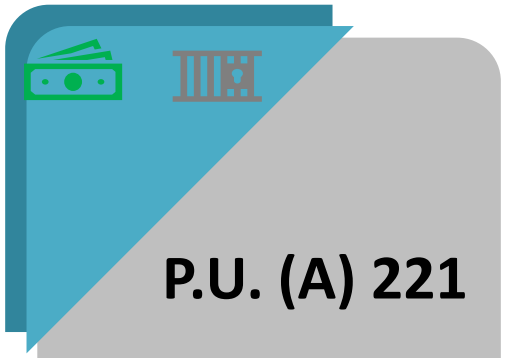
- **RM 500,000**
- **10 years jail**
- **Or both**



P.U. (A) 220

Fails to follow orders to take steps to address or recover from the cyber incident and prevent future incidents

- **RM 200,000**
- **3 years jail**
- **Or both**



P.U. (A) 221

Non-compliance with code of practice

- **RM 500,000**
- **10 years jail**
- **Or both**

Summary of NACSA Chief Executive Directive

Directive No. 1:
Cybersecurity Incident Notification

Establishes **procedures for reporting cybersecurity** incidents by entities managing the National Critical Information Infrastructure (NCII).

- Submission must be given **within 21 days** from the date of designation as an entity.
- within **7 days** if there is a change

Directive No. 2:
Licensing of Cybersecurity Service Providers

Introduce **licensing requirements** for cyber security service providers in Malaysia

Linked to new cybersecurity **rules for licensing** and for **compounding offences**

Directive No. 3:
NCII Entity Designation

Outlines responsibilities for designating NCII entities and maintaining detailed records.

Ensure **critical infrastructure operators comply** with the requirements of Act 854.

Directive No. 4:
National Cyber Security Policy Self-Assessment

Requires NCII entities to **self-assess their cybersecurity maturity** against the National Cybersecurity Guidelines, which include six domains, 15 categories and 33 elements

Must be implemented within **2 weeks** of being designated as an entity

Directive No. 5:
Cyber Security Risk Assessment

Provides a framework for cybersecurity risk assessment of NCII systems, covering asset inventory, threat identification, vulnerability analysis and risk mitigation

Directive No. 6: Extension Of The Waiting Period For Obtaining A Cybersecurity Service Provider License

The purpose of this directive is to **set the extension of the grace period** for individuals and companies to obtain a license as a cybersecurity service provider

Directive No. 7: Preparation of Code of Practice by National Critical Information Infrastructure Sector Heads

To establish the **requirements and guidelines for the preparation of a code of practice** by the NCII Sector Heads

Directive No. 8: Cyber Security-related Audit For National Critical Information Infrastructure Entities

Outlines the mandatory cybersecurity audit requirements for organisations designated as NCII entities in Malaysia.

Personal Data Protection Act Amendment 2024 (PDPA)

The Personal Data Protection (Amendment) Bill 2024, which was passed by the Malaysian Parliament earlier in July, has received royal assent and has been published in the Federal Gazette as the **Personal Data Protection (Amendment) Act 2024 ("Amendment Act") on 17 October 2024.**

Introduction to Biometric Data

Enhances personal data protection by making it more **comprehensive and safeguarding data subjects' privacy more effectively**.

Removal of White-List Countries to Cross-Border Data Transfers

Removal of the "white-list" regime. This change addresses one of the most frequently asked questions about the current data transfer restrictions, **offering more operational flexibility**.

Right to Data Portability

It allows data subjects to **request the transfer of their data to another data controller of their choice**. This request is subject to technical feasibility and compatibility of the data format.

Data Breach Notification to Data Subjects

Dual notification requirements: the data controller **must also notify the affected individual without delay** if a personal data breach is likely to cause significant harm to data subjects. **Increase in penalties up to RM1 million or imprisonment for up to three (3) years for any violation of the existing laws**.

Change from "Data User" to "Data Controller"

It aligns more closely with the common terminology used in other jurisdictions such as the EU, UK, and Singapore.

Data Controller: someone who **decides how and why personal data is used, either by themselves or with others.** *(They are not just following instructions like a data processor.)*

The new Role of "Data Processors"

The current PDPA 2010 mainly focuses on "data users" or "data controllers," without imposing direct obligations on "data processors."

