

IC-AJCC



# CHALLENGES OF RISK MANAGEMENT AND GOVERNANCE IN THE CURRENT CYBERSECURITY LANDSCAPE: Operational Best Practices

6<sup>th</sup> October 2023

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



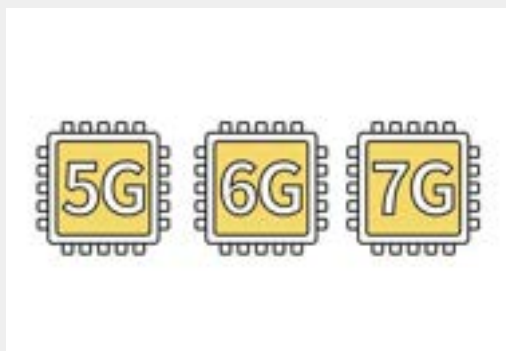
Copyright © 2023 CyberSecurity Malaysia

# WE ARE MOVING INTO A MORE INTERCONNECTED CYBERSPACE

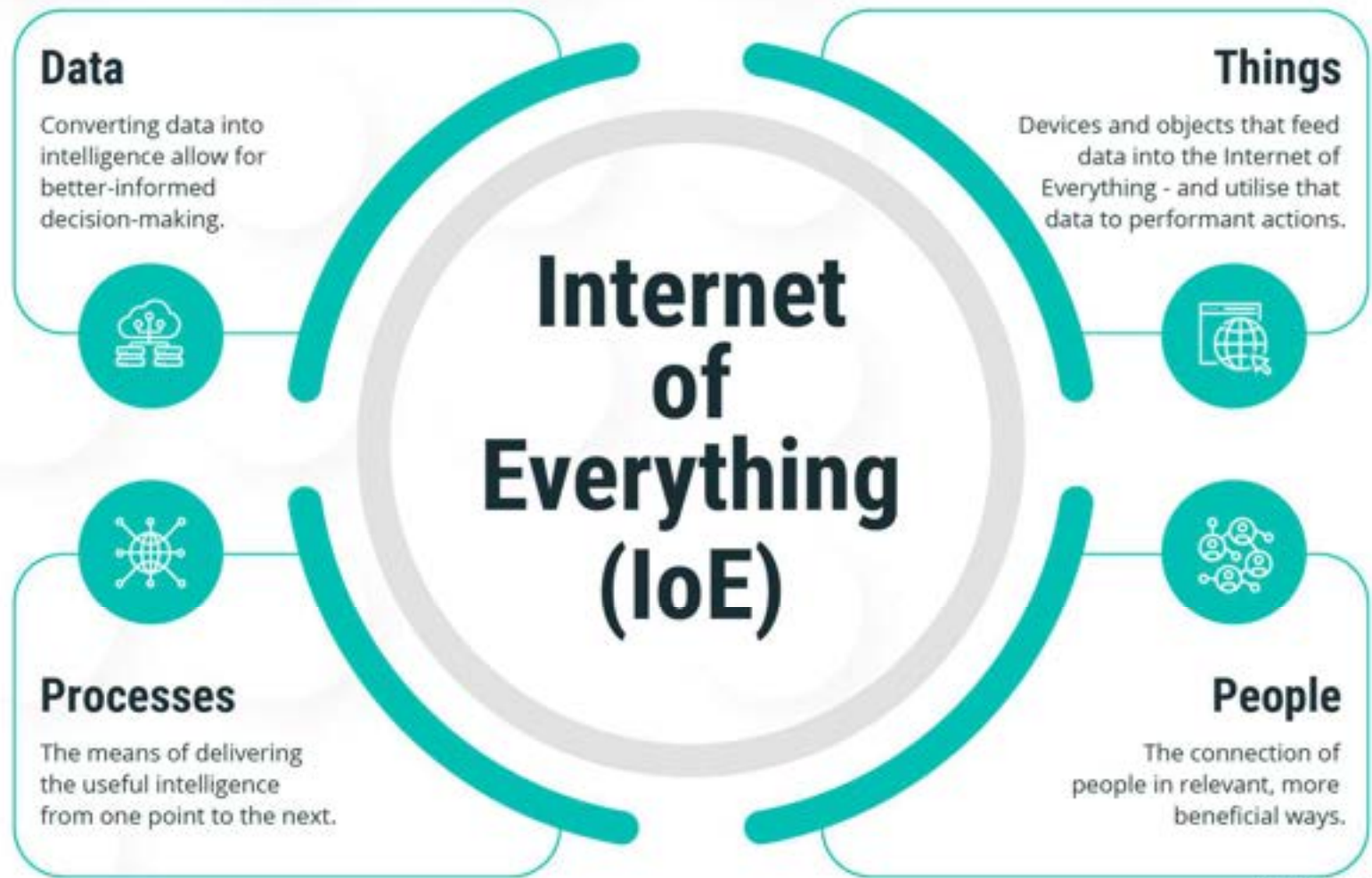


# CONVERGENCE OF TECHNOLOGIES

Add More Complexities to Cyber Space and Digital Transformation



# The World Has Become Heavily Reliant And Connected To One Another Whether It's People, Process And Technology



# IT VS OT VS IOT VS IOE

**Information Technology (IT):** The computer, data storage, and networking infrastructure and processes that are used to create, process, store, secure, and exchange all forms of electronic data. It deals with data, information and communication.

**Operational Technology (OT):** Traditionally, physical devices in industrial, agricultural, and mission-critical sectors or Industrial IoT networks. It deals with machines.

**Internet of Things (IOTs):** Networks not specific to a particular sector.

**Internet of Everything (IoE):** extends beyond IoT by integrating operational technology (OT) and information technology (IT) into a unified ecosystem, enabling seamless communication, data sharing, and intelligent decision-making.

The World Are More Interconnected,  
Opening new opportunities



# THE LANDSCAPE IS **CATALYSED** WITH IR4.0 AND DIGITAL TRANSFORMATION



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



In Phase 2 (2023-2025), inclusive digital transformation will be prioritized.

