

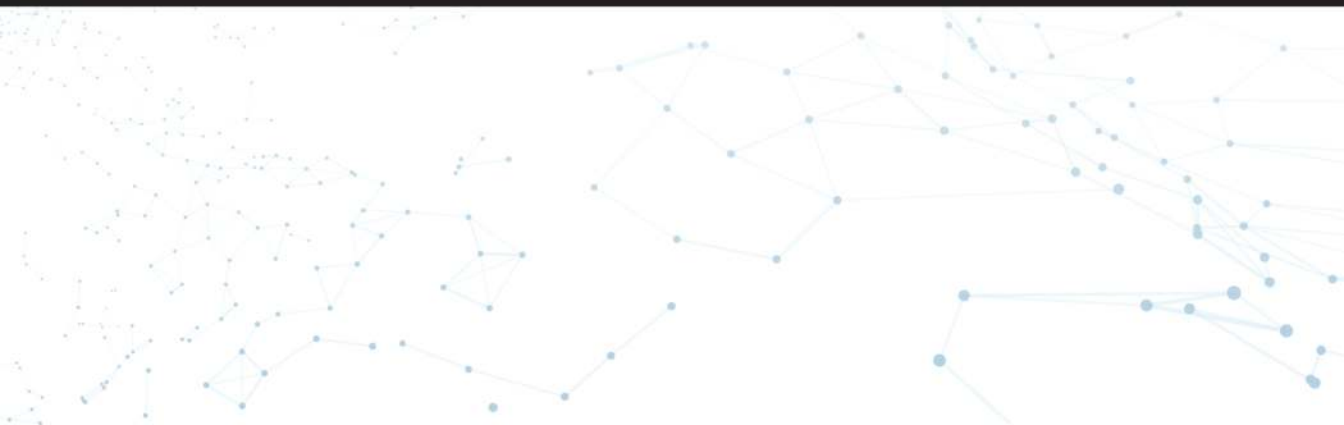


MALAYSIA
**CYBER SECURITY
STRATEGY**

20224

CONTENTS

INTRODUCTION	4
CYBER SECURITY LANDSCAPE & ECOSYSTEM	14
ISSUES & CHALLENGES	20
STRATEGIC PILLARS	28
<hr/>	
1 PILLAR 1 Effective Governance and Management	30
2 PILLAR 2 Strengthening Legislative Framework and Enforcement	44
3 PILLAR 3 Catalysing World Class Innovation, Technology, R&D and Industry	54
4 PILLAR 4 Enhancing Capacity & Capability Building, Awareness and Education	62
5 PILLAR 5 Strengthening Global Collaboration	74
<hr/>	
CONCLUSION	84
ABBREVIATIONS	88





MALAYSIA CYBER SECURITY STRATEGY 2020-2024

INTRODUCTION

INTRODUCTION



Malaysia has been rapidly ushered into the digital age, together with the rest of the world, for the past few decades due to the exponential and unprecedented advancement in the use of Information and Communications Technology (ICT). We have come 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). Hardly any person or thing is unconnected to cyberspace. Businesses are becoming deeply reliant on democratised technologies such as mobile, social, Big Data, Internet of Things (IoT), Artificial Intelligence (AI), and hyper-scale cloud that are all dependant on this connectivity.

Anything connected to the internet is exposed to cyber risks. With this in mind, Malaysia needs to develop a cyber security strategy that is pragmatic and aims for a cyberspace that is secured, trusted and resilient while at the same time fostering economic prosperity and the well-being of its citizens. We believe that our vision can be achieved by fortifying local capabilities to predict, detect, deter and respond to cyber threats by strengthening our cyber security governance, nurturing competent people, supporting best practice processes and deploying effective technologies.

Information sharing platforms, channels and avenues for government agencies, businesses and the general public on cyber security and cyber threats need to be enhanced. Our situational awareness, coordination, and threat mitigation capabilities likewise must be improved.

We are indeed fast becoming a digitalised nation. In 2018 there are 28.7 million Internet users in Malaysia which represent 87.4% of the population. Such astounding figures illustrates our growing dependency and connectedness to cyberspace. On the other side, cyber-attacks have progressed just as fast as, or even faster than the security measures that were put

in place. Governments now have to deal with cyber threats not just aimed at personal and financial gains, but also threats 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 cyber-criminals who can then amplify the use of these powerful cyber-weapons at global scale.

The targets of malicious cyber activity are often the very foundation of a nation. Consequently Malaysia recognises cyber security as a national priority. This has led to the formulation of the National Cyber Security Policy (NCSP) in 2006. The NCSP was specifically developed to address the risks to the Critical National Information Infrastructure (CNII), which are 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 recognises the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cyber

security controls over vital assets, as well as to ensure that the CNII sectors are protected to a level that commensurate with the risks faced.

