ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (19-28), Month: January - March 2021, Available at: www.researchpublish.com

Cybersecurity Strategies and Challenges in Malaysia

Mohamed Asadullah [1], Prof. Dr. Mohd. Adam Bin Suhaimi[2]

[1,2]Kulliyah of Information and Communication Technology, International Islamic University Malaysia Gombak, Malaysia

Abstract: **This paper aims to contribute to the body of knowledge on cybersecurity challenges especially on the new normal of Covid-19 to overcome threats and mitigation controls taken by the Malaysian government. This is important to Malaysia's cyberspace as secured, trusted, and resilient, fostering economic prosperity and citizens' well-being. This is achieved by fortifying capabilities to predict, detect, deter, and respond to threats via structured governance, competent people, support best practices processes, and deploy effective technology. The common challenges and predictions that the Malaysian government faces in past events, threats driven by Covid-19, economic recovery plan, and adjusting to the new normal. This paper will also elaborate on how the Malaysian government implements Malaysia Cybersecurity Strategy 2020-2024 for the economic wellbeing and security of the nation, also the view of Malaysian Public Sector ICT Strategic Plan 2016-2020 in cybersecurity.**

Keywords: **Cybersecurity Strategies, Cybersecurity Challenges, Cybersecurity Malaysia.**

I. INTRODUCTION

Malaysia's aspirations to become a developed country based on the four main pillars in the master framework of the transformation agenda which is (1-Malaysia) People First Achievement Prioritized, Government Transformation Program (GTP), Program Economic Transformation (ETP), and the New Economic Model. Malaysia as a developing country in global adapts information technology as a core value in employment, business industries, and government sectors. The focus area of Information Communication Technology (ICT) strategic thrust based on people-friendly and inclusive which is designed to focus on the Government's digital services that able to meet the increasingly sophisticated expectations of the people. Malaysia has become a long way since the first adoption of the Internet back in 1995. Today, broadband connectivity has become a necessity for businesses, services, and citizens of Malaysia to succeed and be relevant in the Fourth Industrial Revolution (Industry 4.0) [1]. Hardly everyone connected to cyberspace and becoming deeply reliant on democratized technologies such as mobile, computer, social, big data, internet of things (IoT), artificial intelligence, and cloud connectivity. Anything connected to the internet may be exposed to cyber risks. Cyber threats may be brought harmful impact not only on individual or private sectors but also on government agencies and cause reputational issues, interruption of services, damages, economic loss, and in the worst case, the security of a nation. So, Malaysia's cybersecurity strategy is pragmatic for cyberspace that is secured, trusted, and resilient while at the same time fostering economic prosperity and the well-being of its citizens.

II. DISCUSSIONS AND IMPLICATIONS

As published by Statista Research Department, the Malaysian number of internet users from 2018-2020 is increasing 27.56, 29.01, and 30.44 in millions accordingly [2]. On other hand, cyber threats have increased vigorously even faster than the security measures are put in place. Governments now deal with cyber threats not only at personal and financial gains but also from state-sponsored actors aimed at critical targets of national importance. It is worth noting that state-sponsored attacks are not only sophisticated and potent but once deployed, these advanced technologies can fall into the hands of cybercriminals who can then amplify the use of these powerful cyberweapons on a global scale [1]. Since cyber threats are often the very foundation of a nation, Malaysia recognizes cybersecurity as a national priority and leads to the formulation of cybersecurity controls.

Cyber organization and Standardization

The formulation of the National Cyber Security Policy (NCSP) was developed in the year 2006. The main function of NCSP was specifically to address the risks to the Critical National Information Infrastructure (CNII). CNII is made up of 10 sectors namely, National Defence and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; and Food and Agriculture. The NCSP recognizes the critical and highly interdependent nature of the CNII that will ensure the effectiveness of cybersecurity controls over vital assets. Later, the establishment of the National Cyber Security Agency (NACSA) was in 2017. NACSA further reaffirmed the growing importance of cyber issues to Malaysia's national security. NACSA is a dedicated agency that oversees all national cybersecurity functions which are formed under the aegis of the National Security Council (NSC). To adapt to the ever-changing landscape of cyberspace, existing laws should be enhanced and addresses the legal challenges in facing cyber threats or taking action against cybercriminals. The Attorney General's Chambers (AGC) led the review of the laws of Malaysia intending to enhance the existing legislative and regulatory framework used to combat cybercrime. AGC also collaborates with law enforcement agencies and other relevant government bodies. Furthermore, a national policy and procedure have been formulated in managing cyber crises. This is to ensure that cyber-attacks and cyber incidents are being managed proactively through a coordinated approach at the national level. This initiative is closely guided by the National Security Council's Directive No 24: Policy and Mechanism of the National Cyber Crisis Management that outlines the nation's strategy for 'cyber crisis mitigation and response' through public and private collaboration and coordination. There are six (6) main principles under this directive namely national cyber crisis management structure; national cyber-threat levels; Computer Emergency Response Team (CERT); cybersecurity protection mechanisms; response, communication and coordination procedures; and a readiness program [3].