In Phase 3 (from 2026 to 2030) will position Malaysia as a regional leader in digital content and cyber security. MyDIGITAL's mission is to ensure that all Malaysians benefit from the opportunities of the digital revolution.

## CYBER-ATTACKS MAY HAVE PHYSICAL CONSEQUENCES



Cyberattacks On Vehicles Pose A Threat To Drivers And Manufacturers



# DIGITAL TRANSFORMATION IS NOT WITHOUT ITS RISK

- Technology such as wireless technology has changed the way we conduct business, offering workers with constant access to business-critical applications and data.

- While this flexibility is convenient and expands productivity, it introduces complexity and security risk as these new technology and devices become new target for hackers looking to infiltrate a corporate network.

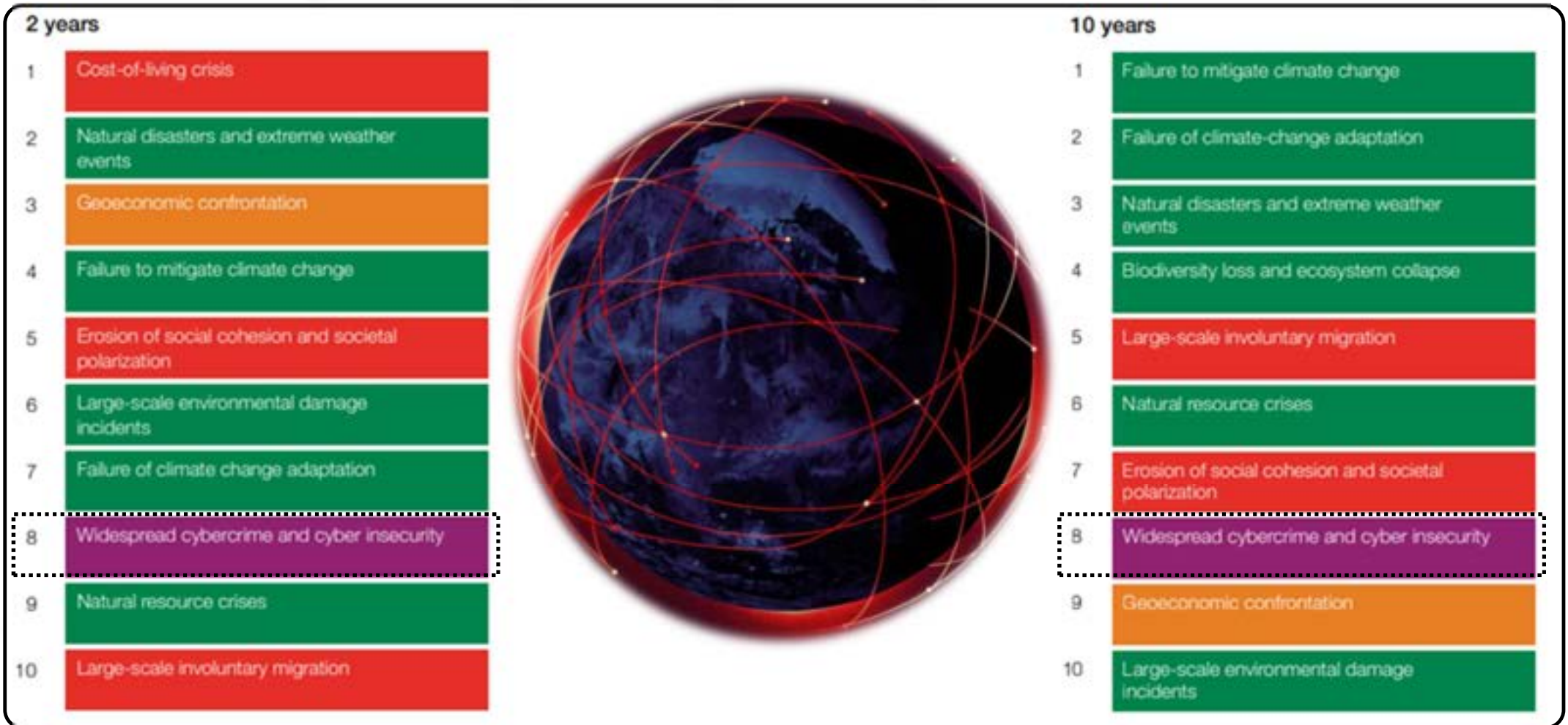


# CYBER RISK

'Cyber risk' means any **risk of financial loss, disruption or damage to the reputation** of an organization from some sort of **failure of its information technology systems**. Hence, **CYBER RISK MANAGEMENT** is needed!



# GLOBAL RISK 2023



# UNDERSTANDING HOW TO HANDLE EACH RISK

- Action is taken to do something different.
- The threat is eliminated

**AVOID**

- No actions are taken.
- Risk is acceptable.

**ACCEPT**

- Actions taken to reduce the probability and impact of risk.
- Implementing relevant controls.

**MITIGATE**

- Shifting the responsibility and impact to a third party.

**TRANSFER**

- Sharing risk with the higher authority or with a third party.

**SHARE**





**RISK MANAGEMENT  
AND GOVERNANCE  
BEST PRACTICES**

# Risk Management And Governance Best Practices

# CYBER HYGIENE

Refers to fundamental cybersecurity **best practices** that an organization's security practitioners and users can undertake.

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 		2 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 

# RISK MANAGEMENT BEST PRACTICES

## INTEGRATED AND CONSISTENT CONTROLS AND POLICIES

A consistent, systemic and integrated approach to risk management can help determine how **best to identify, manage and mitigate significant risks.**

## GAIN BOARD AND MANAGEMENT SUPPORT

Ensure strategic **direction** are **aligned** and resource are **allocated properly**



# RISK MANAGEMENT BEST PRACTICES

## MONITOR THE RISK ENVIRONMENT

Management can act promptly if and when the nature, potential impact, or likelihood of **the risk goes outside acceptable levels**

## IDENTIFY AND UNDERSTAND ONE'S RISK ENVIRONMENT

A process of **documenting any risks** that could keep an organization or program from reaching its objective

## COLLABORATION WITH EXTERNAL PARTIES

Collaborating with external parties can help **identify and mitigate supply chain risks** that can disrupt operations.