The establishment of the National Cyber Security Agency (NACSA) further reaffirmed the growing importance of cyber issues to Malaysia's national security. NACSA is a dedicated agency that oversees all national cyber security functions formed under the aegis of the National Security Council (NSC). NACSA was established as a response to the dynamic nature, increasing sophistication, global nature and heighten socio-economic impact of cyber security threats. It serves as the lead agency that integrates the existing cyber security capabilities. This includes combating cybercrime in a strategic and coordinated manner in partnership with the private sector and other governments.

The efforts are ongoing to assess the current legislative framework for cybercrime issues and cases. In order to adapt to the ever-changing landscape of cyberspace, existing laws need to be enhanced to effectively address the legal challenges in taking action against cyber criminals. The Attorney General's Chambers (AGC) led the review

of the laws of Malaysia with a view to enhance the existing legislative and regulatory framework used to combat cybercrime. The amendments to certain laws are now in progress, where the AGC collaborates with law enforcement agencies and other relevant government bodies.

Furthermore, a national policy and procedure in managing cyber crises has been formulated 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, an executive directive 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); cyber security protection mechanisms; response, communication and coordination procedures; and a readiness programme.






The government has also established the National Cyber Coordination and Command Centre (NC4), a centre that deals with cyber threats and crises at the national level. The NC4 was developed under the purview of the NACSA as a central coordination and command facility responsible for managing cyber security at the national level, including mitigation, preparedness and response functions at a strategic and tactical level. It is connected to the entire main cyber security-operating centre (SOC) in Malaysia namely MCMC Network Security Centre, Government Integrated Telecommunications Network (GITN) SOC, Cyber Defence Operation Centre (CDOC) and Cybersecurity Malaysia SOC. It has the ability to determine the national cyber security threat level and assess the impact of the threats to the country.

Malaysia has also implemented the initiative to ensure the adoption and certification of the CNII agencies (public and private) to the MS ISO/IEC 27001: Information Security Management Systems standard and other related certifications. This initiative is to ensure the CNII agencies and organisations have the necessary information security protection in place and are in compliance with the standard. Appropriate measures will also be prepared to protect other non-CNII sectors such as the 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.



Another important cyber security initiative that has been conducted for the past decade is the National Cyber Crisis Exercise (also known as X-Maya). The exercise was designed to test the effectiveness of the procedures that have been developed under the National Cyber Crisis Management Plan (NCCMP) and to assess the readiness and preparedness of critical national infrastructure agencies against cyber-attacks. To date, six (6) national cyber crisis exercises have been organised with the participation from more than 100 public and private agencies across the 10 CNIs.

On another front, Malaysia has also been actively creating awareness and capacity building programmes. Whilst the rapid of ICT, bring benefits and advantages to our citizen, it is also carries risks to the nation's economy, social harmony and security. To manage such risks, public awareness is crucial. Agencies have been carrying out various awareness programmes to educate Malaysians. As a mean to coordinate these programmes, NACSA is developing the National Cyber Security Awareness Master Plan. This Master Plan aims to increase the level of cyber security awareness among Malaysian



cyber citizens through concerted and effective programmes and initiatives. Under this Master Plan, four (4) main target groups, (kids, youth, adults/parents and organisations), were identified for specific cyber security awareness programmes and initiatives. This Master Plan outlines an implementation strategy to ensure it achieves its anticipated goals and objectives.

To address the critical shortage of skilled cyber security professionals, a comprehensive capacity building plan on cyber security will be established riding on the existing initiatives with a more

coordinated mechanism and clear measurement. It will start from the development of school curricula in cyber security; followed by focus-based skills at the institutions of higher learning; and training and skills development schemes for expert and non-experts in both public and private sectors. The government will further enhance the current initiatives especially the Centre of Excellence, a collaboration with the local universities to address the shortage of local talent in the cyber security workforce.

NATIONAL CYBER DRILL EXERCISE



X-Maya is a National Cyber Crisis Exercise, a large scale cyber-attack simulation on Critical National Information Infrastructure

Objectives

- To exercise the workability, identify the gaps and further improve the National Cyber Security Response, Communication & Coordination Procedure
- To raise awareness of the national security impact associated with a significant cyber incident amongst all participants
- To familiarise the participants with cyber incident handling experience
- To test the capability of CNII agencies/organisations in dealing with significant cyber incidents and workability of internal incident handling procedure within CNII agencies /organisations
- To familiarise communications between CNII agencies /organisations with their respective Sector Leads when cyber incidents occur



It is crucial to acknowledge that the security of cyberspace is paramount, now more than ever. In the past, we have seen how the infrastructure of nations and businesses were brought down with significant financial implications.