* Data Processor: someone who **handles personal data only for the data controller and doesn't use it for themselves**

The Appointment of Data Protection Officer (DPO)

Data controllers and data processors must appoint a DPO who will be accountable for compliance with the PDPA 2010.

Mandatory Data Breach Notification to the Personal Data Protection Commissioner

if a personal data breach occurs.

BRIEF EXPLANATION ON THE TERMS

Data transfer abroad

Data can be transferred to countries with adequate protection laws. This facilitates the protection of international data transfers

Data controller

In the 2024 Act, the term “data controller” replaces "data user". This refers to those who processes any personal data or has control over or authorises the processing of any personal data.

Data processor

This refers to those who processes personal data on behalf of data controller. Data processors are now obliged to take steps to protect personal data from loss, misuse, unauthorised access and other risks.

Data protection officer (DPO)

Data controllers and data processors must designate a DPO. The DPO will be accountable to the data controller and data processor for ensuring the organisation's adherence to the PDPA.

Mandatory data breach notification

Data controllers must promptly notify the PDP Commissioner of any data breach, or face a fine of up to RM250,000 and/or up to two years in prison.

Biometric data

"Biometric data" has been added to the 2024 Act and is now classified as sensitive personal data, which requires more stringent handling procedures.

Data portability rights

Individuals can now request their data to be transferred to another service which facilitates easier switching between service providers.

Personal Data Protection Act 2024 (PDPA)

The Personal Data Protection (Amendment) Bill 2024, which was passed by the Malaysian Parliament earlier in July, has received royal assent and has been published in the Federal Gazette as the **Personal Data Protection (Amendment) Act 2024 ("Amendment Act") on 17 October 2024.**

- **Amendment of Section 5: Inserting responsibilities** to Data Processors.
- **New provision of Section 12A: Mandatory appointment of a Data Protection Officer** responsible for ensuring compliance with Act 709.
- **New Provisions of Section 12B: Requiring Data Controllers to submit notifications** of data breach incidents to PDP Commissioners as soon as practicable.
- **New Provisions of Section 43A:** Enabling Data Subjects to **Apply for Transfer of Personal Data from Data Controller to Another Data Controller**.

Personal Data Protection Act 2024 (PDPA)

1. **The penalty** for violations of the seven (7) Personal Data Protection Principles has been **increased from RM300,000.00 to RM1,000,000.00**, and the **imprisonment term has been extended from a maximum of 2 years to 3 years.**

2. The requirement to designate specific **locations for the transfer of any personal data outside Malaysia has been removed from Act 709.**

3. Provisions related to **the appointment of any Data Controller as the lead for the Data Controller Forum will empower the Personal Data Protection Commissioner to designate any Data Controller** or an organisation as the lead of a Data Controller Forum.

4. Amendment to allow the delivery of notices electronically in addition to the existing delivery methods.

5. Amendment to the provisions regarding the management of the Personal Data Protection Fund account, allowing the Commissioner to administer the account through any means authorized by the Commissioner.

6. Editorial amendment by replacing the term “Registrar” with “Commissioner” in the Malay text of Act 709.

WHAT DIFFERENCES DO YOU SEE BETWEEN MALAYSIAN COMPLIANCE REQUIREMENTS AND THOSE IN SINGAPORE, HONG KONG, OR THE EU (E.G., GDPR)?

- Malaysia's PDPA 2024 aligns more closely with international standards, especially the EU GDPR
- Cross-border data transfers allowed to countries with similar data protection laws; whitelist regime removed (broader than the EU's strict mechanisms)
- Singapore and Hong Kong remain less prescriptive:
  - No mandatory breach notification or DPO mandate in both jurisdictions
  - Singapore enforces stricter cross-border data transfer rules compared to Hong Kong

ONLINE SAFETY ACT 2024

Duties of ASPs and CASPs

a) **Mitigating Exposure to Harmful Content**: Implement measures to reduce the risk of users encountering harmful content

b) **User Guidelines**: Provide users with clear guidelines on implemented safety measures and terms of use of their services.

c) **Online Safety Tools**: Offer tools and settings that allow users to manage their online safety.

d) **Reporting Mechanisms**: Mechanisms must be in place for users to report harmful content and to seek responsive assistance for online safety concerns or inquiries about safety measures.

e) **Blocking Priority Harmful Content**: Establish systems that make priority harmful content inaccessible on their platforms.

f) **Child Safety Measures**: Specific protections for children must be implemented.

g) **Online Safety Plan**: Service Providers must **develop**, **submit** to the MCMC, and **publicly share an Online Safety Plan** detailing compliance with these obligations.

