MDBC 2023

MINISTRY OF COMMMUNICATIONS AND DIGITAL

CyberSecurity MALAYSIA

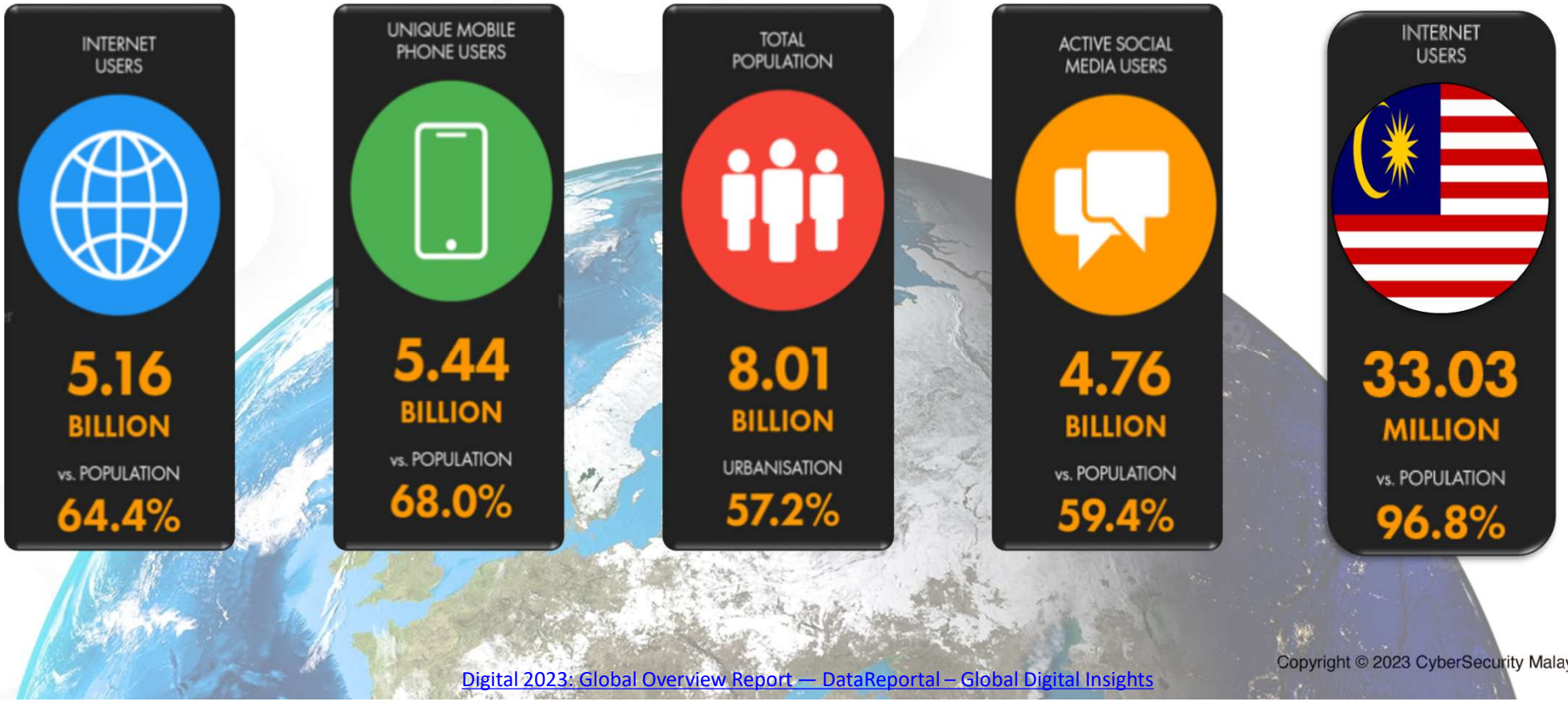
Cyber Hygiene
And Cyber Resilience

20 JULY 2023

Ts. DR. SOLAHUDDIN BIN SHAMSUDDIN
Chief Technology Officer
Cybersecurity Malaysia