This is not a far-fetched scenario for Malaysia, especially if we refer to the results of a study conducted by Microsoft in collaboration with Frost & Sullivan on *Understanding the Cybersecurity Threat Landscape in Asia Pacific : Securing the Modern Enterprise in a Digital World* published in July 2018. The study revealed that the potential economic loss in Malaysia due to cyber security incidents could hit up to RM51 billion, which is more than 4% of the total Gross Domestic Product.

As the foundations of our economy become increasingly rooted in digital technologies, Malaysia will model and promote standards that protect our economic security and reinforce the vitality of the nation as a viable marketplace and source of innovation. This will include, among others, the initiatives to promote local industry in emerging technologies and 5G.

The Malaysia Cyber Security Strategy (MCSS) has been designed with tools to provide trust in our cyber environment not only for national security, but

also to support the government agenda in the digital economy, Industry 4.0 and the adoption of other disruptive technologies for Malaysia's advancement. This Strategy will replace the existing NCSP as it is developed to be more inclusive and comprehensive covering protection of CNII, businesses, industries and also citizen. This document includes specific Pillars to define key areas of our concern as well as the necessary strategies for each of them. Each strategy will in turn comprise of a number of action plans and measurement mechanisms that will be implemented within the effective period of this document. Regardless of those mechanisms we need to, we have to realistically remind ourselves that none of these strategies will be effective in combating cyber security issues without the cooperation from all stakeholders.

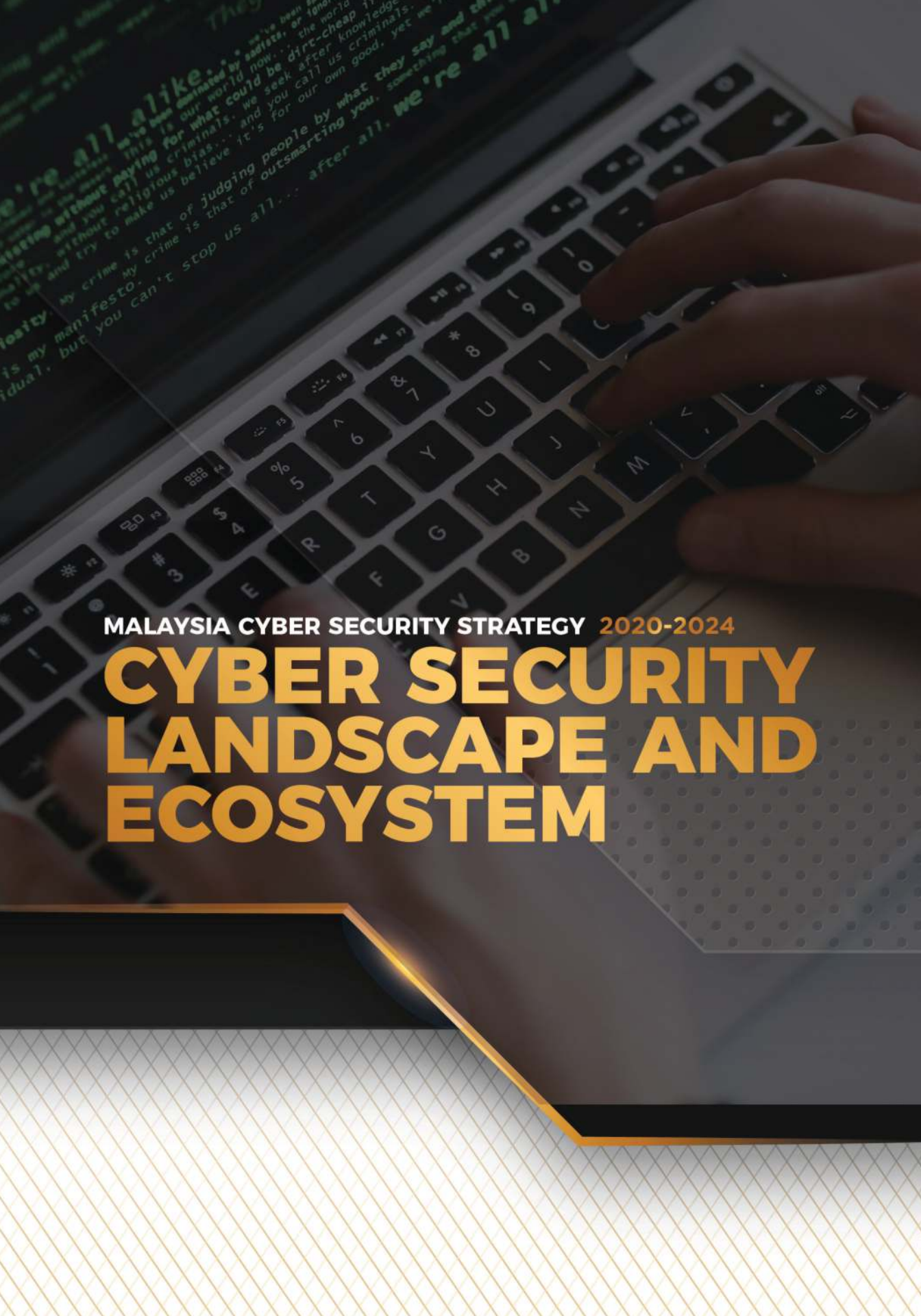
Cyber threats are persistent and there will always be the risk of targeted cyberattacks of massive scale and consequences. Such threats can never truly be eradicated as long as everything stays connected. Yet, they can be mitigated. For this to happen, everyone will have to play their role and work together to enhance Malaysia's overall cyber security readiness, capacity and capabilities.