# GOVERNANCE BEST PRACTICES



## HOLISTIC APPROACH

A holistic approach to governance includes various elements within an organization or a government in a comprehensive manner.



## ADAPTIVE APPROACH

Adaptive security is a security approach that's used to respond to potential cyberthreats in real-time by continually monitoring user sessions.



## ZERO TRUST

Continuous verification. Always verify access, all the time, for all resources or simply put it as "Trust No One".



## DEFENCE-IN- DEPTH

A multifaceted approach to safeguard the organization's overall well-being, compliance, and ethical standards.

# GOVERNANCE BEST PRACTICES



## TRAINING & AWARENESS

Promote awareness and training programs to inform the clients or shareholders of their responsibilities and functions within an organisation.

## COLLABORATION

Sharing of information, resources, and expertise among various national and international entities to collectively address cyber threats.

SOURCE: <https://www.datamation.com/big-data/data-governance-trends/>



# RISK IS EVERYBODY'S RESPONSIBILITY

CYBERSECURITY DOES  
NOT OPERATE IN SILO!

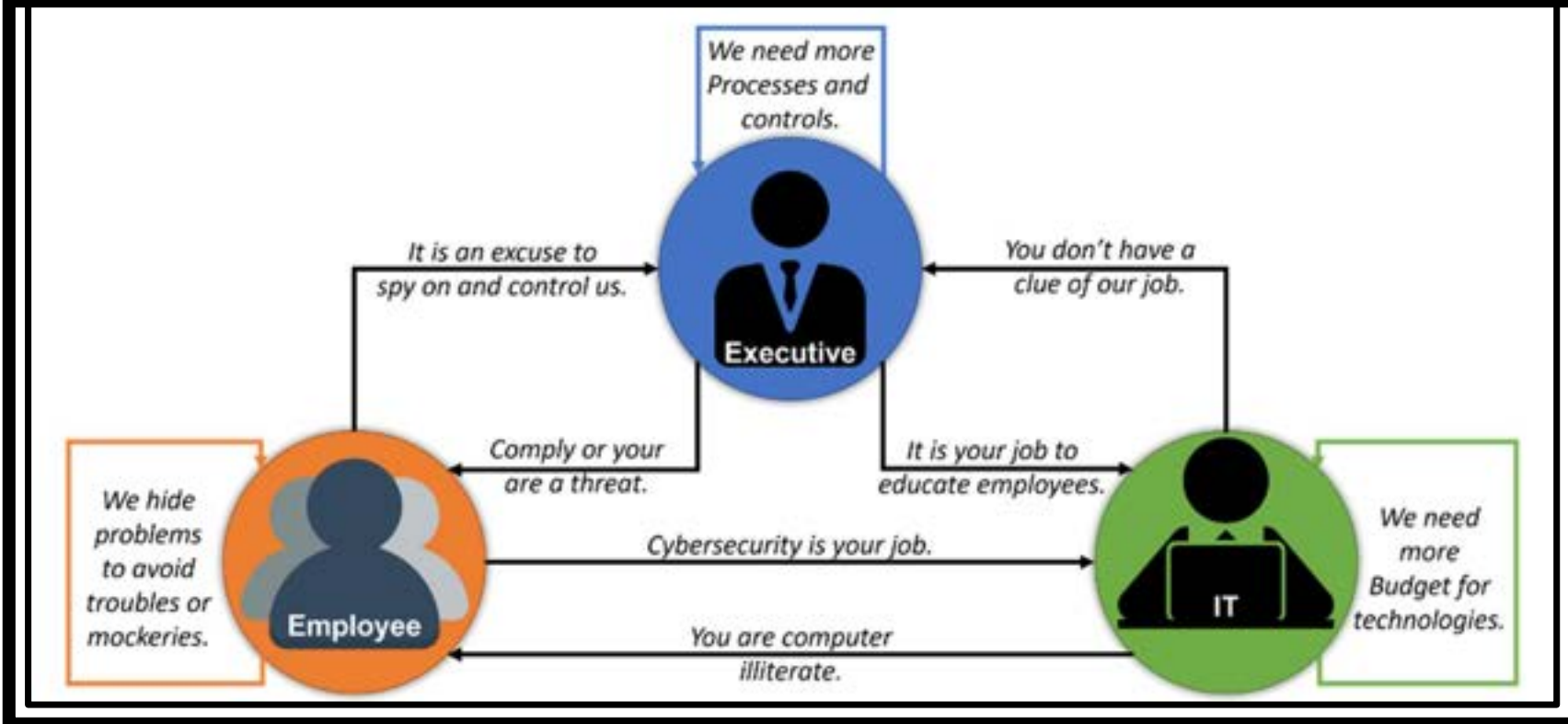
THE MANAGEMENT MUST  
SHOW THE EXAMPLE, BY

# LEADING

THE ORGANISATION IN  
**ENHANCING**  
**CYBERSECURITY**



# CYBERSECURITY, RISK MANAGEMENT, AND GOVERNANCE: A SHARED RESPONSIBILITY





# CYBERSECURITY MALAYSIA'S INITIATIVES

---



# SiberKASA

OFFICIAL LAUNCH ON 23 MARCH 2021

CSM initiatives aimed at developing, empowering, sustaining and strengthening cybersecurity infrastructure and ecosystem in Malaysia to ensure network security preparedness.



**CYBERSECURITY MALAYSIA'S INITIATIVES**

# HOLISTIC APPROACH

Adoption of holistic approach that identifies potential threats to organization and impacts to the national security & public well-being ; and

To develop the nation to become **cyber resilience** having the **capability** to safeguard the interests of its stakeholders, reputation, brand and value creating activities.