SECURING OUR CYBERSPACE

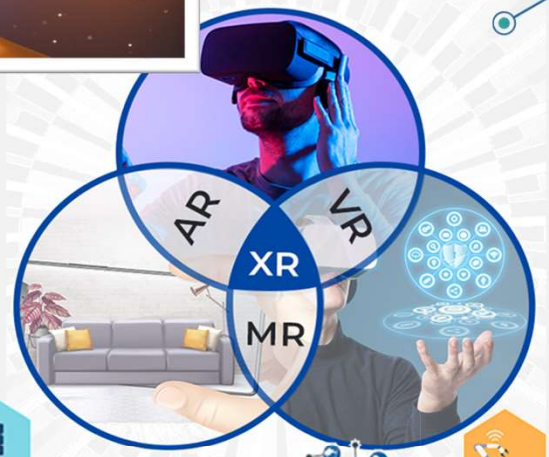
WE ARE MOVING INTO A MORE INTERCONNECTED CYBERSPACE

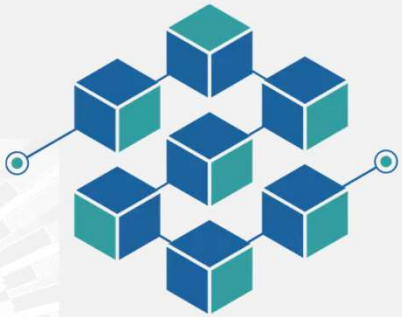


Digital 2023: Global Overview Report — DataReportal – Global Digital Insights

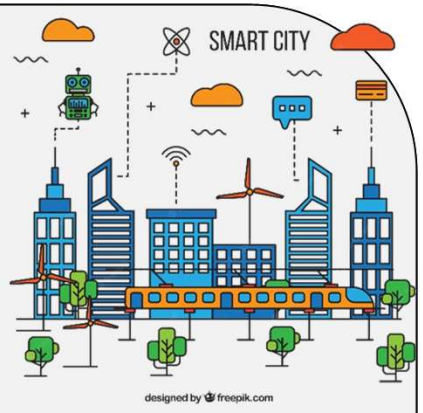
CONVERGENCE OF TECHNOLOGIES

Add More Complexities to Cyber Space



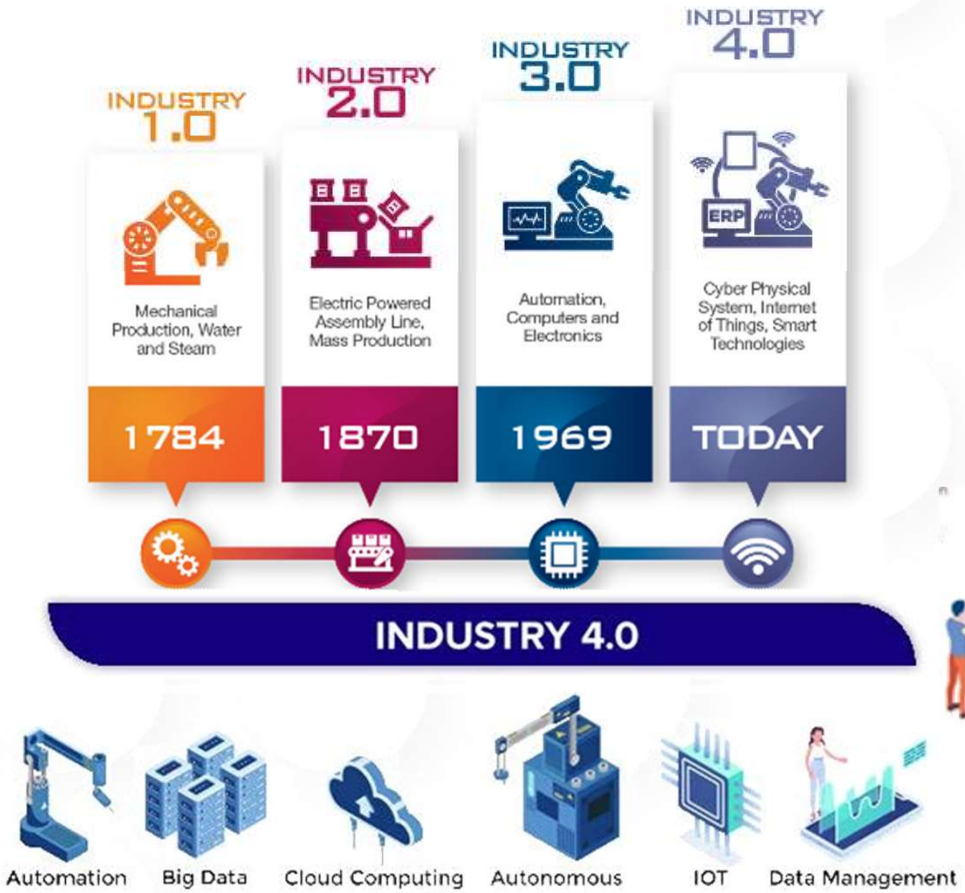


BLOCKCHAIN

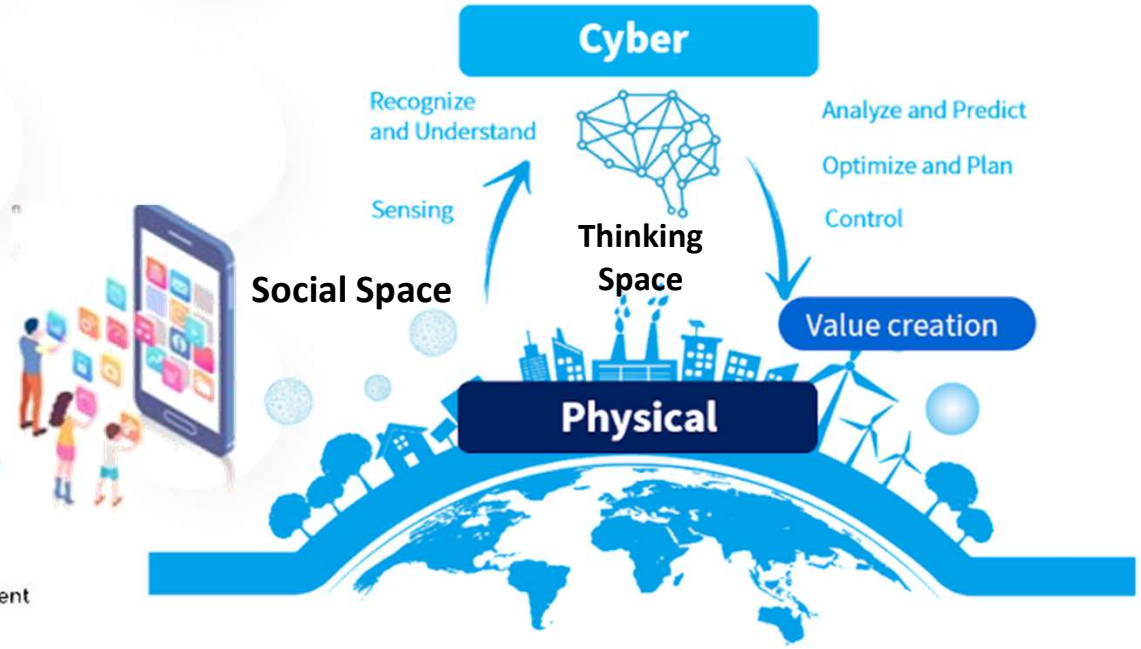


DIGITAL TRANSFORMATION

CyberSecurity MALAYSIA

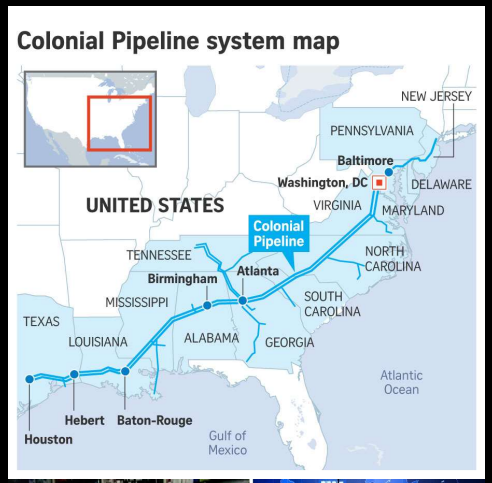


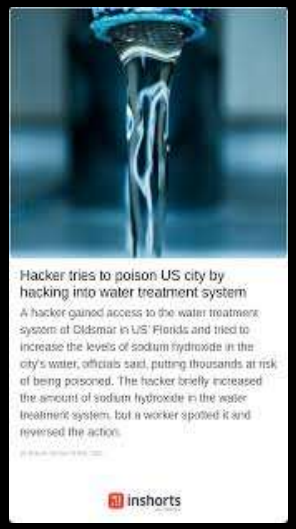
A Smart World whereby there is deep convergence between the new cyberspace and the traditional ones such as physical, social and also thinking space.