Vision

Malaysia cyberspace is **secured, trusted** and **resilient**, fostering economic prosperity and citizens' well-being

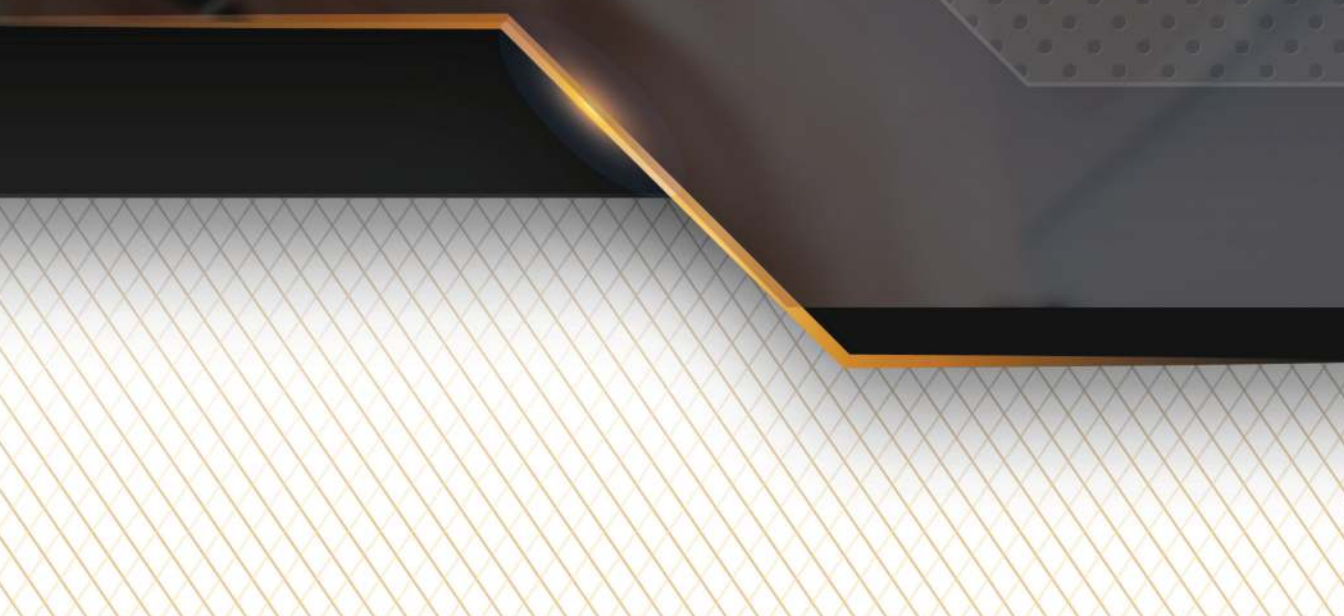
Mission

Fortifying local capabilities to **predict, detect, deter** and **respond** to cyber threats through structured governance, competence people, support best practices processes and deploy effective technology