MCMC is empowered to impose a financial penalty of up to RM10 million on Service Providers that fail to comply with any of the aforementioned duties.

https://law-partnership.com/intro_online_safety_bill_2024/

Risk Management in Technology (RMiT)

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

This policy outlines various frameworks and requirements to safeguard customer data, systems, and technology infrastructure against cyber threats.

Technology Risk Management Framework (TRMF):

- Establishes a comprehensive framework for managing technology risks, **including cybersecurity threats**.
- Requires digital banks to **conduct regular risk assessments, identify vulnerabilities, and implement appropriate controls**.
- Promotes a **proactive approach** to cybersecurity, focusing on prevention rather than just reaction.

1

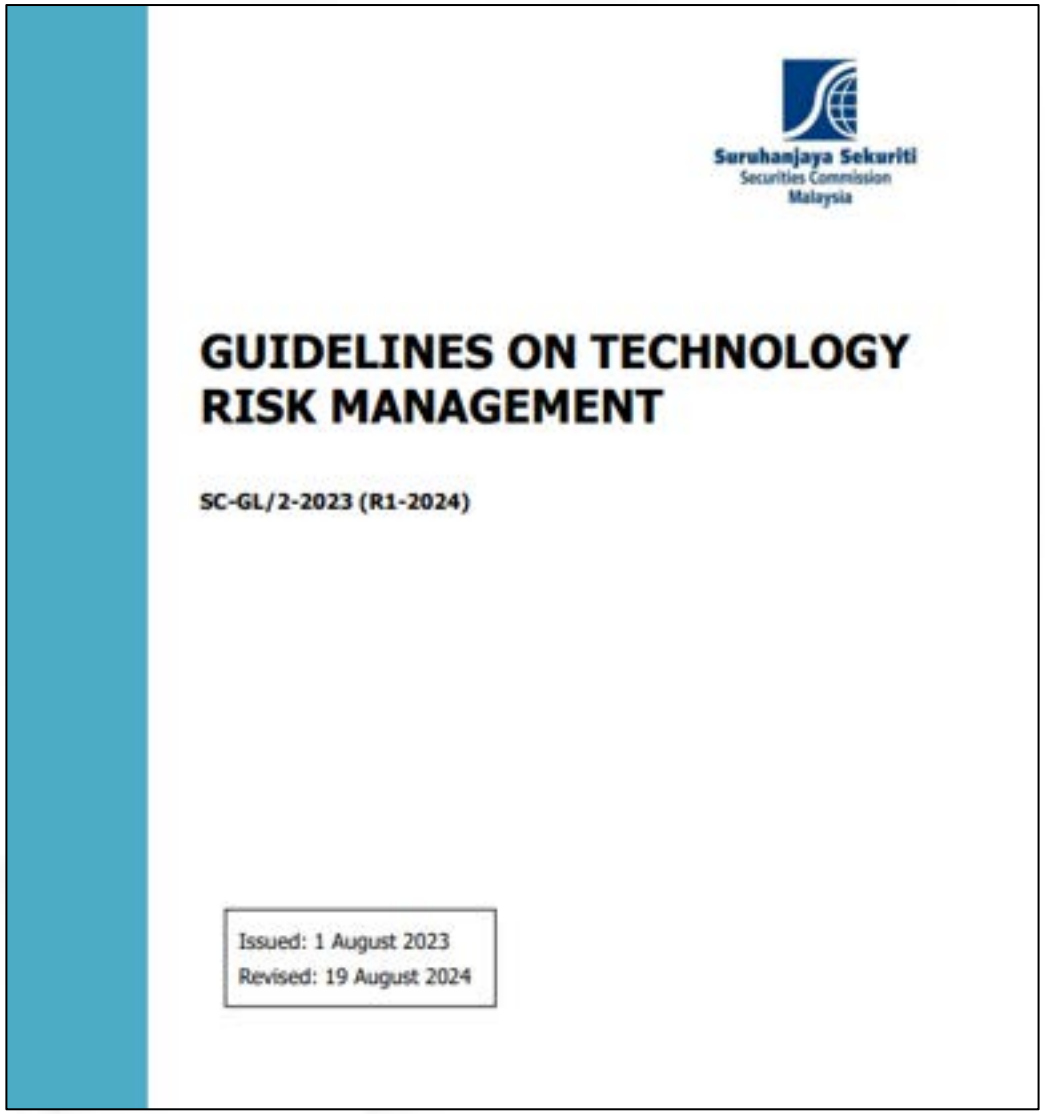
Cyber Resilience Framework (CRF):

- Helps digital banks build **resilience against cyberattacks** by ensuring their systems and operations can **withstand and recover from disruptions.**
- **Mandates incident response planning**, **disaster recovery testing**, and **ongoing monitoring of critical systems.**
- Aim to **minimize the impact of cyberattacks** on customers and operations.