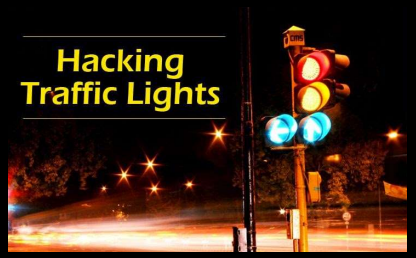


DIGITAL TRANSFORMATION IS NOT WITHOUT ITS **RISK**

CYBER-ATTACKS MAY HAVE PHYSICAL CONSEQUENCES







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.

GLOBAL RISK 2023

2 years

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

10 years

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

Source: WEF_Global_Risks_Report_2023.pdf (weforum.org)

EVOLUTION OF CYBER THREATS

THE MORE WE'RE **INTERCONNECTED** TO THE CYBER SPACE

THE MORE WE ARE AT **RISK TO CYBER THREATS**

CYBER THREATS BECOMING MORE **ACTIVE AND EVOLVING**

PAST

Password guessing

Password cracking

GENERAL CYBER ATTACK

- Less complex
- Less sophisticated

PRESENT

Advance scanning

Packet of spooling

Denial of service

DIRECTED CYBER ATTACK

- Fairly complex
- Relative sophisticated

FUTURE

Bots

Morphing

Malicious Codes

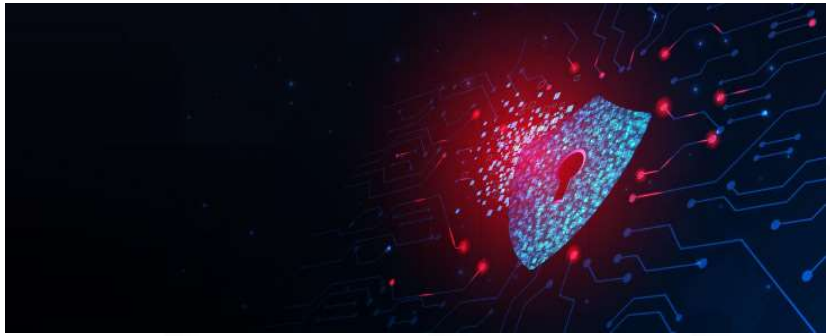
STRATEGY CYBER ATTACK

- Very complex
- Highly sophisticated

THE MORE WE ARE INTERCONNECTED THE MORE WE ARE EXPOSED GLOBALLY

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

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

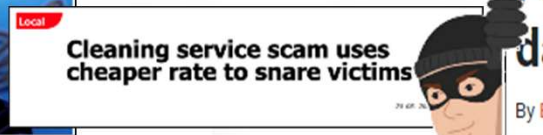
by The Gurus — May 19, 2023 in Featured

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)

CYBERCRIME OCCURS EVERYWHERE EVEN IN MALAYSIA



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

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".

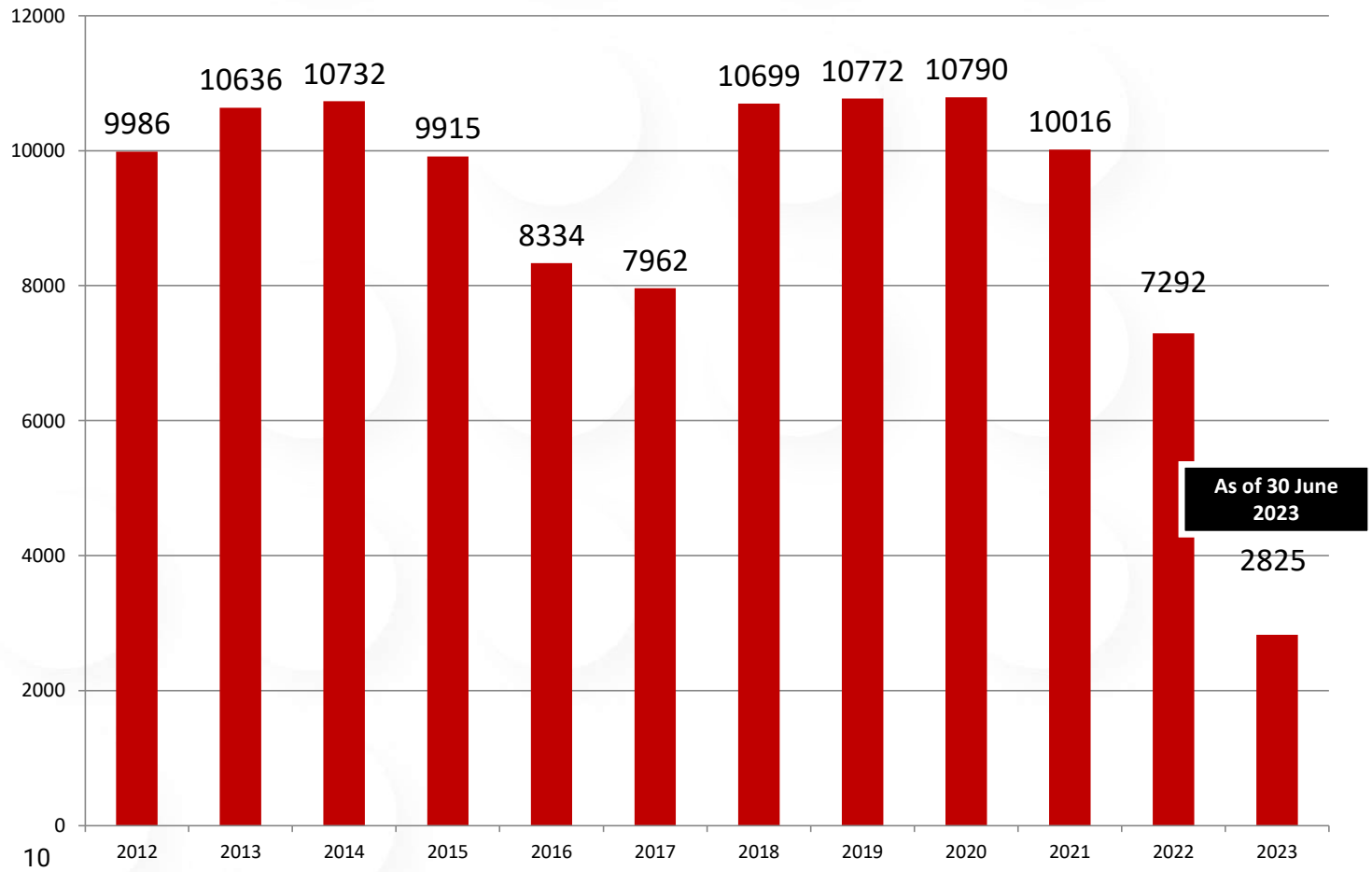
By Aqasha Nur'aiman — 04 Apr 2023, 02:24 PM — Updated about 2 months ago