Cyber Crisis Centre

The government has formed a crisis centre such as National Cyber Coordination and Command Centre (NC4) where the centre is previewed under the NACSA as a central coordination and deal with a crisis at the national level. The centre is mainly connected with the entire cybersecurity-operating called Malaysian Communications and Multimedia Commission (MCMC). This ensures the ability to the national cybersecurity threat level and accesses the impact on the country.

Cyber Crisis Exercise

The government has conducted a national cyber crisis exercise for the past decade which is known as X-Maya. The main objective is to ensure the effectiveness of the procedures that have been developed under the National Cyber Crisis Management Plan (NCCMP) and to assess the preparedness of critical national infrastructure agencies against cyber-attacks. To date, there were six (6) national cyber crisis exercise has been conducted.

Cyber Alert Programs

Malaysia has also been actively creating a cybersecurity awareness program. As to coordinate these programs, NASCA is developing the National Cyber Security Awareness Master Plan where the main aim is to increase the level of awareness among the Malaysian by four (4) main target groups such as kids, youth, adults/parents, and organizations.

Produce Skilled Cyber Security Professionals and Institutions

Education of cybersecurity starts from the development of school curricular; followed by the focus-based skills at the institutions of higher learning; training and skills development schemes for experts and non-experts in both public and private sectors. The government will also further enhance the current initiatives especially the Centre of Excellence, a collaboration with the local universities with international institutes to address the shortage of local talent in the cybersecurity workforce.

Malaysia Cyber Security Strategy 2020 - 2024

Malaysia cybersecurity strategy outlines five (5) strategic pillars, together with twelve (12) strategies that will govern all aspects of cybersecurity planning and implementation up to the year 2024 as follows: -

Pillar 1: Effective Governance and Management

Strategy 1: Enhancing National Cyber Security Governance and Ecosystem

Strategy 2: Improving Organization Management and Business Operation (Government, CNII and Business)

Strategy 3: Strengthening Cyber Security Incident Management and Active Cyber Defence

Pillar 2: Strengthening Legislative Framework and Enforcement

Strategy 4: Enhancing Malaysia's Cyber Laws to Address Current and Emerging Threats

Strategy 5: Enhancing the Capacity and Capability of Cybercrime Enforcement

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

Strategy 6: Spurring National Cyber Security R&D Programme

Strategy 7: Promoting a Competitive Local Industry and Technology

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

Strategy 8: Enhancing National Cyber Security Capacity and Capability Building

Strategy 9: Enhancing Cyber Security Awareness

Strategy 10: Nourishing Cyber Security Knowledge Through Education

Pillar 5: Strengthening Global Collaboration

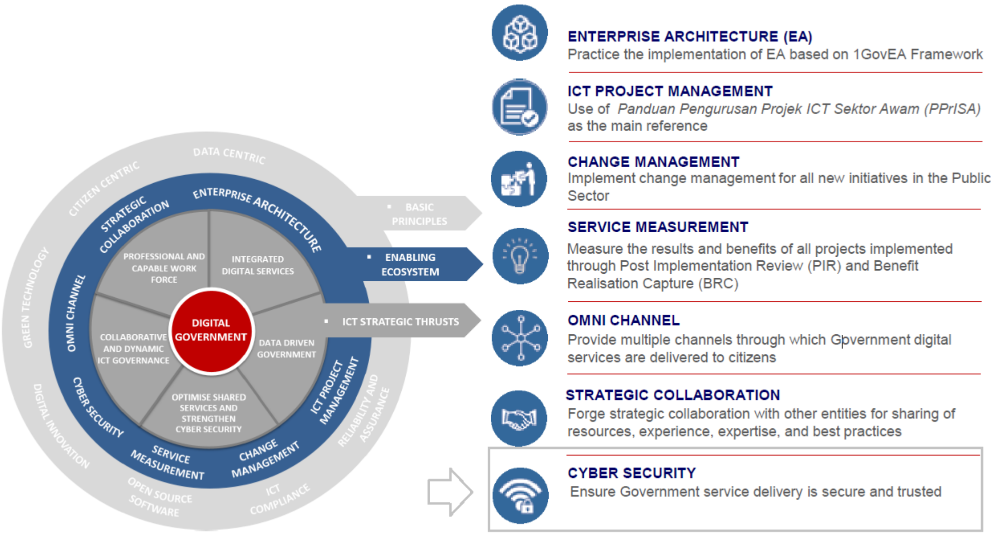
Strategy 11: Strengthening International Collaboration and Cooperation in Cyber Security Affairs

Strategy 12: Demonstrating Malaysia's Commitment to Promoting Secure, Stable and Peaceful Cyberspace to Uphold International Security

[Source: Malaysia Cyber Security Strategy 2020 - 2024]

Malaysian Public Sector ICT Strategic Plan 2016-2020

On the other hand, Malaysia adopts its Public Sector ICT Strategic Plan (PSISP) in Cybersecurity. It outlines the strategic direction of ICT implementation in the Malaysian Public Sector for the next 5 years [4]. The ICT framework consists of four (4) main components such as ICT vision, ICT Strategic Thrusts, Enabling Ecosystem, and Basic Principles [4]. A conducive ecosystem is required to support and enable the successful implementation of the ICT Strategic Thrusts [4]. One of the key elements in the Ecosystem is Cyber Security. The element ensures government service delivery is secure and trusted.