## (Program PemerKASAan Keselamatan Siber)

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

### HUMAN

Covers aspects of skills, knowledge, ethics, behavior and talent

### PROCESS


Covers aspects of policy development, strategy, Standard Operating Procedure (SOP), recognition of international standards

### TECHNOLOGY


Involves technology in particular matters related to minimizing vulnerabilities, digital forensic analysis, malicious code (malware) and data

### PRODUCTS AND SERVICES

P  
R  
O  
D  
U  
C  
T

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

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

- 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)

S  
E  
R  
V  
I  
C  
E

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

- 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

- 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

The image features five dark silhouettes of people standing in a row against a light gray background with a faint grid pattern. Each silhouette is overlaid with various data points, including numbers and small colored circles (red, green, blue). A white rectangular box is centered over the silhouettes, containing the word "PEOPLE" in large, bold, white capital letters. The overall aesthetic is digital and data-driven.

# PEOPLE

# CYBERSECURITY CAPACITY BUILDING FRAMEWORK

**GLOBAL ACE**  
Global Accredited Cybersecurity Education (ACE) Scheme

**Global ACE Scheme**

<https://www.cybereducationscheme.org>

**CyberGuru**

CYBER SECURITY PROFESSIONAL DEVELOPMENT

**Cyberguru**

<https://www.cyberguru.my>

**CyberSAFE™**

**Cybersafe**

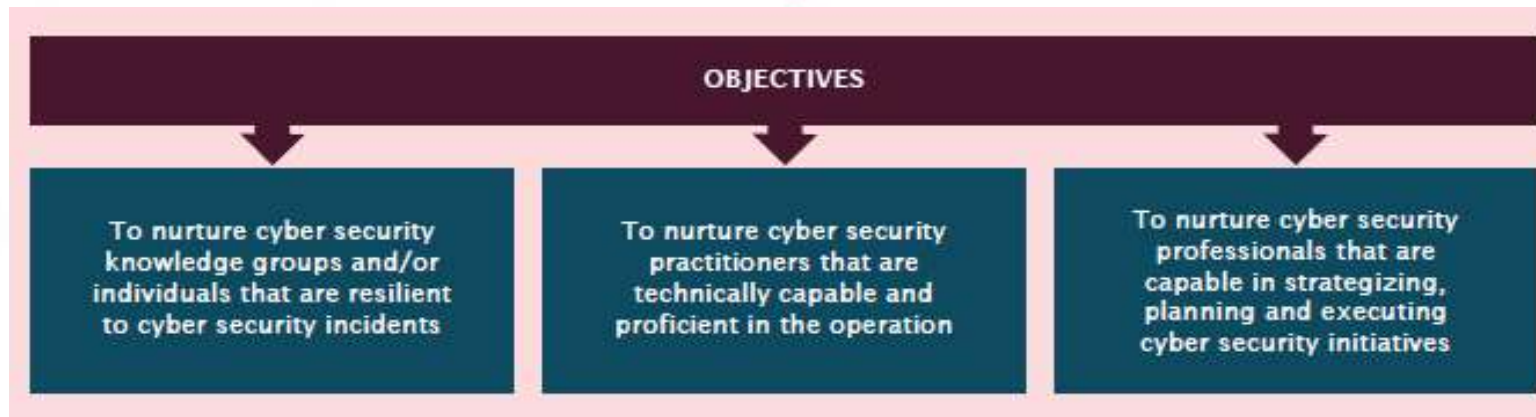
<https://www.cybersafe.my>



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



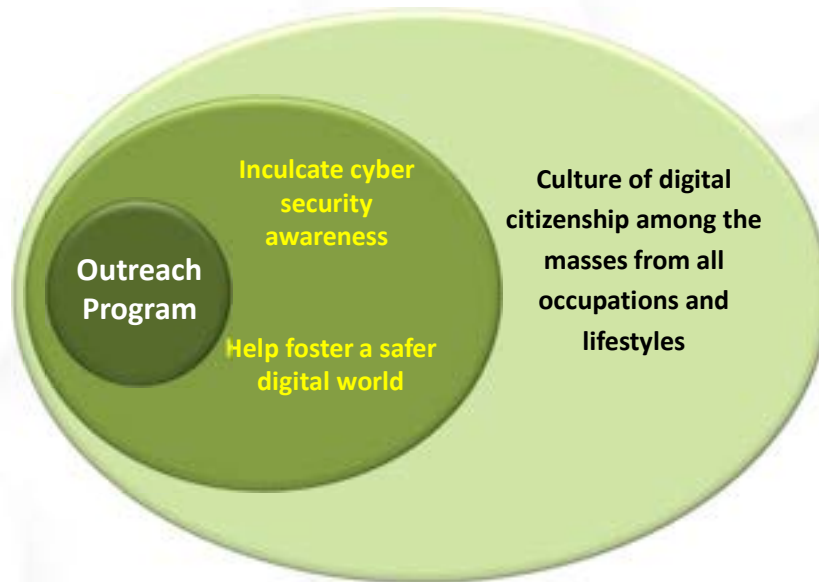


# CYBERSECURITY AWARENESS FOR EVERYONE (CyberSAFE)



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

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



# DEVELOP CYBERSECURITY PROFESSIONALS

## CyberGuru

### Cyber Security Capacity Development Collaboration

CyberSecurity Malaysia bundles its training programs into selected local and international training programs and work closely with industry collaborators to further enhance, deliver and market these services effectively and efficiently.

### Cyber Security Academic Collaboration



# BUILDING CYBER SECURITY MANAGERS, STRATEGISTS AND PROFESSIONALS

## GLOBAL ACE CERTIFICATION



Global ACE Certification was selected as the Winner of the 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

# GLOBAL ACE CERTIFICATION TRAINING PROGRAMMES



## 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

# PROCESS



WAWASAN KEMAKMURAN BERSAMA

2030



### Rancangan Malaysia Kedua Belas (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



## SiberKASA



CSM's Role in **Supporting National Cybersecurity Related Policies & Strategic Plans**

National Technical Cybersecurity Agency responsible to **advise & implement** cybersecurity related programs