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

CYBER INCIDENTS REFERRED TO CYBERSECURITY MALAYSIA (2012 – 30 June 2023)



MyCERT Incident Statistics

Security Alert

TOP FOUR CYBER INCIDENTS IN MALAYSIA (CYBER999)

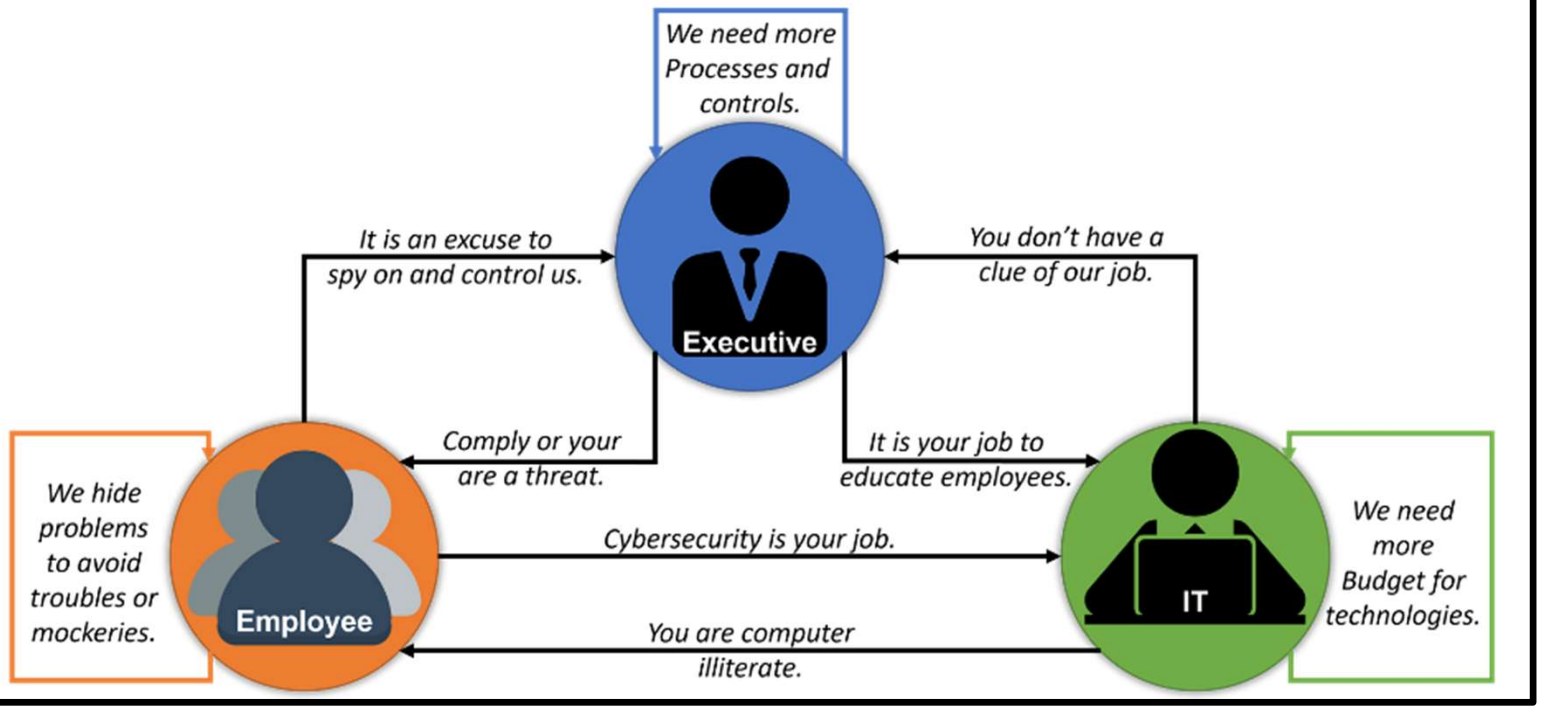
1. **Fraud**
2. **Malicious Code**
3. **Intrusion**
4. **Content Related**

Types of incidents

1. **Intrusion**
2. **Intrusion Attempt**
3. **Denial of Service Attack (DOS)**
4. **Fraud**
5. **Spam**
6. **Content Related**
7. **Vulnerabilities Report**
8. **Malicious Codes**