ENTERPRISE ARCHITECTURE (EA)
Practice the implementation of EA based on 1GovEA Framework

ICT PROJECT MANAGEMENT
Use of *Panduan Pengurusan Projek ICT Sektor Awam (PPrISA)* as the main reference

CHANGE MANAGEMENT
Implement change management for all new initiatives in the Public Sector

SERVICE MEASUREMENT
Measure the results and benefits of all projects implemented through Post Implementation Review (PIR) and Benefit Realisation Capture (BRC)

OMNI CHANNEL
Provide multiple channels through which Gpvernment digital services are delivered to citizens

STRATEGIC COLLABORATION
Forge strategic collaboration with other entities for sharing of resources, experience, expertise, and best practices

CYBER SECURITY
Ensure Government service delivery is secure and trusted

Fig 1: Enabling Ecosystem [4]

The third (3rd) strategic thrust of Malaysian Public Sector ICT Strategic Plan 2016-2020 is 'Optimize Shared Services and Strengthen Cyber Security', the objective is to increase sharing of ICT resources through a centralized and structured initiative, and to ensure secure and trusted digital services [4]. The strategies (S) and programs (P) are as follows: -

S1 Strengthen Public Sector ICT Infrastructure

P1 Strengthen Public Sector Data Center (PDSA)

P2 Enhance Government Cloud services

S2 Strengthen Digital Communication Capability

P1 Upgrade and expand 1Gov*Net network services

P2 Coordinate and strengthen Public Sector agencies networks

P3 Strengthen and expand Government consolidated communication services

S3 Strengthen Public Sector Cyber Security

P1 Enhance cybersecurity services

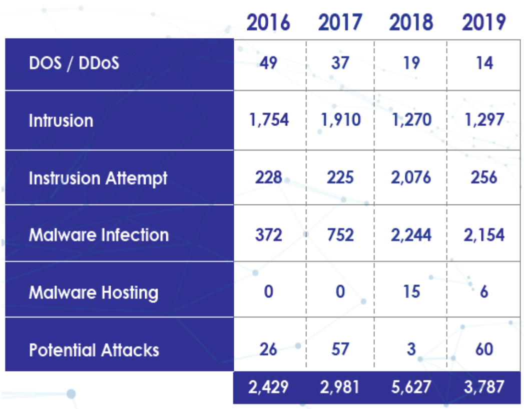
P2 Compliance to Public Sector security guidelines

P3 Strengthen cybersecurity environment

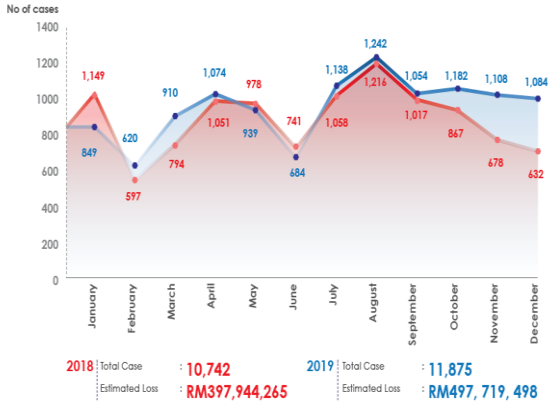
[Source: MaMPU, The Malaysian Public Sector ICT Strategic Plan 2016 - 2020]

III. ISSUES AND CHALLENGES

The risk of cyber threats is always persistent and there will chances of cyberattacks at any time. Such threats could not be eradicated as long as the precautions and security measures are not in place. It is everyone's responsibility to enhance Malaysia's overall cyber readiness, capacity, and capabilities. In Asia, it is estimated that there are over 5 million IP addresses connected to millions of infected devices observed in the region, including India and China, and among the top 25 infected countries globally, eight of them are from Asia such as India, China, Indonesia, Thailand, Vietnam, the Philippines, Malaysia and Sri Lanka [5]. The comparative study of cyber threats in Malaysia in the year 2018 to 2019 has estimated losses RM397,944,265 and RM497,719,498 subsequently.