### Kerangka Strategik KKD

- 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



### 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)

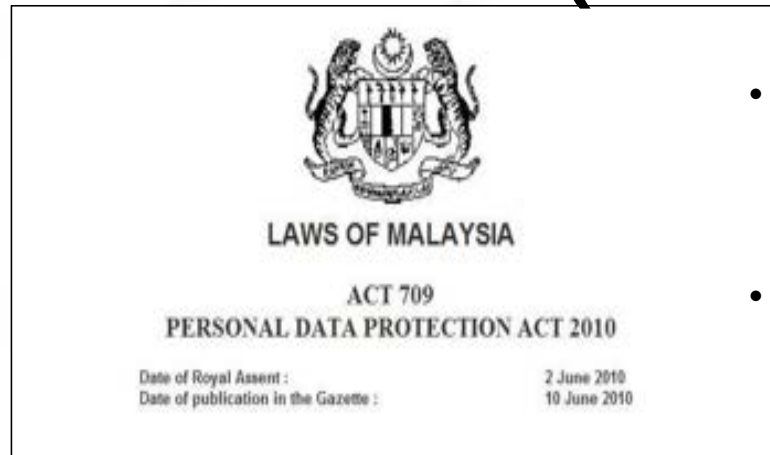
- Thrust 1:** Equip the Rakyat with 4IR knowledge and skill sets
- Thrust 3:** Future-proof regulations to be agile with technological changes

# Personal Data Protection Act 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 Act 2010 (Act 709)



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

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

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

## Malaysia urgently needs comprehensive cybersecurity laws, says PM

By MAZWAN NIK ANIS



# ADDRESSING CYBERSECURITY ISSUES THROUGH GUIDELINES

## 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



# ADDRESSING CYBERSECURITY THROUGH ENCRYPTION TECHNOLOGY



- **NATIONAL CRYPTOGRAPHY POLICY** approved by The Government In January 2013

- Comprehensive applications of cryptography in Government to Government (G2G), Government to Citizens (G2C), Government to Business (G2B) and Business to Business (B2B) activities towards ensuring a secure and trusted cyber environment.

- Cryptography also supports the National Digital Economy and the realization of the National Transformation Agenda to transform Malaysia into becoming an advanced and high-income nation



## 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

# MANAGEMENT SYSTEM CERTIFICATION



**Process Certification**

**Continuous Audits conducted by Independent and Accredited Certification Body**

**ISO/IEC 27001**  
**Information Security Management Systems**

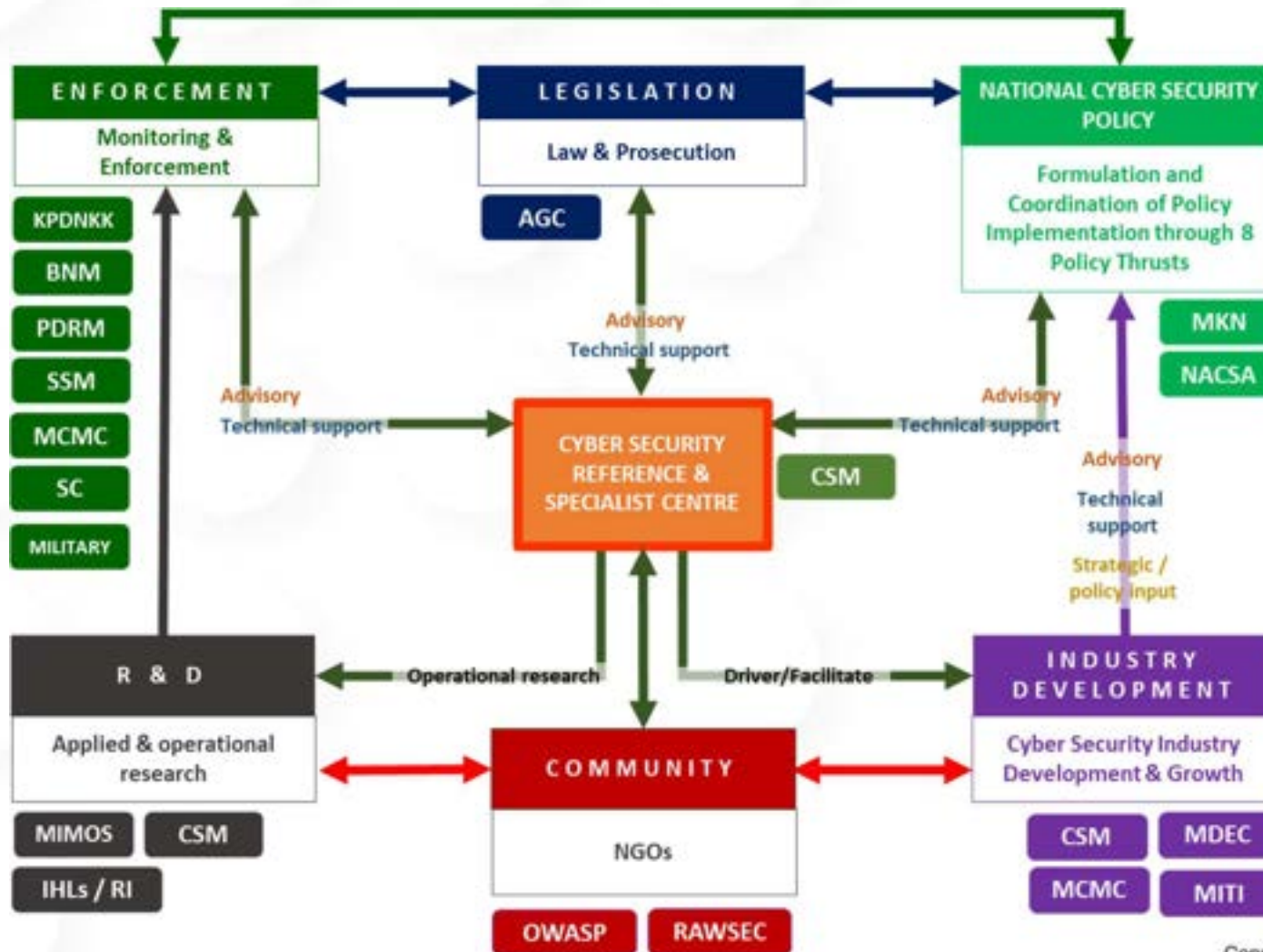
Specifies requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization which includes requirements for the **assessment and treatment of information security risks** tailored to the needs of the organization.