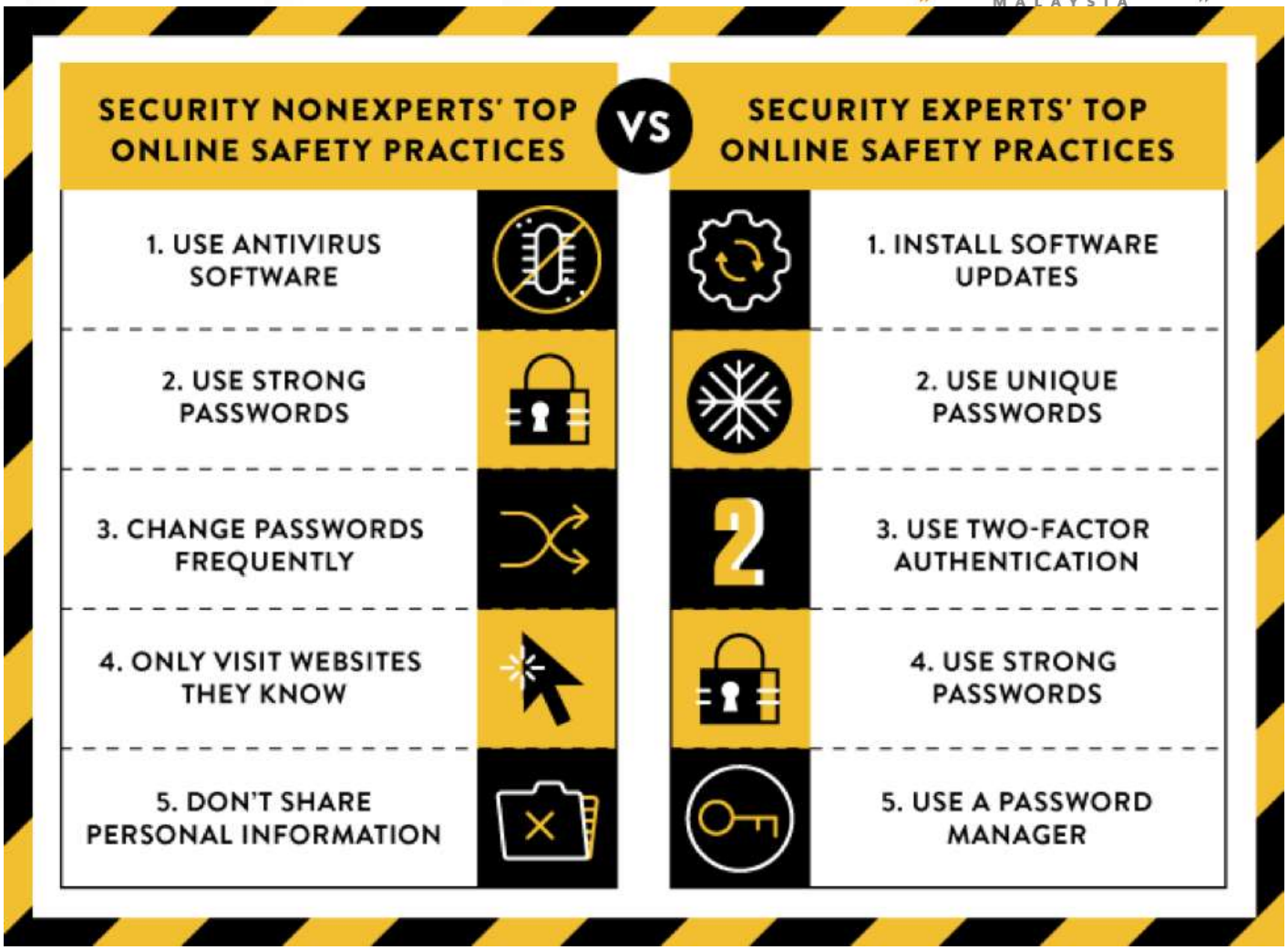
CYBERSECURITY IS A SHARED RESPONSIBILITY

CYBERSECURITY AND CYBER RESILIENCE: A SHARED RESPONSIBILITY



CYBER HYGIENE

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



Practice Great Cyber Hygiene - Cyber Risk Opportunities

Cyber Resilience – so much more than Cybersecurity

No matter how secure is an organization, there is **no such thing as 100% secure**

It is no longer the question of **how to secure oneself** from being attack

It's just a **matter of time** that a cyber-attack can occur to an organization. Similarly, human error can also affect a business's operations and render it incapable of serving its customers.

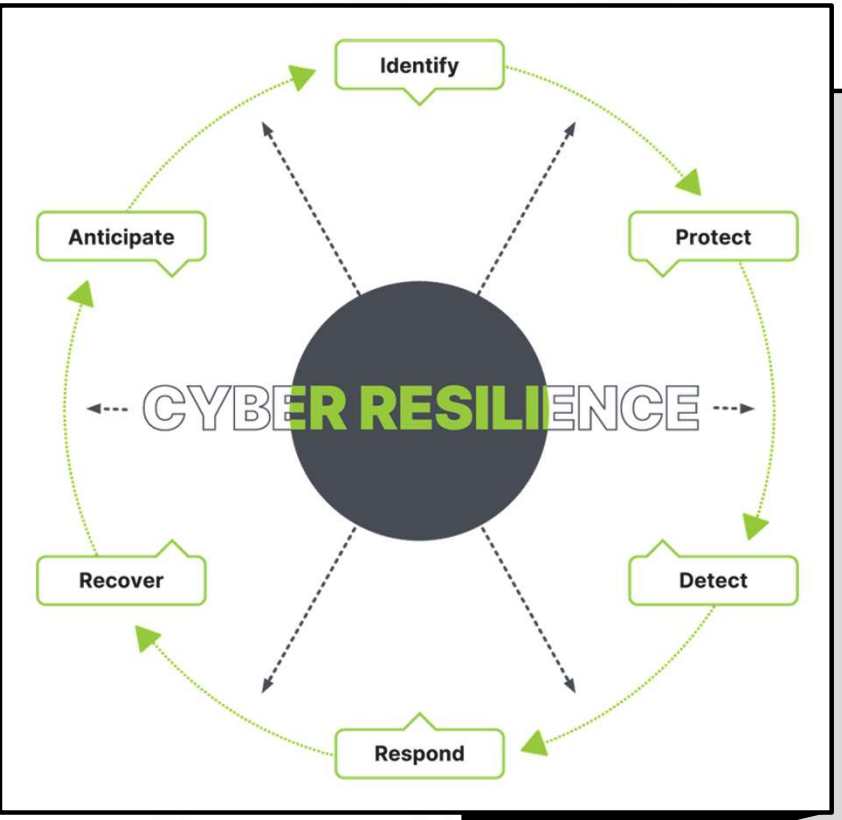
Hence, what is more important is that the organisation try their **best to strategize** in order to lessen the impact due to cyber-attacks. It is crucial to know **how to act and recover or bounce back once being attacked**

CYBERSECURITY VS CYBER RESILIENCE

CYBERSECURITY	CYBER RESILIENCE
Definition: **procedures followed**, or measures taken to **ensure the safety** of a state or organisation	**Definition**: the capacity to **recover quickly** from difficulties; **toughness**
Technologies and processes are **designed to protect** an organisation from **cybercrime**	Technologies and processes designed to **keep delivering intended services** in spite of **cyber incidents**
Works to **reduce the risk of cyber-attacks** and to **protect the organisation** from **cyber theft/ espionage**	Works to ensure **continuity on a wider scope**, **comprising cybersecurity** and **business requirements**
Can work effectively without **compromising** the usability of **other systems**	Requires **organisation-wide culture shift** that normalises and embeds **security best practices**
Includes a **business plan** to **resume operation** in the event of a **successful attack**	Requires the organisation to become **agile and adaptable** in the **face of cyber-attacks and incidents**

Action/plan/program in reducing risk and implementing security approach	**Action/plan/program upon occurred incidents and what to do next**

Cyber Resilience



– so much more than Cybersecurity

- Traditional security measures are no longer enough to protect a company's data and network security.
- Improve security system, internal process and work culture.
- It provides many benefit to an organization such as to increase their security posture and reducing the risk of exposure to their infrastructure.
- Helps reduce financial loss and reputational damage.
- Inspires trusts in its clients and customers.