2

PD-RMiT-June2023.pdf (bnm.gov.my)

SECURITY COMMISION



- **These guidelines broaden previous cyber risk requirements to cover various technology risks, emphasizing operational reliability, security, and resilience for capital market entities.**

- **Key focus areas include governance, change management, third-party service providers, reporting, technology audits, and board accountability, all aimed at bolstering the security and stability of Malaysia's capital market infrastructure.**

WHAT CAN COMPANIES DO OR WHERE CAN THEY GO TO FIND OUT WHAT IS CYBER SECURITY SAFE?

HOW CAN COMPANIES DO A TEST TO FIND VULNERABILITIES'?

WHO DO THEY TALK TO?

CYBERSECURITY IN MALAYSIA

CyberSecurity MALAYSIA

CyberSecurity Malaysia?

Cybersecurity Malaysia Operates in a Very Competitive Ecosystem…

MCMC
REGULATORY
(TELCO AND CONTENT RELATED)

MDEC
INDUSTRY
DEVELOPMENT

RMP
REGULATORY
(CRIME)

BNM
REGULATORY
(FINANCIAL)

NACSA, MKN
POLICY
MAKING

MAMPU
GOVERNMENT
ICT AUTHORITY

“Confusion in the market”

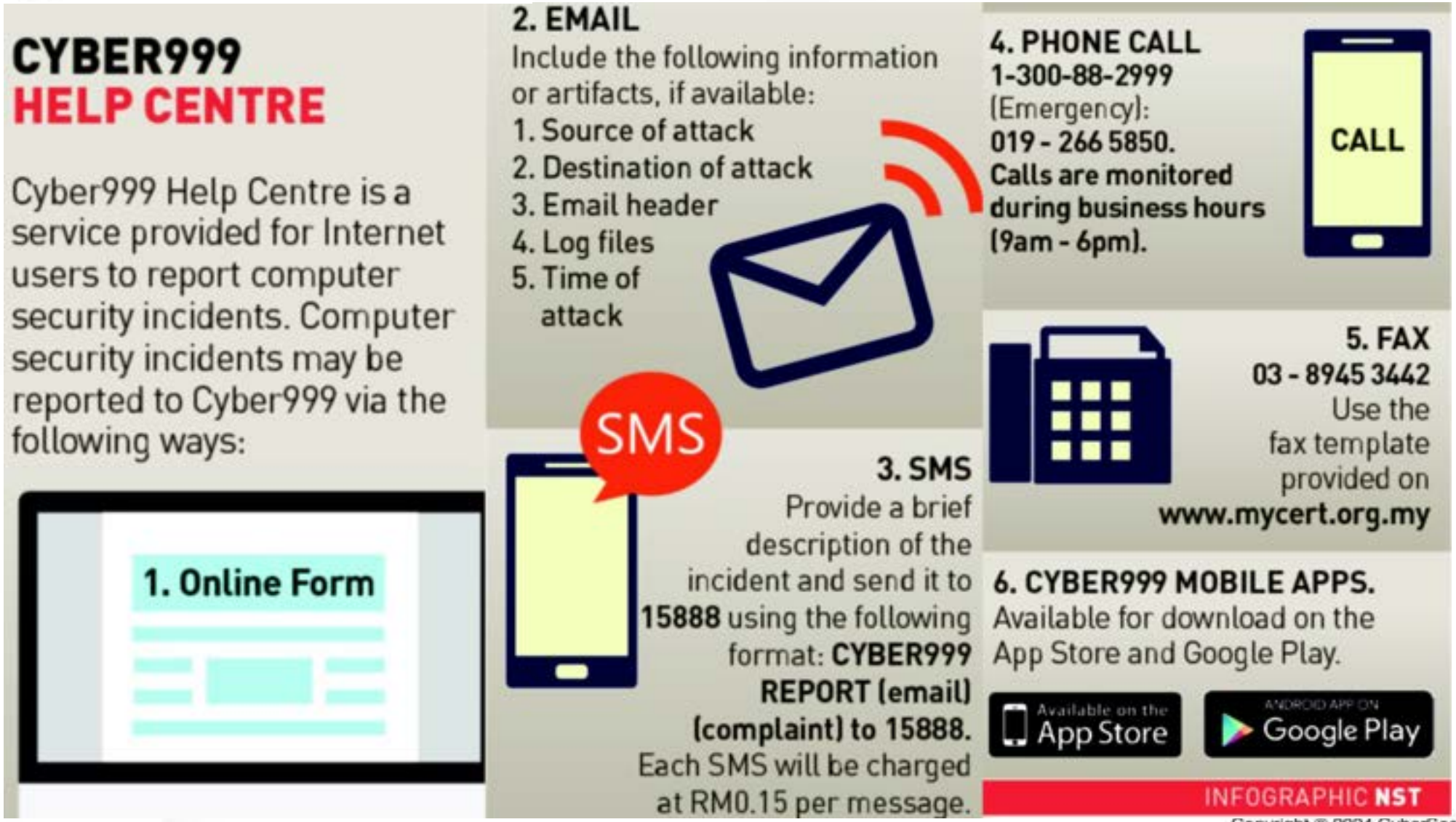
Who is doing what?