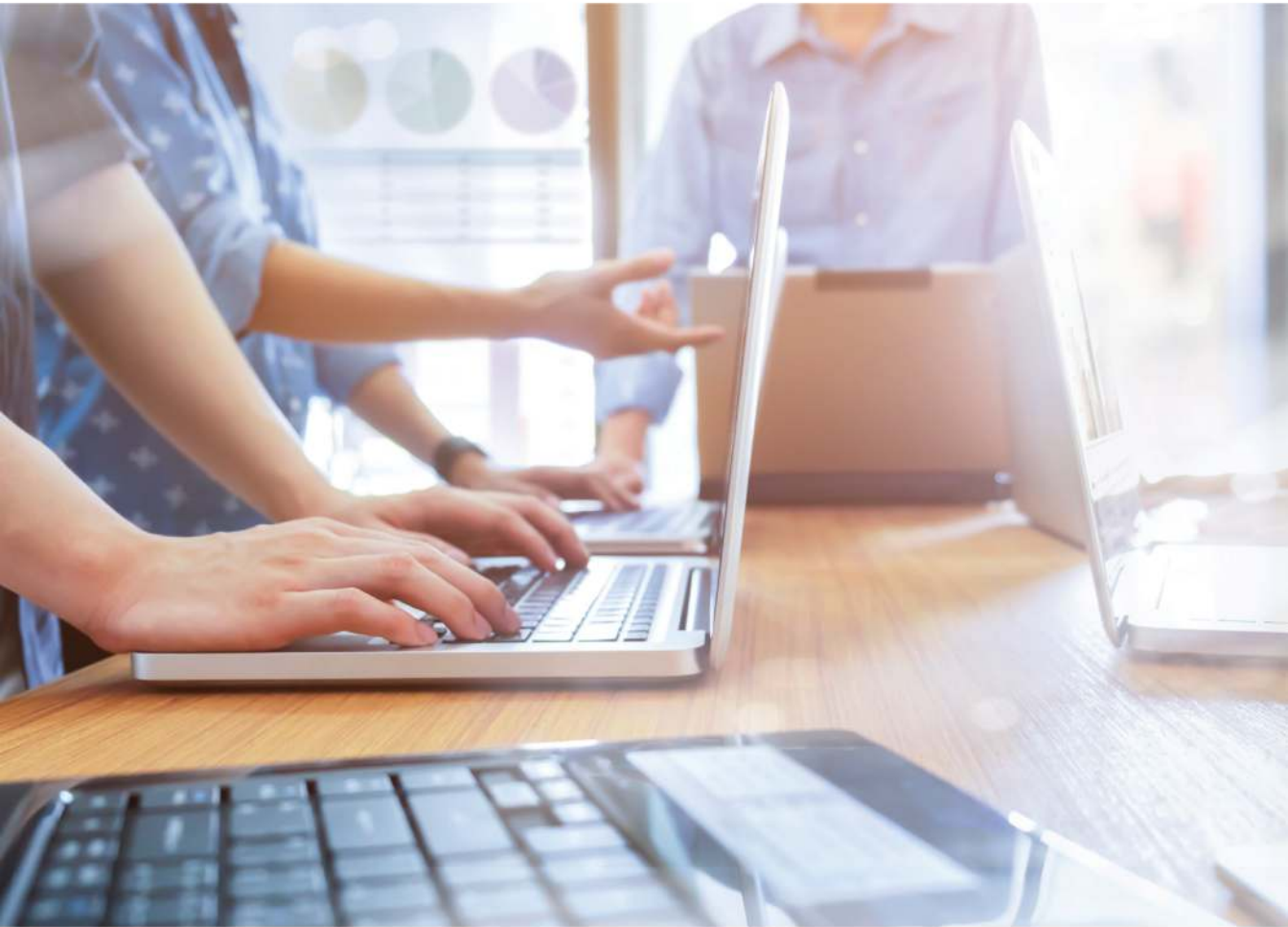


MALAYSIA CYBER SECURITY STRATEGY 2020-2024

CYBER SECURITY LANDSCAPE AND ECOSYSTEM

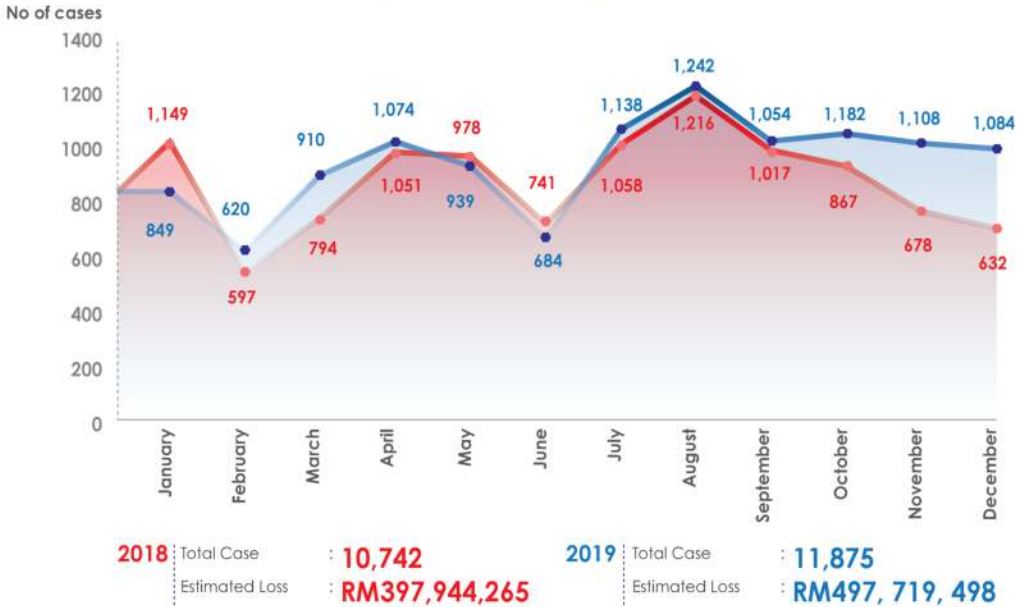


CYBER SECURITY LANDSCAPE AND ECOSYSTEM



According to the Digital Crimes Unit of Microsoft Asia (January 2019), roughly 720 people become preys to cyber criminals all over the world in every minute which translates to more than 1 million victims every day. In 2018, the Royal Malaysia Police had to deal with 10,742 cybercrime cases with an estimated loss amounting to almost RM400 million, while in 2019, the number has increased to 11,875 cases with an estimated loss to almost RM500 million. The numbers may be shocking to some but not if we consider the fact that cyber criminals these days are no longer conduct hacking merely out of curiosity or to test their intrusion and penetration skills, but also for economic gain.

Cybercrime Statistics (2018 & 2019)



SOURCE: Royal Malaysian Police

NC4 reporting reveals that cyber security incidents are increasing since 2016 to 2018. In 2018, a total of 5,627 cyber security incidents were reported to the NC4 compared to 2,981 in 2017 and 2,429 a year before that. Malicious software infections top the rest with 2,244 cases, followed by intrusion attempts and actual

intrusions at 2,076 and 1,270 cases, respectively. However, in 2019 the total number of incidents reported to NC4 has shown a significant decrease to 3,787 cases compared to 2018. This reflects the effectiveness of proactive measures that has been put in place to secure our cyberspace.