**ISO 22301**  
**Business Continuity Management Systems**

Specifies requirements to plan, establish, implement, operate, monitor, review maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, **respond to and recover from disruptive incidents when they arise.**

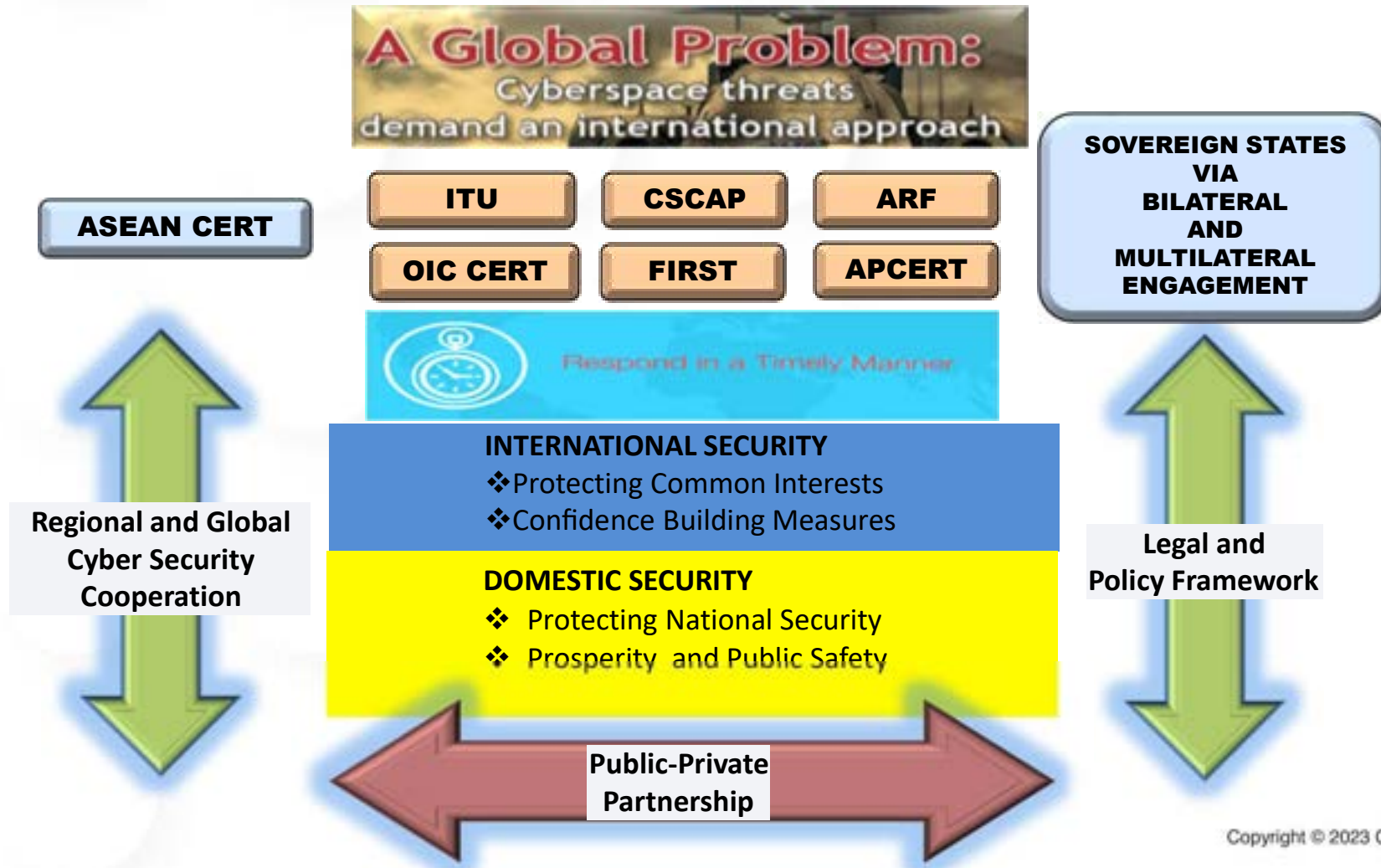
## DOMESTIC COLLABORATION

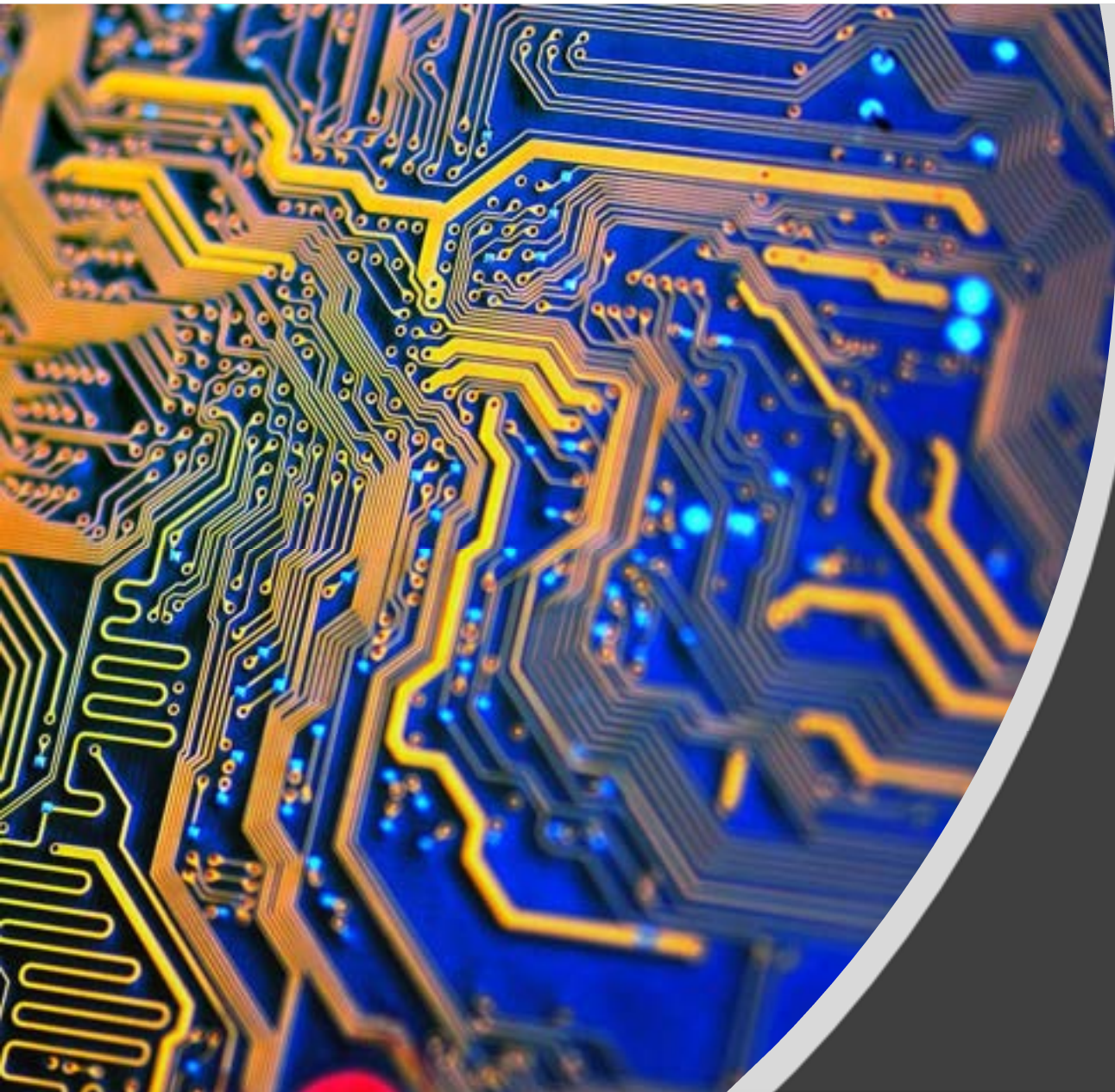
# CYBERSECURITY MALAYSIA ENGAGEMENT ECOSYSTEM



# INTERNATIONAL COLLABORATION