	2016	2017	2018	2019
DOS / DDoS	49	37	19	14
Intrusion	1,754	1,910	1,270	1,297
Instrusion Attempt	228	225	2,076	256
Malware Infection	372	752	2,244	2,154
Malware Hosting	0	0	15	6
Potential Attacks	26	57	3	60
	2,429	2,981	5,627	3,787



Tab 1: Cyber Security Incidents in Malaysia 2016 - 19 [1] **Fig 2: Cybercrime Statistics of Malaysia 2018 - 19 [1]**

Challenges Confronting an Enterprise

The new pandemic has changed the business environments. According to management consultancy of Mckinsey & Company, Automotive industries already facing down and it creates the opportunity to include the huge shift to online shopping by adopting to software subscriptions; Food industries operations changed to new long-term economic model in optimizing takeaway and drive-through operations and mid-range restaurants have to adapt the new normal of online food menu systems; Banking industries require software in automated underwriting and calculating the creditworthiness of a small business rather staff making decisions where raised their margin by 5% to 10%; Insurance industries faces the key strategy for traditional insures that requires both responsibility to customers during Covid-19 crisis and the first to launch products focused to pandemic; Healthcare industries has hugely accelerated growth of margins and digital healthcare that requires multilevel technology systems; and Education faces the lower income of students by 55% and with remote learning they have reconfigure the physical and virtual space by reducing or terminating the number of lecture halls and turn into flexible remote working hubs [6].

Threats Driven by Covid-19

There are certain levels of threats identified during the Movement Control Order (MCO) in Malaysia. The threats are using Covid-19 as a theme uncovered during the MCO period can be classified as follows: -

- COVID 19 Phishing emails/websites
- COVID 19 Scam Domains
- COVID 19 based malware
- COVID 19 Android Malware
- COVID 19 Vulnerable Sectors and Infrastructures (Health Sector)

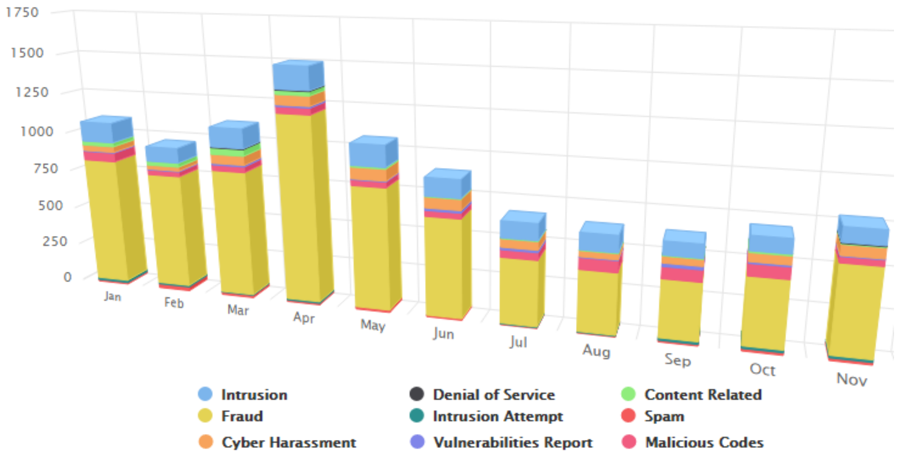
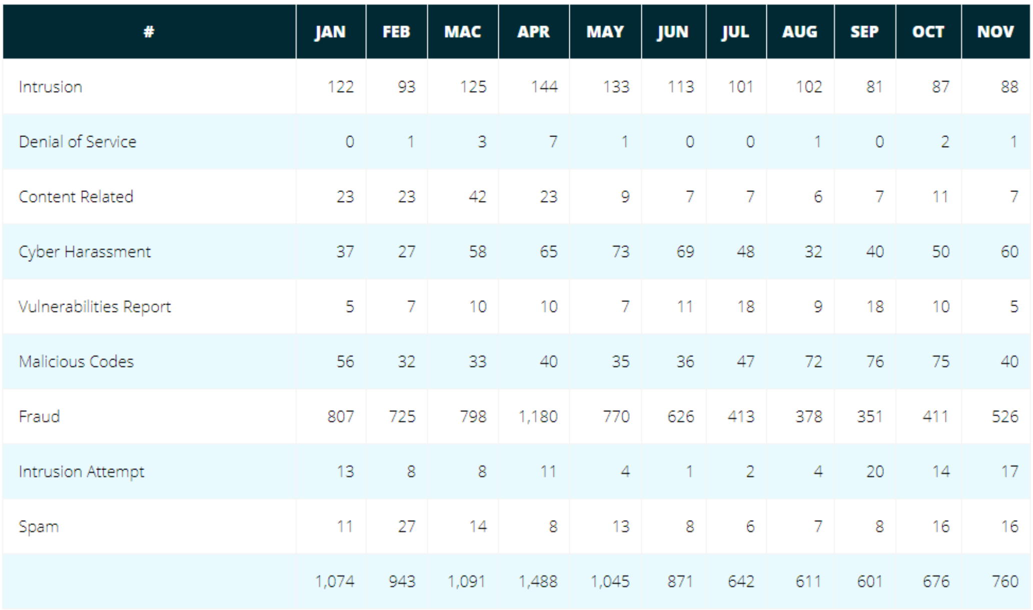