Cyber Security Incidents (2016 - 2019)

	2016	2017	2018	2019
DOS / DDoS	49	37	19	14
Intrusion	1,754	1,910	1,270	1,297
Intrusion 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
Total	2,429	2,981	5,627	3,787

Malaysia is also a target of Advanced Persistent Threat (APT) attacks, with the most recent incident manifested by way of email spear phishing. These threats can escalate further given that many Malaysian organisations continue to operate a number of legacy and unsupported systems, which can no longer be updated with the latest security patches. These legacy systems may have multiple vulnerabilities, which are susceptible to attack payloads and tools available to cyber criminals.

There are also concerns about the increasing number of content-related issues in Malaysian cyberspace. While these incidents are relatively still small in number, the impact on the nation is not. Given the speedy and widespread nature of the Internet as a medium of delivery, the effects of content-related issues are potentially more detrimental and damaging. For this reason, Internet-based contents, in the form of fake news, misinformation, contents that are seditious and slanderous in nature, or with racial or religious overtones, are taken very seriously by the

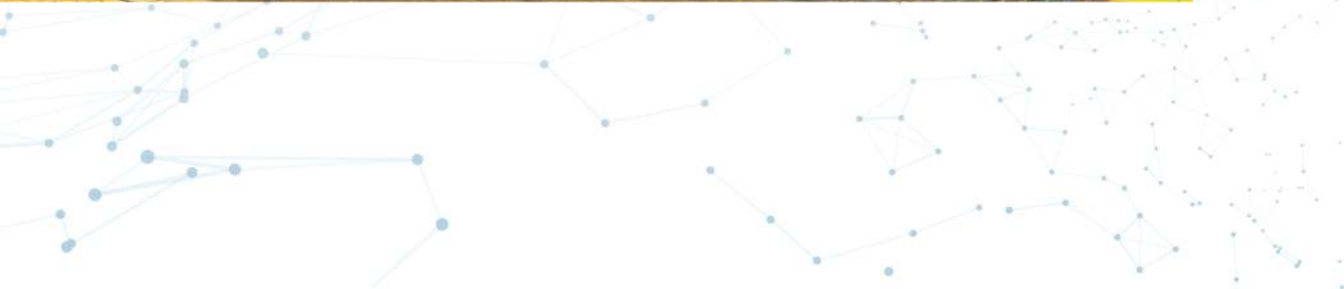
government, while respecting the right to freedom of speech.