CyberSecurity Malaysia's Initiatives

CyberSecurity MALAYSIA

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

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

SiberKASA

(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.

PEOPLE	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

People

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

Process

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

Technology

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

People

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

Process

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

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


PEOPLE

CYBERSECURITY CAPACITY BUILDING FRAMEWORK

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

Cyberguru
https://www.cyberguru.my

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

OBJECTIVES

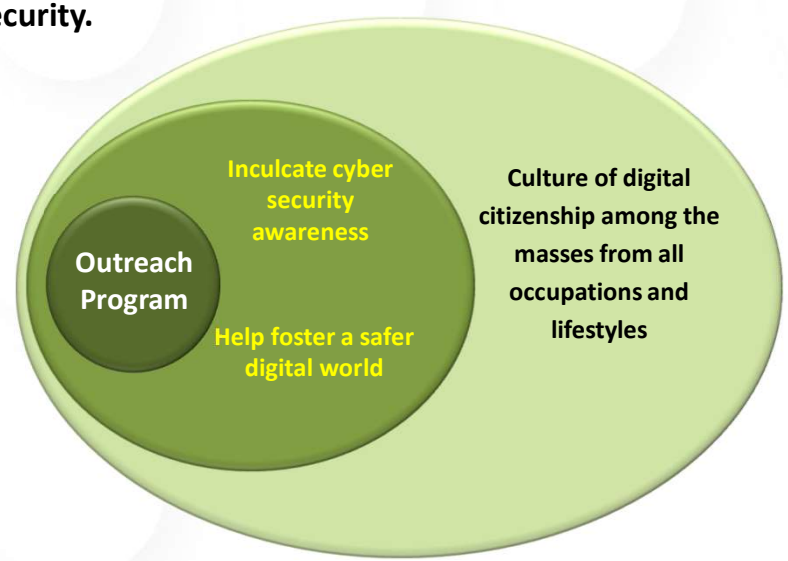
- To nurture cyber security knowledge groups and/or individuals that are resilient to cyber security incidents
- To nurture cyber security practitioners that are technically capable and proficient in the operation
- To nurture cyber security professionals that are capable in strategizing, planning and executing cyber security initiatives

CYBERSECURITY AWARENESS FOR EVERYONE (CyberSAFE)

CyberSAFE
Cyber Security Awareness For Everyone

- **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 PROGRAMMES

1. Certified Cyber Security Awareness Educator (CCASE)
2. Certified Information Security Awareness Manager (CISAM)
3. Certified Penetration Tester (CPT)
4. Certified Secured Applications Practitioner (CSAP)
5. Certified Security Operations Centre (CSOC)
6. Certified Data Security Analyst (CDSA)
7. Certified Digital Forensics First Responder (CDFFR)
8. Certified Information Security Management System Auditor (CISMSA)
9. Certified MyCC Evaluator
10. Certified Incident Handling and Network Security (CIHNS)
11. Certified IP Associate
12. Certified IT Associate
13. Certified IoT Security Analyst
14. Certified Cybersecurity Data Science Analyst
15. Certified Mobile Security Analyst
16. Certified Cyber Law Practitioner
17. Certified Cybersecurity Risk Manager
18. Certified Industrial Control System Security Analyst
19. Certified Secure Web Application (PHP) Developer
20. Certified Smart Card Reader Analyst
21. Certified Cloud Security Auditor
22. Certified IoT Blockchain Practitioner
23. Certified Cyber Forensics Analyst
24. Certified Web Application Penetration Tester
25. Certified Data Privacy Officer
26. Certified Data Privacy Specialist
27. Certified Chief Data Privacy Officer
28. Certified Cryptocurrency Seizing Officer

BUILDING CYBER SECURITY MANAGERS, STRATEGISTS AND PROFESSIONALS

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

PROCESS

MCD 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

Twelfth 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

SiberKASA

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

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

Malaysia Digital Economy Blueprint (MyDIGITAL)

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 (Industry4WRD)

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

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

ADDRESSING CYBERSECURITY THROUGH POLICY

STRATEGI KESELAMATAN SIBER MALAYSIA
CYBER SECURITY STRATEGY

5 PILLARS
12 Strategies

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

MALAYSIA'S DIGITAL ECONOMY BLUEPRINT

6 STRATEGIC THRUSTS,
22 STRATEGIES,
48 NATIONAL INITIATIVES AND
28 SECTORAL INITIATIVES

6 THRUSTS

1	2	3	4	5	6
Drive digital transformation in the public sector	Boost economic competitiveness through digitalisation	Build enabling digital infrastructure	Build agile and competent digital talent	Create an inclusive digital society	Build trusted, secure and ethical digital environment

6
Build trusted, secure and ethical digital environment

S1: Strengthening safety and ethics in digital activities and transactions

S2: Enhancing institutions commitment to personal data protection and privacy

S3: Improving cross-border data transfer

S4: Increasing cyber security uptake among businesses

SOURCE: https://27.group/what-is-mydigital-initiative-digital-nasional-berhad-about/

Personal Data Protection Act 2010 (PDPA)

LAWS OF MALAYSIA

ACT 709

PERSONAL DATA PROTECTION ACT 2010

Date of Royal Assent : 2 June 2010
Date of publication in the Gazette : 10 June 2010

- **Governs Personally Identifiable Information(PII) data collected via commercial transaction.**
- **Malaysia's PDPA is align with the EU's GDPR.**

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.