Who’s in charge of what?

Who do they go for help ?

NATIONAL SCAM RESPONSE CENTRE (NSRC)

Cyber999 (CYBERSECURITY MALAYSIA)



CYBERSECURITY MALAYSIA

CyberSecurity Malaysia Vision & Mission

VISION

World-class cyber security specialist agency

MISSION

Leading the development of a safer and more resilient cyber ecosystem to enhance national security, economic prosperity and social harmony through

- Provision of quality and impactful services
- Frontier-expanding cyber knowledge and technical supremacy
- Continuous nurturing of talent and expertise

SiberKASA

(Cyber Safety Empowerment Programme)

Objective: Empowering, strengthening and preserving the cyber security infrastructure and ecosystem in Malaysia so that it is always sustainable, protected and resilient.

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

PRODUCT / SERVICE — PRODUCTS AND SERVICES

HUMAN

PRODUCT

1. Global Accredited Cybersecurity Education (ACE)Scheme
2. CyberSAFE L.I.V.E Gallery
3. Cybersecurity Competency Training (CyberGuru)

SERVICE

1. CyberDrill Exercise
2. Behavioral Competency Assessment (BCA)
3. Cyber Safety Awareness for Everyone (CyberSAFE)
4. CyberSecurity Malaysia Awards, Conference & Exhibition (CSM-ACE)

PROCESS

PRODUCT

1. Information Security Governance, Risk & Compliance Health Check Assessment (ISGRiC)
2. ISMS Guidance Series
3. Information Security Management System(ISMS)

SERVICE

1. Business Continuity Management System (BCMS) Certification
2. Digital Forensics (DF) Case Management
3. Incident Handling Case Management
4. Cyber Discovery
5. MyTrustSEAL
6. Penetration Testing Service Provider(PTSP) Certification
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 Scheme (MyCC)
13. Cybersecurity Strategic and Technical Advisory

TECHNOLOGY

PRODUCT

1. Crypto Random Test Tool
2. X-Forensics Tools
3. PenDua Tool
4. Coordinated Malware, Eradication, and Remediation Platform (CMERP)
5. LebahNet
6. CamMuka (Facial Recognition)

SERVICE

1. MyCyberSecurity Clinic (MyCSC)- Data Recovery and Data Sanitization Services
2. Lab Quality Management
3. Cybersecurity Lab Services
4. CyberSecurity Malaysia Cryptographic Evaluation Lab (MyCEL)
5. CCTV Forensics Service
6. Cyber Threat Intelligence Service
7. Cloud Security Compliance Audit
8. Cloud Security Assessment Audit
9. Cloud Security Audit for ISMS
10. Security Operation Centre Service
11. Red Teaming Service

CYBERSECURITY MALAYSIA

EDUCATION AND AWARENESS

GLOBAL ACE CERTIFICATION

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSAFE
Cyber Security Awareness For Everyone

CyberSecurity MALAYSIA

"Let's Make The Internet A Safer Place"