As Malaysia continues to embrace digital technologies, there is an increasing need to streamline the management of cybercrimes and incidents to assure the public that all cybercrimes and incidents will be handled appropriately and effectively by the respective law enforcement agencies. There is a need to eliminate duplicative efforts and maximise resource utilisation among the law enforcement agencies.

One of the main reasons for the establishment of NACSA was to coordinate and complement all efforts on cyber security to make sure that all aspects are given due attention. While focusing on cyber security policy, governance and coordination matters, NACSA will also be administering other areas of concern, which will be mandated to specialised agencies.

Efforts concerning other target areas, namely the CNII, cybercrime, awareness, capacity building and international cooperation will be delegated to







selected groups of lead agencies, law enforcement arms and institutions that have the relevant expertise and direct responsibility, as well as the required capacity and capability to deal with the related issues and initiatives.

In Cyber Security Ecosystem, NACSA will serve as the focal point on all matters related to cyber security that also spans vertically to include other existing and aligned national initiatives such as the Digital Infrastructure, Digital Trade, National Security, Digital Malaysia and Digital Government. NACSA serves as an entity that is responsible for streamlining all cyber security planning, development and implementation. To ensure the successful

implementation of the strategy, an effective ecosystem and governance, this Strategy will outline the roles and responsibilities of agencies involved in managing national cyber security. This will be realised by legislating a new National Security Council's Directive, which will elucidate our enhanced national cyber security governance arrangements and the restructuring of committees directly responsible for national cyber security, and delineating the exact roles and responsibilities of all relevant agencies.

MALAYSIA CYBER SECURITY STRATEGY 2020-2024

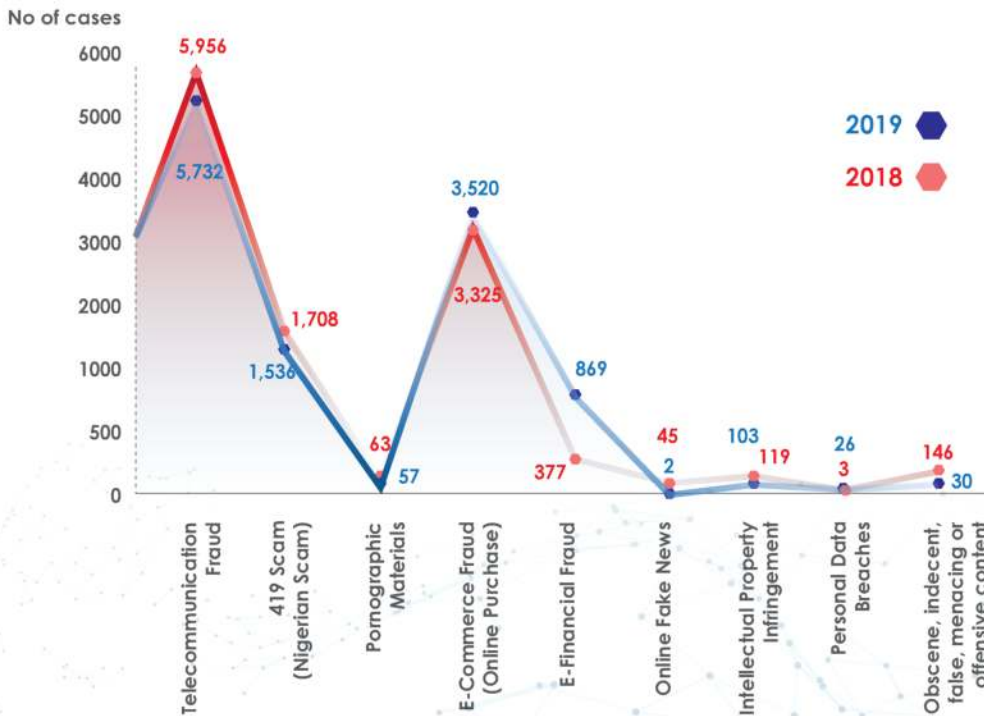
ISSUES AND CHALLENGES

ISSUES AND CHALLENGES

Due to the borderless nature of cyber threats, it can be safely assumed that any or all of them can befall upon any nation. To date, Internet-related fraud has been the most prevalent cyber threat in Malaysia. This is supported by the cybercrime reports received by Royal Malaysian Police in 2018 and 2019 which shows that telecommunication fraud, e-commerce, 419 scam

(also known as Nigerian Scam) and e-financial fraud are among the most prominent threats. Such cases have been known to cause huge monetary losses to the victims. If this trend is sustained, Malaysians will project a greater concern in doing business through an online platform, which indirectly erodes the consumers' confidence in our cyber security measures.