Fig 3: Reported Incidents based on General Incident Classification Statistics 2020 in Malaysia [7]

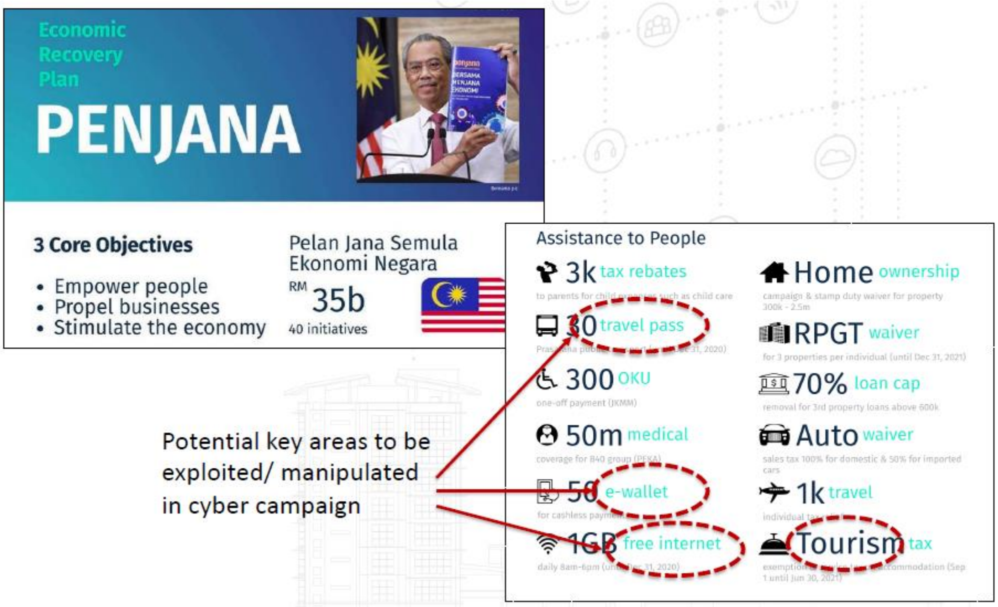


#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV
Intrusion	122	93	125	144	133	113	101	102	81	87	88
Denial of Service	0	1	3	7	1	0	0	1	0	2	1
Content Related	23	23	42	23	9	7	7	6	7	11	7
Cyber Harassment	37	27	58	65	73	69	48	32	40	50	60
Vulnerabilities Report	5	7	10	10	7	11	18	9	18	10	5
Malicious Codes	56	32	33	40	35	36	47	72	76	75	40
Fraud	807	725	798	1,180	770	626	413	378	351	411	526
Intrusion Attempt	13	8	8	11	4	1	2	4	20	14	17
Spam	11	27	14	8	13	8	6	7	8	16	16
	1,074	943	1,091	1,488	1,045	871	642	611	601	676	760

Tab 2: Reported Incidents based on General Incident Classification Statistics 2020 in Malaysia [7]

Economic Recovery Plan

Covid-19 affect the overall production of the country. Moreover, the Movement Control Order (MCO) and the complete lockdown during the pandemic have caused a serious impact on the country's economy. The government had taken an initiative to provide financial aid and support, implementing schemes and new guidelines such as Coronavirus SME guarantee scheme, announcing moratorium period for selected loans, implementing the reduction of tax especially for tourism and hotel management which affected, free health services, providing free internet services, usage of MySejahtera application, e-wallet and so on. Nevertheless, ICT nor cybersecurity could not be separated and have taken full control of every sector in whatever initiative that the government had taken.



Economic Recovery Plan

PENJANA

3 Core Objectives

- Empower people
- Propel businesses
- Stimulate the economy

Pelan Jana Semula Ekonomi Negara

RM 35b

40 initiatives

Assistance to People

3k tax rebates
to parents for child ... such as child care

30 travel pass
Pras...ana public ... Dec 31, 2020)

300 OKU
one-off payment (JKMM)

50m medical
coverage for 840 group (PEKA)

50 e-wallet
for cashless paym...

1GB free internet
daily 8am-6pm (un... Dec 31, 2020)

Home ownership
campaign & stamp duty waiver for property 300k - 2.5m

RPGT waiver
for 3 properties per individual (until Dec 31, 2021)

70% loan cap
removal for 3rd property loans above 600k

Auto waiver
sales tax 100% for domestic & 50% for imported cars

1k travel
individual ta...

Tourism tax
exemption ... accommodation (Sep 1 until Jun 30, 2021)

Potential key areas to be exploited/ manipulated in cyber campaign

Fig 4: Economic Recovery Plan [8]

Adjusting to The New Normal

Pandemic has been caused industries even government agencies have to remotely connect to the network to continue their service to the public. Access to a trusted Virtual Private Network (VPN) with multi-level authentication is essential to access all the core systems. Again, to enhance the cybersecurity by adopting to the Malaysian Public Sector ICT Strategic

Plan's key strategies of S1 Strengthen Public Sector ICT Infrastructure, S2 Strengthen Digital Communication Capability, and S3 Strengthen Public Sector Cyber Security. Data Center should be strengthened and enhancement of government cloud services. Since the increase in remote users, the government has upgraded and expanded its network services. The overall cybersecurity environments are strengthened by implementing adequate processes and procedures.