## - Global Collaborative Efforts And Engagements





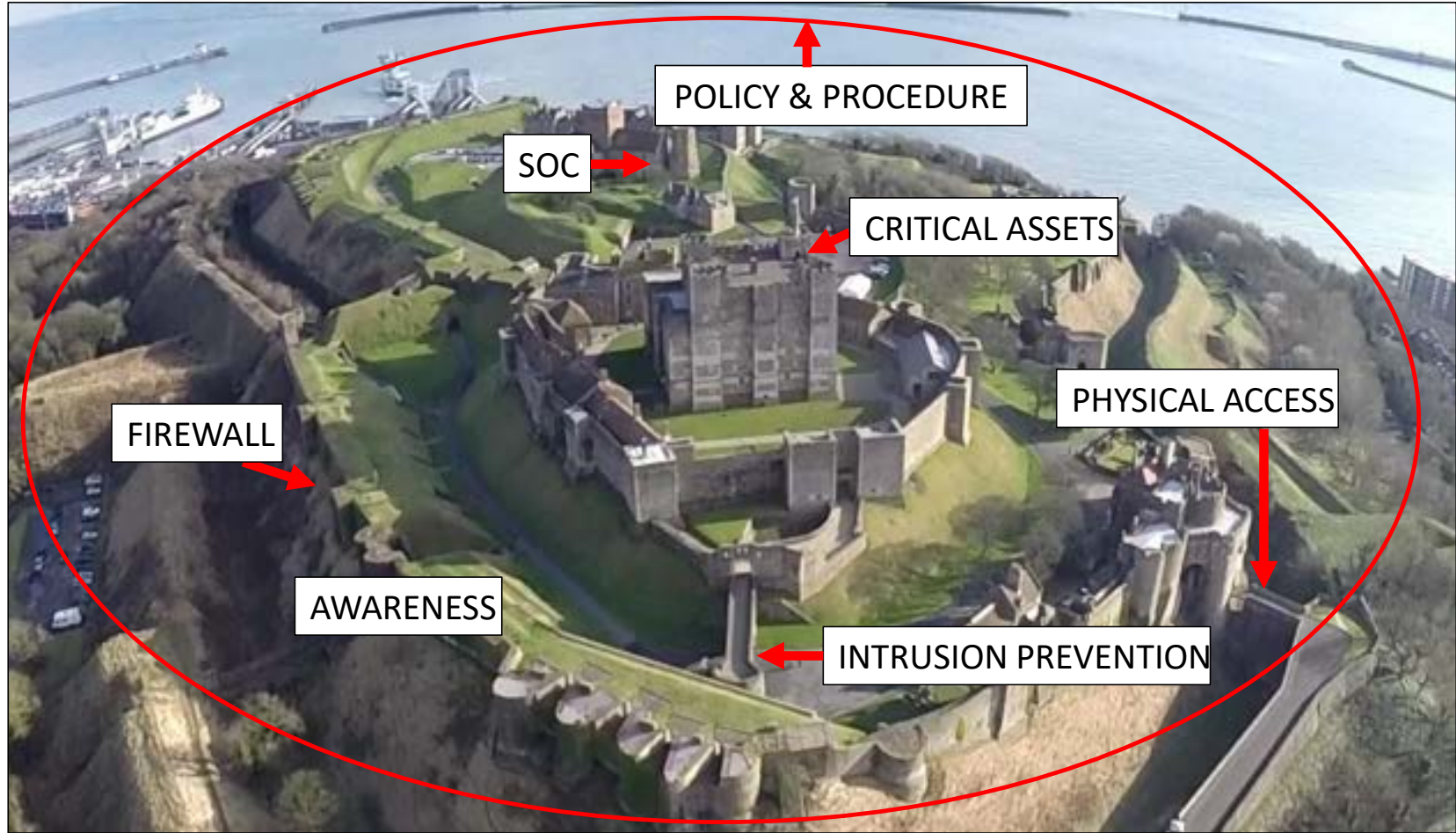
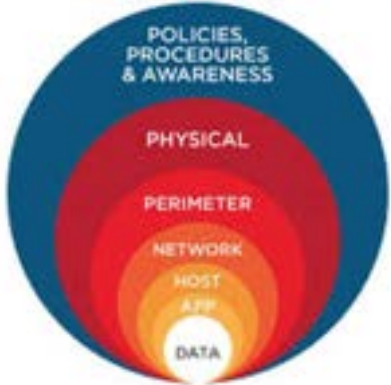
**TECHNOLOGY**

# TRADITIONAL CYBERSECURITY APPROACH

- Not sufficient to deal with smart cyber threats

Protecting networks, data and devices in today's environment requires a multipronged approach that accounts for every possible vulnerability and entry point. We are way beyond firewalls and antivirus here.