CyberSAFE
Cyber Security Awareness For Everyone

BUILDING CYBER SECURITY MANAGERS, STRATEGISTS, AND PROFESSIONALS

GLOBAL ACE CERTIFICATION

Global ACE Certification was selected as one of the Champion Projects under Category 5: Building Confidence and Security in the Use of ICT at WSIS Prizes 2020

GOAL & OBJECTIVES

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 professional programmes globally

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

ADDRESSING CYBERSECURITY THROUGH PREVENTION MEASURES VIA FULL COMPLIANCE TO INTERNATIONAL STANDARDS & PROCESSES

Recognized and certified guarantee

ISO 17025 ACCREDITED LABORATORY

MySEF – Malaysia Security Evaluation Facility

Continuous audits conducted by Independent and Accredited Certification Bodies

- ISO27001- Information Security Management System
- ISO22301- Business Continuity Management System

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

Proactive Services

Information Security Certification Body (ISCB)

Information Security Certification Body (ISCB) is a department within CyberSecurity Malaysia that **manages certification services focusing on the information security according to international standards and guidelines**. Among the services under ISCB:

- Information Security Management System (ISMS) Audit and Certification - CSM27001 Scheme
- Privacy Information Management System (PIMS)
- Business Continuity Management System (BCMS)
- MyTrustSEAL – web security validation
- Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme

SEVERAL
CYBERSECURITY MALAYSIA TECHNOLOGY & SERVICES

DIGITAL FORENSICS (DF)

CyberCSI
crime scene investigation

CyberDEF
Uncovering Future Threats
Cyber Detect, Eradicate and Forensics (CyberDEF)


Evidence Preservation Facility

CyberDiscovery


Digital Forensics Lab

X-Forensics Tools

PenDua x-Forensik 2.0
Kloner x-Forensik 2.0

CamMuka V2.0


Expert Development Lab


Data Recovery Lab

MyCERT
Malaysia Computer Emergency Response Team

CMERP
Detection | Eradication | Remediation
Coordinated Malware Eradication & Remediation Project (CMERP)

LebahNET.MY
CyberSecurity Honeynet Project
Lebahnet (Honeynet Project)

MASSA

SECURITY THREAT
Cyber Early Warning


Technical Coordination Centre

CyberSecurity Malaysia malware research centre
Malware Research Center

Cyber Threat Research Centre (CTRC)

Computer Security Incident Response Team (CSIRT) Consultancy

Cyber999
Cyber999 Help Centre

SERVICE FOR THE ENHANCEMENT OF NATIONAL INFORMATION SECURITY ASSURANCE:

MyVAC (National Vulnerability Assessment Center)	MySEF (Malaysian ICT Security Evaluation Facilities)
• Vulnerability Assessment And Penetration Testing Services for CNII sectors	• Common Criteria (CC) evaluation service
• Security Assessment for control system (SCADA/DCS)	• ICT Product Security Assessment (IPSA) Service
	• Common Criteria (CC) Protection Profile (PP) evaluation service