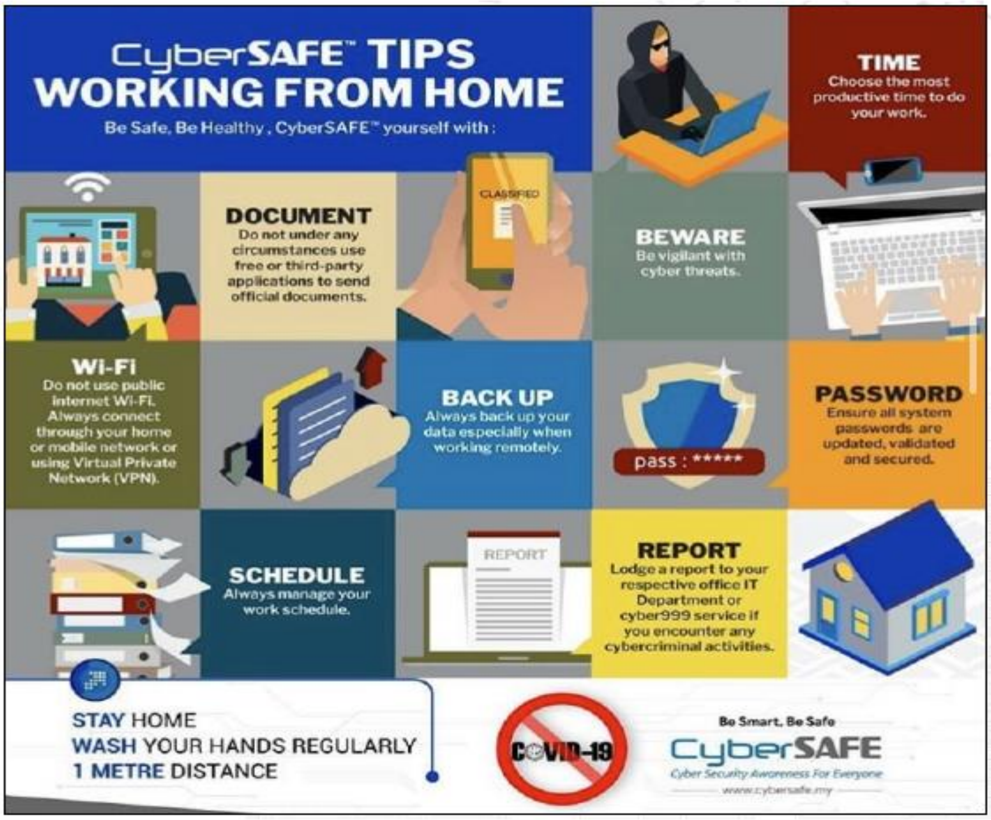

CyberSAFE™ TIPS
WORKING FROM HOME
Be Safe, Be Healthy, CyberSAFE™ yourself with:
TIME
Choose the most productive time to do your work.
CLASSIFIED
DOCUMENT
Do not under any circumstances use free or third-party applications to send official documents.
BEWARE
Be vigilant with cyber threats.
WI-FI
Do not use public internet Wi-Fi. Always connect through your home or mobile network or using Virtual Private Network (VPN).
BACK UP
Always back up your data especially when working remotely.
pass : *****
PASSWORD
Ensure all system passwords are updated, validated and secured.
SCHEDULE
Always manage your work schedule.
REPORT
REPORT
Lodge a report to your respective office IT Department or cyber999 service if you encounter any cybercriminal activities.
STAY HOME
WASH YOUR HANDS REGULARLY
1 METRE DISTANCE
COVID-19
Be Smart, Be Safe
CyberSAFE
Cyber Security Awareness For Everyone
www.cybersafe.my

Fig 5: CyberSafe Tips [8]

IV. CYBERSECURITY IMPLEMENTATIONS

Professional Certification

The Malaysian government has implemented the initiative to public and private sectors by ensuring the adoption of security-related certifications, standards, and certification of the CNII agencies to the MS ISO/IEC 27001: Information Security Management Systems standard. This will ensure the CNII agencies and organizations have the necessary protection and compliance are in place. Appropriate measures are also prepared to protect sectors such as manufacturing, construction, education, and retail since cyber threats and attacks in these sectors also pose risks to the overall economic wellbeing and security of the nation. Malaysia has also started its efforts to increase the number of local cybersecurity professionals through the Global Accredited Cybersecurity Education (ACE) scheme.

Computer Emergency Response Team (MyCERT)

National Computer Emergency Response Team (MyCERT) consists of specialists and analysts in the areas of incident handling and malware research. MyCERT operates the Cyber999 help center. It provides an emergency response to cybersecurity incidents at a national level. The one-stop-center meets all the security needs for not only government sectors and private companies but also home users. It provides services such as alerts and advisories, incident report, cyber threat research center, and incident statistics.