## DEFENSE IN DEPTH



This is an approach that relies on using a layered and redundant defensive mechanism to protect data and assets from cyber-attacks.

# ADDRESSING CYBER RESILIENCY THROUGH **ADAPTIVE SECURITY**

## To be more proactive, dynamic and integrated in cybersecurity approach

Adaptive Security is an approach to cybersecurity that **analyzes behaviors and events** to protect against and **adapt** to threats before they happen. With an Adaptive Security Architecture, an organization can **continuously assess risk and automatically provide proportional enforcement** that can be dialed up or down

### PREDICTIVE

- Periodic Vulnerability assessment
- Threat hunting
- Cyber threat intelligence

### RESPONSIVE

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



### PREVENTIVE

- Server hardening
- Security patching
- Source code review

### DETECTIVE

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



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



# STRENGTHENING CYBERSECURITY THROUGH PREDICTIVE CYBER THREAT INTELLIGENCE (CTI)



AHMAD FAUZI (dua dari kanan) dan Amiruddin (dua dari kiri)

## Makmal khas tangani serangan siber

Oleh AHMAD ISYAFIQ MAD, DESA

**JOHOR BAHRU** - Universiti Teknologi Malaysia (UTM) mengubah makmal khas bertujuan melaksanakan kajian mengenai kaedah menangkis serangan siber yang semakin merular 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 je-

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

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



# ADDRESSING CYBERSECURITY THROUGH RESPONSIVE TECHNOLOGY & SERVICES

## DIGITAL FORENSIC (DF)

**CyberCSI**  
Crime Scene Investigation

**CyberDEF**  
Discovering Future Threats

Cyber Detect, Eradicate and Forensics (CyberDEF)



Evidence Preservation Facility

**CyberDiscovery**



Digital Forensic Lab

### X-Forensics Tools

**PenDus**  
x-forensics 1.0

**Kloner**  
x-forensics 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



Cyber Threat Research Centre (CTRC)



Computer Security Incident Response Team (CSIRT) Consultancy

**malware**  
research centre

Malware Research Center

**Cyber999**

Cyber999 Help Centre

# STRENGTHENING CYBER SECURITY **PREVENTION** THROUGH TECHNOLOGY VULNERABILITY ASSESSMENT

Secure Software Development Lifecycle (SSDLC) Lab & Services



Internet of Things (IOT) Lab



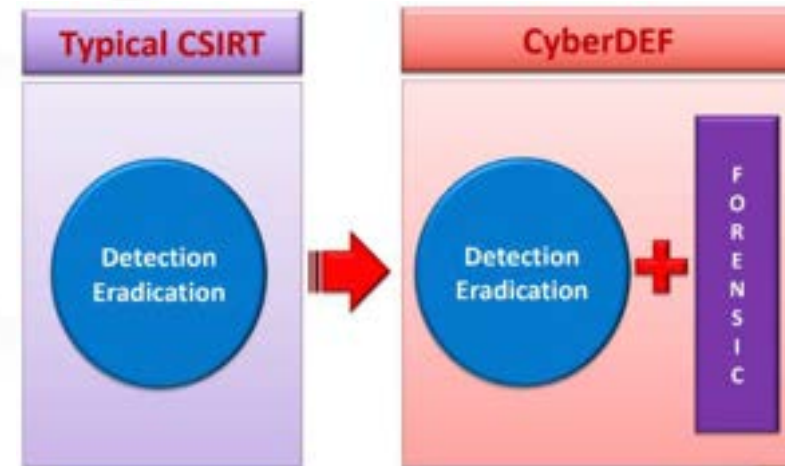
Robotic Lab (4<sup>th</sup> Industry Revolution)



# ADDRESSING CYBERSECURITY THROUGH STRENGTHENING DETECTION TECHNOLOGY

## CyberD.E.F

- Detection
- Eradication
- Forensic



Detection	Eradication	Forensics
<p>Identify any loopholes, vulnerabilities and existing threats</p> <ol style="list-style-type: none"> <li>1. Sensors</li> <li>2. Sandbox</li> <li>3. Analytics</li> <li>4. Visualization</li> </ol>	<p>Close loopholes, patch vulnerabilities and neutralize existing threats</p> <p>Perform cyber threats exercise or drill to test the feasibility and resiliency of the new defense / prevention system</p>	<ol style="list-style-type: none"> <li>1. E-Discovery</li> <li>2. Root cause analysis</li> <li>3. Investigation</li> <li>4. Forensics readiness</li> <li>5. Forensic compliance</li> </ol>



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 adversaries
  - + 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.

## CONCLUSION AND WAY FORWARD

- ❖ There is no such thing as 100% security. There is still much room for improvement. We need to increase and strengthen our cybersecurity manpower and professional skills.
- ❖ This involves an ongoing process of identifying security risks and implementing plans to address them. Risk is determined by considering the likelihood that known threats will exploit vulnerabilities and the impact they may have on valuable assets.
- ❖ Furthermore, there is a need to ensure a secure, resilient, and trusted cyber environment to sustain progress 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.
- ❖ Additionally, our approach also needs to be adaptive, dynamic, and innovative, covering people, processes, and technology.





# 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 +61 300 88 2999

[www.cybersecurity.my](http://www.cybersecurity.my) | [info@cybersecurity.my](mailto:info@cybersecurity.my)