MySEF
Malaysian Security Evaluation Facility

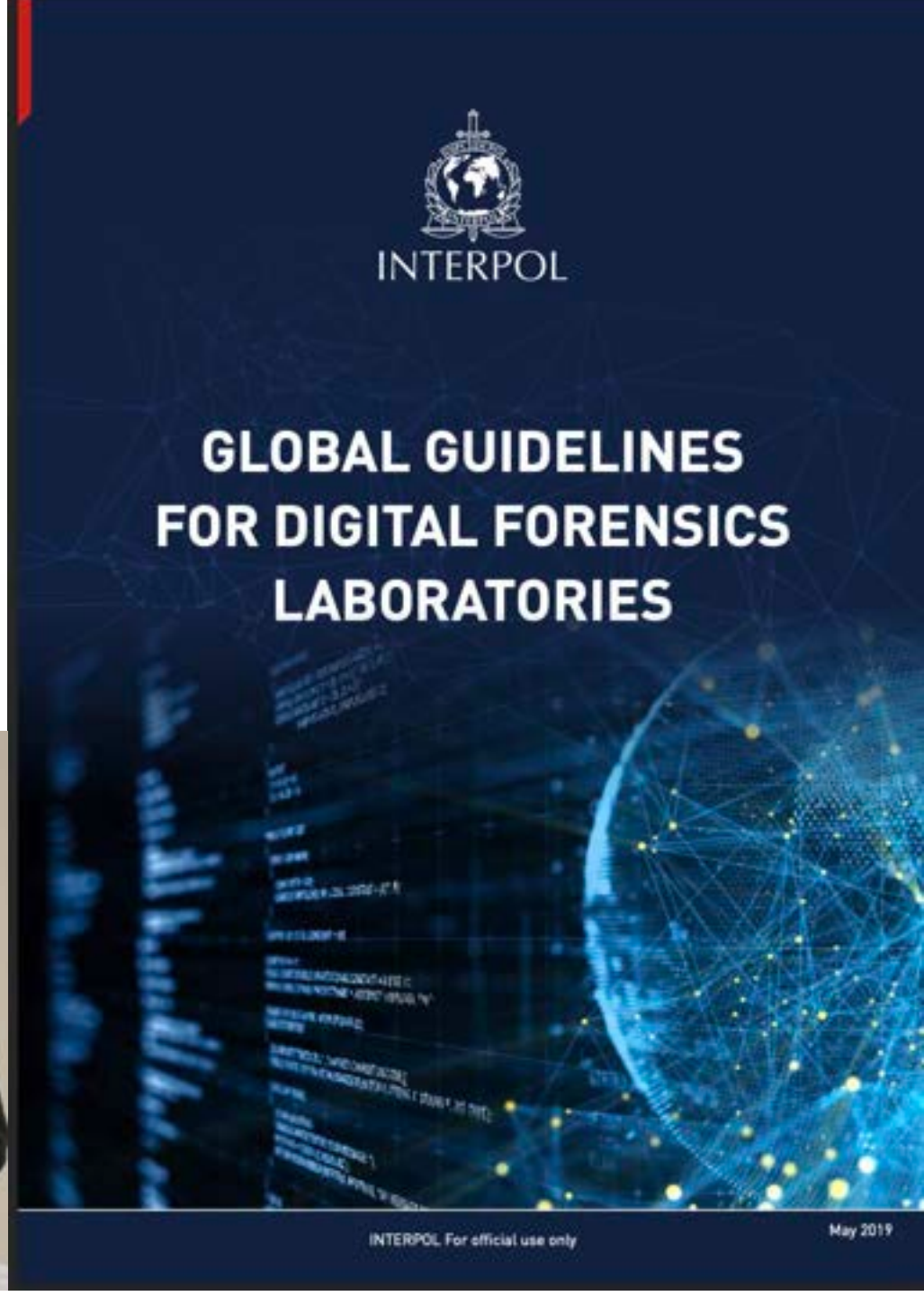
Cloud Security Services is a niche security service on cloud computing, focusing on cloud computing implementation on all types. Allow organizations to ensure secured cloud deployment and service subscription

Malaysia Policy & Procedure for cryptocurrency investigation & prosecution

- CSM drives initiative of developing procedure for cryptocurrency investigation & prosecution
- Will serve as standard procedure **for more than 20 LEAs in Malaysia**
- With the procedure, it ensures that process is accurate, able to preserve cryptocurrency evidence, and ensuring evidence admissibility into the court.
- The procedure was launched in late 2022.

INTERPOL Global Guidelines for Digital Forensics Laboratories

- CSM initiatives collaboration with INTERPOL in developing the Global Guidelines for Digital Forensics Laboratories.
- The objective of this document is to assist members countries in developing own forensic lab
- It was launched to 97 members countries in 2019 in Sao Paolo.



Malaysia's Virtual Asset Forensic Investigation Capacity & Capability

Internal Capability Development

Conference presentation

Best Paper Award

Recognition as Regional Expert for Cryptocurrency Investigation

65

Malaysia's Virtual Asset Forensic Investigation Capacity & Capability

CyberSecurity Malaysia Initiative

Awareness & trainings to Malaysia Law Enforcement & Regulatory officers

Guidelines for Search & Seizure of cryptomining machines

CSM x United Nations initiatives

RESPONSIVE TECHNOLOGY: CERTIFIED LABORATORY

1) Digital Forensics Lab - ANSI National Accreditation Board(ANAB)
2) Data Recovery Lab
3) Cyber Crime Scene Investigation (CSI) Lab
4) Cyber Discovery Lab
5) Cyber Detect, Eradicate and Forensics (CyberDEF)
6) *Cyber Security X Lab UTM*