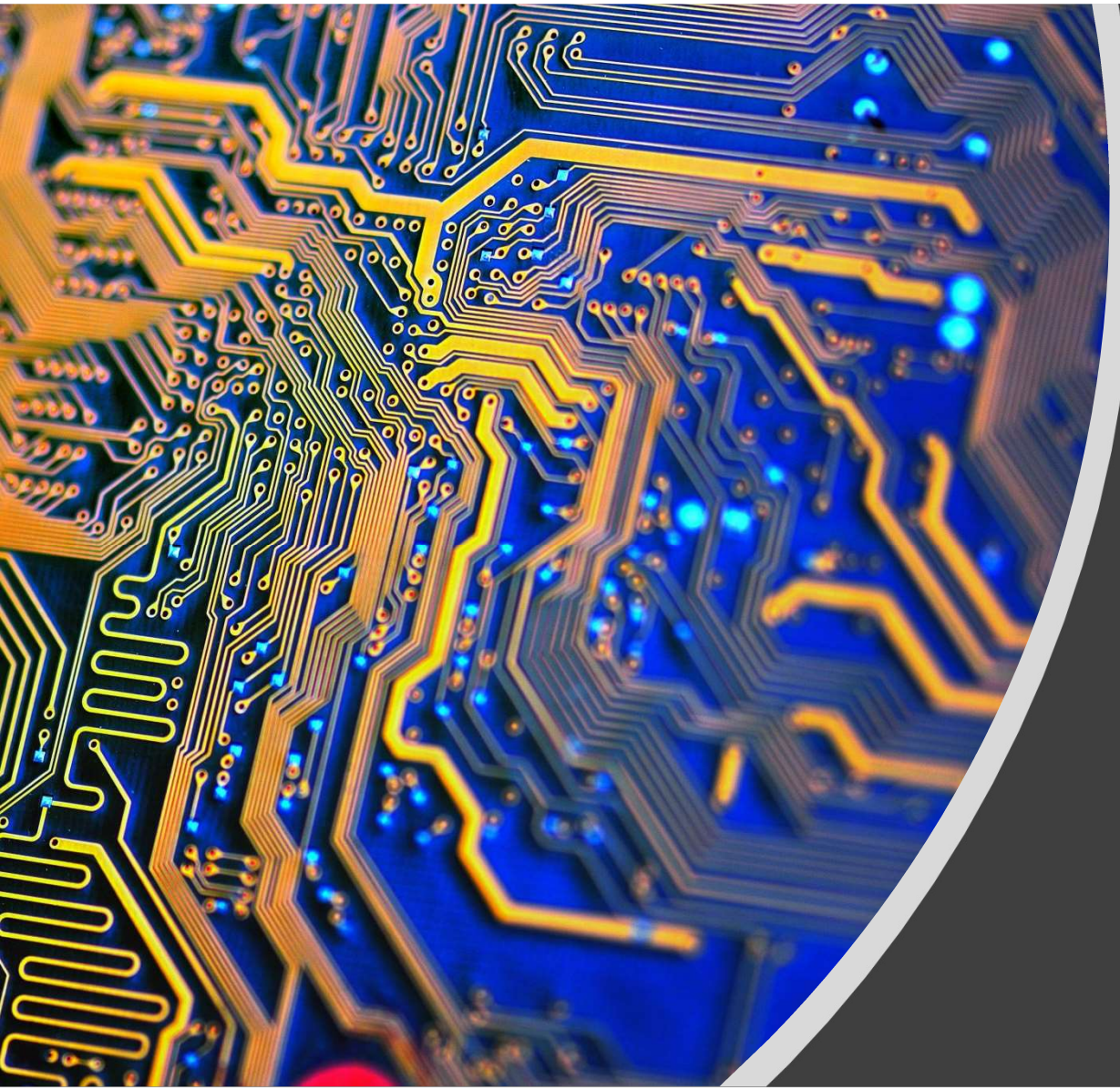
- Cryptography also supports the National Digital Economy and the realization of the National Transformation Agenda to transform Malaysia into becoming an advanced and high-income nation

ADDRESSING CYBERSECURITY 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



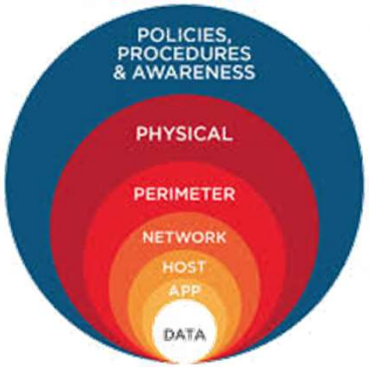
TECHNOLOGY

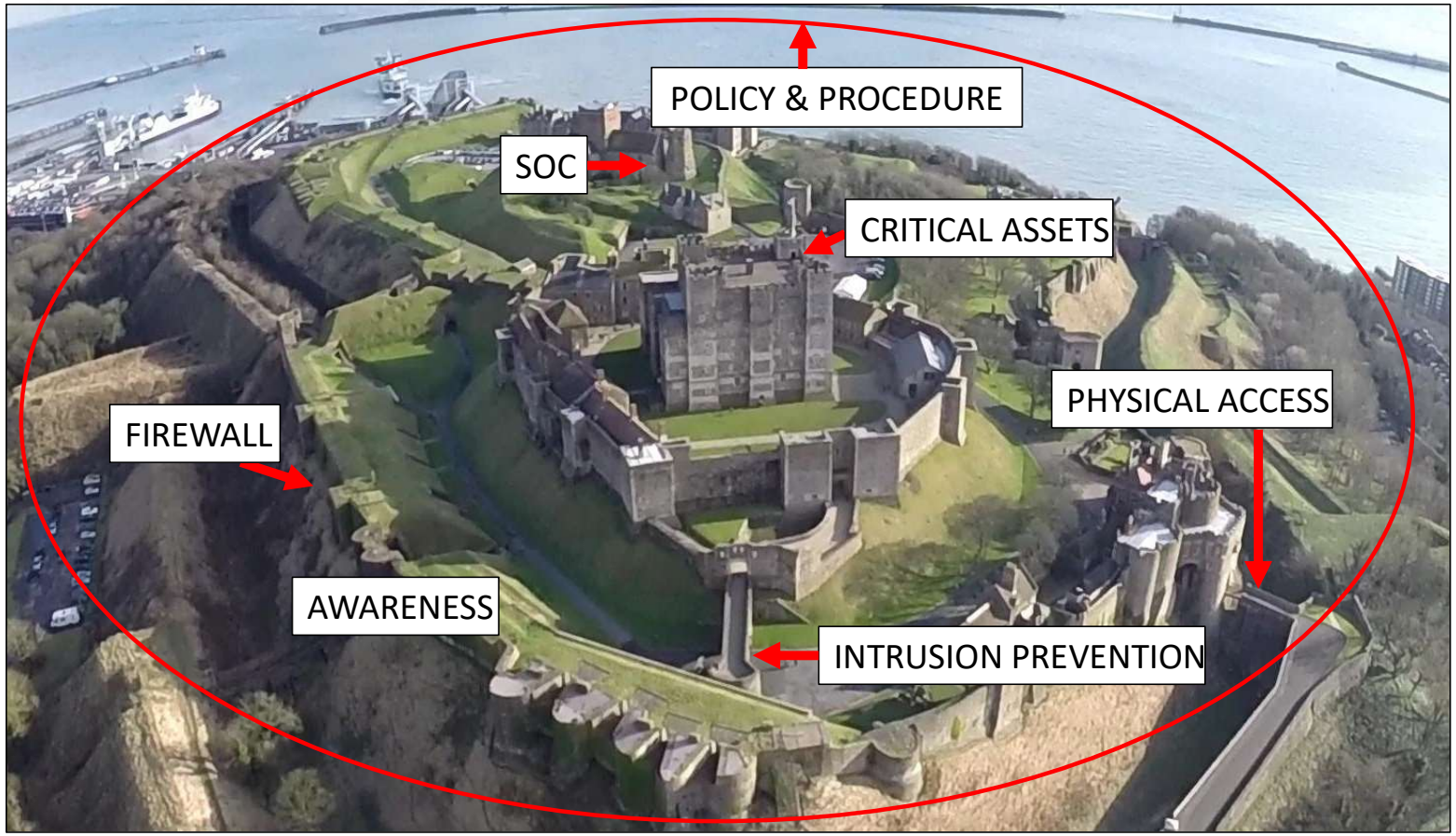
TRADITIONAL CYBERSECURITY APPROACH
- Not sufficient to deal with smart cyber threats