Alerts and advisories produced by MyCERT during MCO as follows: -

- MA-779.032020: MyCERT Advisory - COVID-19 Cyber Scams and Campaigns
- MA-780.032020: MyCERT Advisory - Work-From-Home: Security Advice & Best Practices

- MA-781.032020: MyCERT Alert - Vulnerability in Adobe Type Manager Library
- MA-782.042020: MyCERT Advisory - Online Video Tele-conferencing (VTC) Application Security Guidelines
- MA-783.042020: MyCERT Alert - Vulnerabilities in Mozilla Firefox & Firefox ESR
- MA-785.042020: MyCERT Alert - Bogus Scam Email
- MA-786.042020: MyCERT Advisory - Microsoft Releases April 2020 Security Updates
- MA-788.062020: MyCERT Alert - Malicious Android APK theme Covid-19 targeting Malaysia users
- MA-789.062020: MyCERT Advisory - StayAtHome malicious APK campaign
- MA-790.072020: MyCERT Alert - SMSSpy using Malaysian Law Enforcement as a theme

[Source: MyCERT (Malaysia Computer Emergency Response Team)]

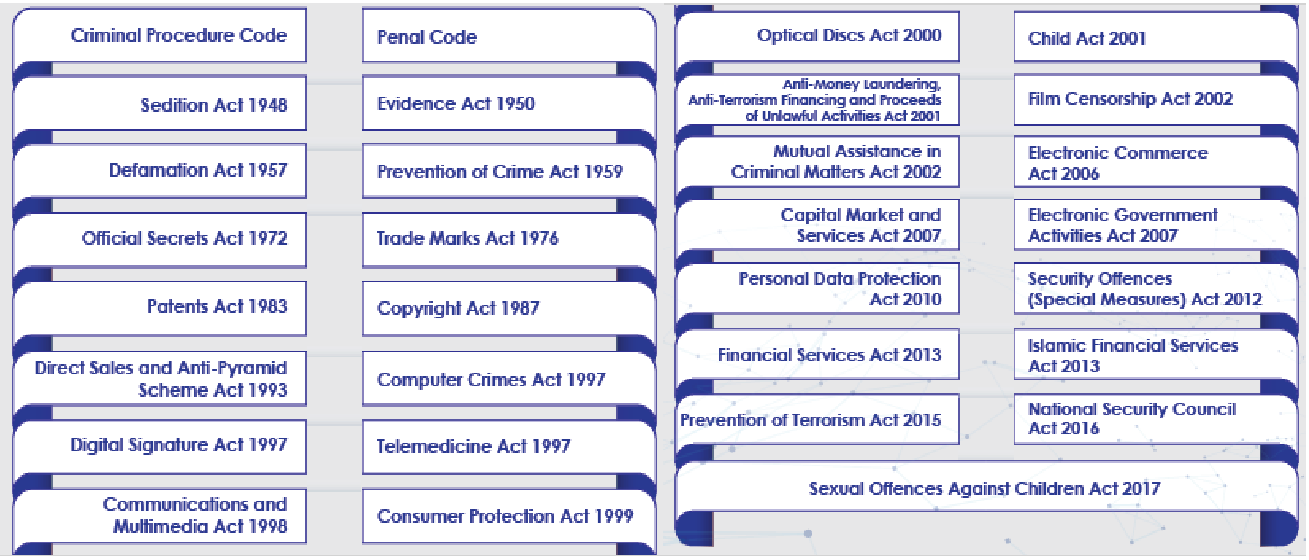
Implementing Cyber Incident Response Plan (CIRP), Policies and Procedures

As cyber-attacks become more sophisticated, an organization should evaluate and enhance its security defenses towards real-time incidents. Multi-layered security solutions should be implemented in the organization. Implementation of security awareness and risk management exercises should be conducted [8]. Collaboration with local & International organizations to address cyber threat issues [8]. Risk management of an organization is required to develop CIRP, together adapt the Operational Risk Integrated Online Network (ORION), a risk surveillance system for financial institutions by Bank Negara Malaysia (BNM). A policy document for ORION was issued by BNM on 22 June 2018 which requires all financial institutions to adhere to its standards. It classifies Risk Exposures (RE) through indicators such as Loss Event Data, Key Risk Indicators, and Scenario Analysis [9]. The main objective of this policy document is to require REs to submit information to the Bank concerning operational risk exposure [9]. A new policy from BNM on Risk Management in Technology (RMiT) also came into effect in 2020 and applies to all financial institutions in Malaysia. This policy document will help organizations to comply with RMiT security obligations [10]. The standards of cyber risk management in RMiT which all financial institutions must comply in Malaysia.

[Source: BNM, RMiT)

Malaysia Cyber Laws

Malaysia has its comprehensive cyber-related laws in South East Asia. Since the 1990s, Malaysia has introduced numerous laws to cater to cybersecurity issues.