Digital Forensic Lab

Cyber Threat Lab

1) MyCERT Security Operation Centre
2) Coordinated Malware Eradication & Remediation Platform (CMERP) Lab UteM
3) Cyber Early Warning System Lab (CEWS)
4) Malware Research Centre
5) Cyber Threat Research Centre Lab (CTRC)

20 LABORATORY

1) Vulnerability Assesment Lab - MS ISO/IEC 17025:200
2) Internet of Things (IoT) Security Lab
3) Secure Software Development Life Cycle Lab SSDLC
4) Industrial Control System (ICS) Security Lab)
5) Robotic Lab
6) ICT Product Assesment (IPSA) Lab
7) ICT Security Evaluation Facility - ISO/IEC 17025

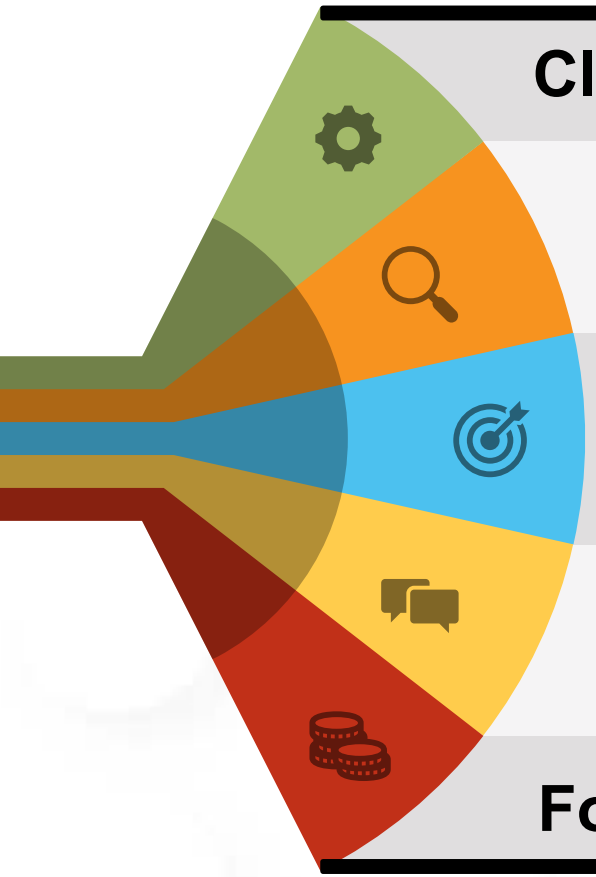
Assesment & Evaluation Lab

Cryptography Lab

1) Cryptanalysis Lab
2) Cryptography Evaluation Lab) - ISO/IEC 17025:2005 National Voluntary Laboratory Accreditation Program (NVLAP)

HOW DO MALAYSIA STACKS UP IN CYBERSECURITY?

Malaysia is among the better-prepared ASEAN states on paper (strong laws, institutions, CERT, funding increases) and scores in the top tier of the ITU Global Cybersecurity Index (GCI 2024).



Clear and active policy and legal frameworks

Institutional footprint with a strong national agencies

Increasing cybersecurity budget/spend

Regional leadership and commitment

Focus on infrastructure and talent

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

CONCLUSION AND WAY FORWARD

- There is no such thing as 100% security. There is still much improvement to be made. We need to increase and strengthen our cybersecurity manpower and professional skills.

- There is a need to ensure for a secure, resilient and trusted cyber environment in order to sustain progression and prosperity. In this regard, a more innovative and proactive adaptive security approach is required to address such situations. Adaptive cybersecurity encompasses predictive, detective, responsive and corrective capabilities.

- In addition, our approach also has to be adaptive, dynamic and innovative covering people, process and technology.

- Strengthening Public-Private-Academia Partnership and national, bilateral, regional and International Collaboration.

- Malaysia should gear itself towards cyber resilience as the threat of a global cybersecurity breach continues to pose a major risk.

MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

THANK YOU

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 1 300 88 2999

www.cybersecurity.my | enquiry@cybersecurity.my

CyberSecurityMalaysia | cybersecuritymy | cybersecuritymy | CyberSecurity Malaysia | cybersecurity_my | cybersecuritymy

DIGITAL MALAYSIA MADANI

ASEAN MALAYSIA 2025

Recognition of Excellence 2023 CyberSAFE by OpenGov