CyberSecurity MALAYSIA

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



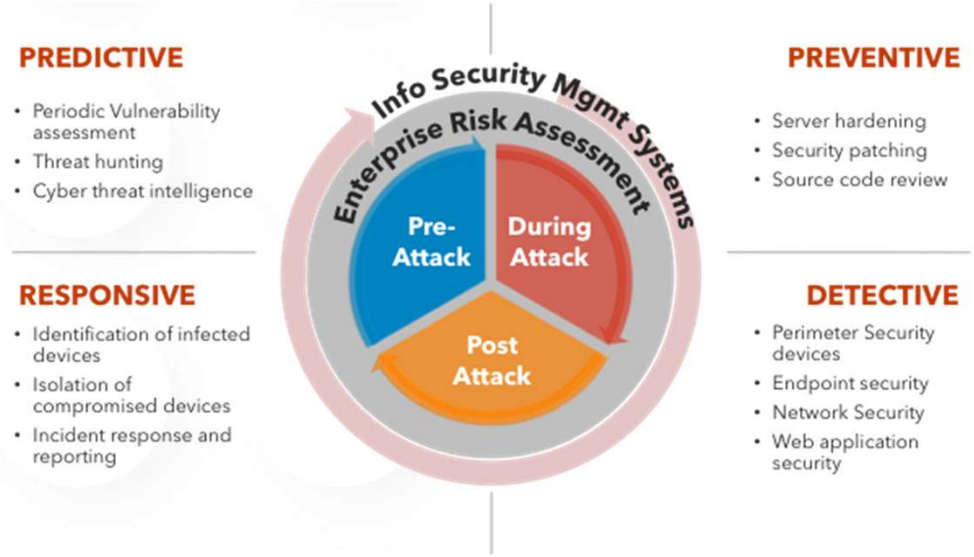


This is an approach that relies on using a layered and redundant defensive mechanism to protect data and assets from cyber-attacks.

ADDRESSING CYBER SECURITY 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



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) 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 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

CyberSecurity MALAYSIA

DIGITAL FORENSIC (DF)

CyberCSI crime scene investigation

CyberDEF Uncovering Future Threats

Cyber Detect, Eradicate and Forensics (CyberDEF)

Evidence Preservation Facility

CyberDiscovery

Digital Forensic 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)

Cyber Early Warning

LebahNET.MY CyberSecurity Honeynet Project

Lebahnet (Honeynet Project)

Technical Coordination Centre

Cyber Threat Research Centre (CTRC)

Computer Security Incident Response Team (CSIRT) Consultancy

CyberSecurity Malaysia malware research centre

Malware Research Center

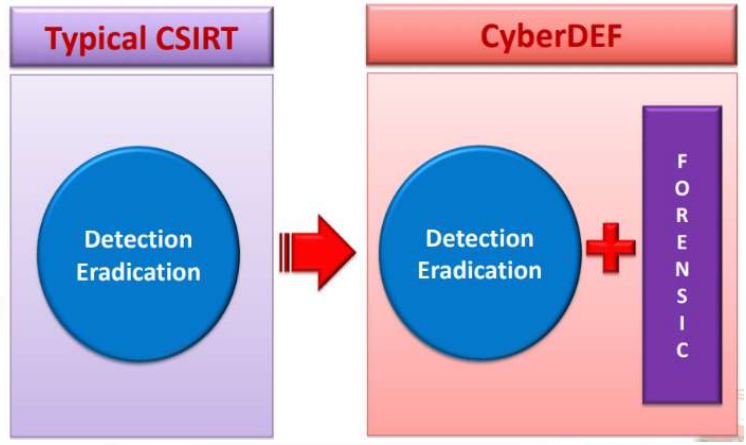
Cyber999

Cyber999 Help Centre

ADDRESSING CYBERSECURITY THROUGH STRENGTHENING DETECTION TECHNOLOGY

CyberD.E.F

- Detection
- Eradication
- Forensic



Detection	Eradication	Forensics
Identify any loopholes, vulnerabilities and existing threats 1. Sensors 2. Sandbox 3. Analytics 4. Visualization	Close loopholes, patch vulnerabilities and neutralize existing threats Perform cyber threats exercise or drill to test the feasibility and resiliency of the new defense / prevention system	1. E-Discovery 2. Root cause analysis 3. Investigation 4. Forensics readiness 5. Forensic compliance

STRENGTHENING CYBERSECURITY PREVENTION THROUGH TECHNOLOGY VULNERABILITY ASSESSMENT

Secure Software Development Lifecycle (SSDLC) Lab & Services

Internet of Things (IOT) Lab

Robotic Lab (4th Industry Revolution)

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.

- Organizations should gear themselves towards cyber resilience as the threat of global cybersecurity breaches continues to pose major risks.

MINISTRY OF
COMMMUNICATIONS AND 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 +61 300 88 2999

www.cybersecurity.my | info@cybersecurity.my

CyberSecurityMalaysia cybersecuritymy cybersecuritymy CyberSecurity Malaysia cybersecurity_my

JUBLI PERAK 1997 - 2022 CyberSecurity MALAYSIA

SIBER MALAYSIA MADANI

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013 CERT. NO. : ISMS 00114

ACB ISMS 02 SAMM 456

MSC MALAYSIA Status Company

Best Child Online Protection Website

WSIS PRIZES 2020 WINNER www.wsis.org

THE MALAYSIA BOOK of RECORDS