Criminal Procedure Code
Sedition Act 1948
Defamation Act 1957
Official Secrets Act 1972
Patents Act 1983
Direct Sales and Anti-Pyramid Scheme Act 1993
Digital Signature Act 1997
Communications and Multimedia Act 1998

Penal Code
Evidence Act 1950
Prevention of Crime Act 1959
Trade Marks Act 1976
Copyright Act 1987
Computer Crimes Act 1997
Telemedicine Act 1997
Consumer Protection Act 1999

Optical Discs Act 2000
Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001
Mutual Assistance in Criminal Matters Act 2002
Capital Market and Services Act 2007
Personal Data Protection Act 2010
Financial Services Act 2013
Prevention of Terrorism Act 2015

Child Act 2001
Film Censorship Act 2002
Electronic Commerce Act 2006
Electronic Government Activities Act 2007
Security Offences (Special Measures) Act 2012
Islamic Financial Services Act 2013
National Security Council Act 2016

Sexual Offences Against Children Act 2017

Fig 5: Existing Laws for Cybercrime in Malaysia [1]

Cyber Security Campaigns and Training

Realizing cybersecurity is a backbone and attitude towards technology, government inculcates the importance of adhering to cyber hygiene practices among government sectors, businesses, and the public. Currently, there are cybersecurity awareness initiatives undertaken by relevant agencies, organizations throughout various approaches to specified target groups.

- NACSA has published the 10 Easy Steps for Cyber Security Awareness that outlines all of the most sensible practices in cyberspace;

- Malaysian Modernization and Management Planning Unit (MAMPU) has been organizing cybersecurity awareness programs for the public sector such as the Cyber Security Awareness Month and Public Sector ICT Security Conference;

- Royal Malaysia Police through the Be Smart campaign ensures the community are more aware and cautious about cybercrime;

- Malaysian Communications and Multimedia Commission has organized various programs under the Klik Dengan Bijak initiative, a media and digital literacy initiative to nurture positive and responsible Internet use among ICT users based on the Rukun Negara together with its strategic partners including the Ministry of Communications and Multimedia Malaysia, Ministry of Health (MOH), Ministry of Education (MOE), Ministry of Women, Family and Community Development (MWFCD), Royal Malaysia Police, Communications and Multimedia Forum of Malaysia (CMCF) as well as civil society partners such as United Nations Children's Fund (UNICEF), Scouts Association of Malaysia, Malaysian Youth Council and others;

- Ministry of Health also has come out with Semak Sebelum Klik campaign;

- Chief Government Security Office (CGSO) through the Protective Security Training Centre provides ICT security awareness courses to government officials as part of its annual cybersecurity awareness program;

- Cybersecurity Malaysia in collaboration with MOE and DiGi Telecommunications Sdn. Bhd. runs the CyberSAFE campaign to nurture positive and responsible Internet use among ICT users; and

- Central Bank of Malaysia has been raising awareness to all banking users on online fraud and safety tips for Internet banking services.

[Source: Malaysia Cyber Security Strategy 2020 - 2024)

V. CONCLUSION

In conjunction to create citizen-centric digital services and applications, cybersecurity plays an important role. Therefore, Malaysia has committed to providing cyberspace that is secured, trusted, and resilient, and at the same time, it also encourages economic prosperity and supports social well-being. The government is confident that this can be accomplished by strengthening the capabilities to predict, detect, deter, and respond to cyber threats.

REFERENCES

[1] Malaysia Cyber Security Strategy 2020 - 2024

[2] Statista Research Department, 2020, Number of internet users in Malaysia, https://www.statista.com/statistics/553752/number-of-internet-users-in-malaysia/

[3] National Cyber Security Agency (NACSA), Malaysia, 2020, National Security Council's Directive No.24, https://www.nacsa.gov.my/directive24.php

[4] Malaysian Administrative Modernization and Management Planning Unit (MaMPU), The Malaysian Public Sector ICT Strategic Plan 2016-2020

[5] Microsoft, 2020, Cyber Crime Centre, Meet Microsoft's Cybercrime fighters in Asia, https://news.microsoft.com/apac/features/meet-microsofts-cybercrime-fighters-in-asia-2/

[6] McKinsey & Company, 1996-2020, https://www.mckinsey.com/

[7] Cyber Security Malaysia 2020, MyCERT (Malaysia Computer Emergency Response Team), https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=1baddc7b-feae-4029-93d5-753139fc3730

[8] Cybersecurity Malaysia, 2020, https://www.cybersecurity.my/en/index.html

[9] Bank Negara Malaysia (BNM), Issued on 22 June 2018, A Policy document: Operational Risk Integrated Online Network (ORION)

[10] Bank Negara Malaysia (BNM), Circular No. BNM/RH/PD 028-98, Risk Management in Technology (RMiT), Issued on 19 June 2020, Appendix 5 Control Measures on Cybersecurity