Cybercrime Statistics By Offences (2018 & 2019)



SOURCE: Royal Malaysian Police



However, it is important to note that lack of awareness is the main factor in most of these fraud cases. In phishing incidents, for example, people can be easily duped by bogus sites and services due to their negligence. The same goes for scams whereby unsuspecting victims would transfer huge amount of money to recipients whom they have never met and whose identity cannot be verified – all done for the expectation of an honest purchase, attractive investments and even promises of love.

On another alarming note, the healthcare sector now has other cyber threat concerns that are even more worrying than the attacks and intrusions on electronic medical records. Medical robotic technology and robot-assisted surgical procedures are now connected to computer systems

and networks which expose them to cyber threats. As the patient records are digitised, the risks of breach and disclosure of confidential information are also rampant.

Clearly, much has to be done in terms of creating awareness among the general public. This would explain why cyber security education will soon be introduced even as early as in primary education. Cyber security awareness and education aims to educate citizens from making errors of judgement while transacting on the Internet.

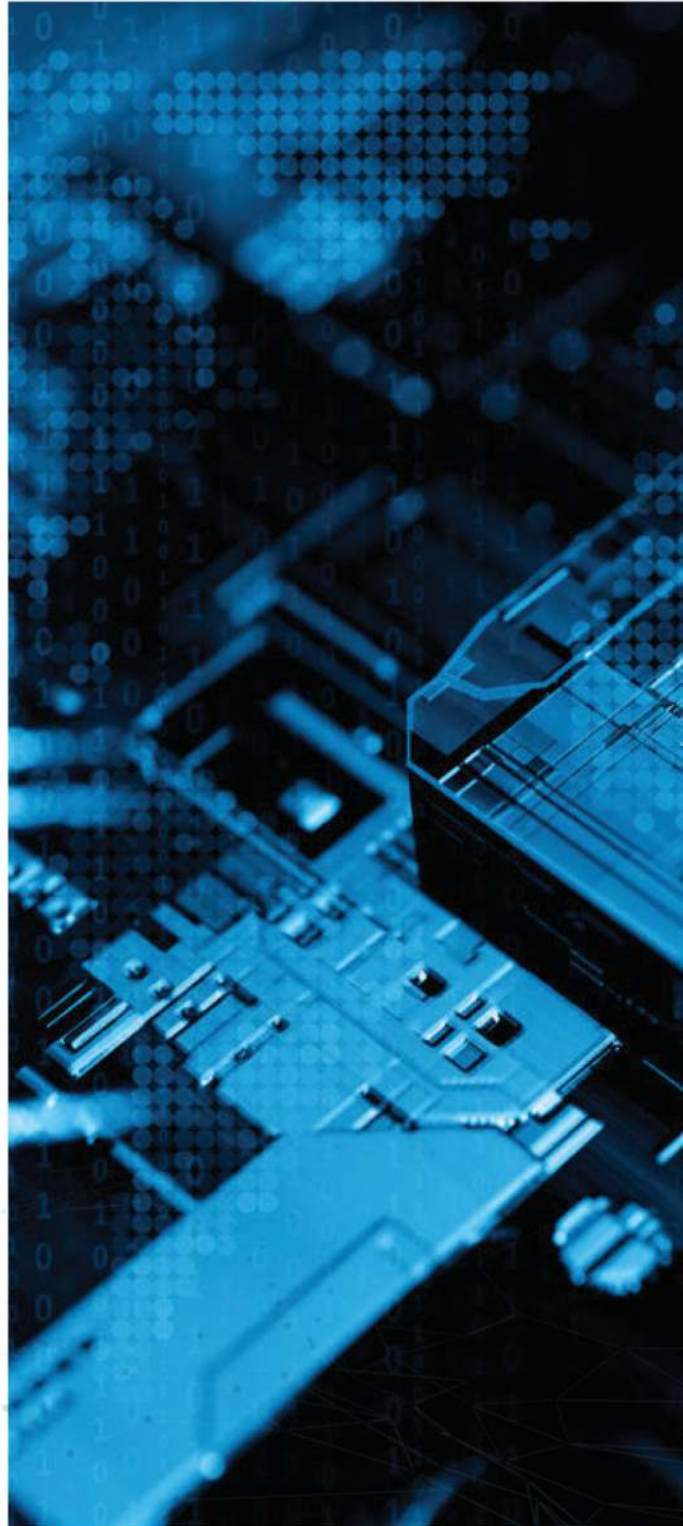
Aside from that, Malaysia is also facing a shortage in its cyber security workforce and talent gaps in many sectors. In today's constantly connected and borderless world, such inadequacy can be disastrous

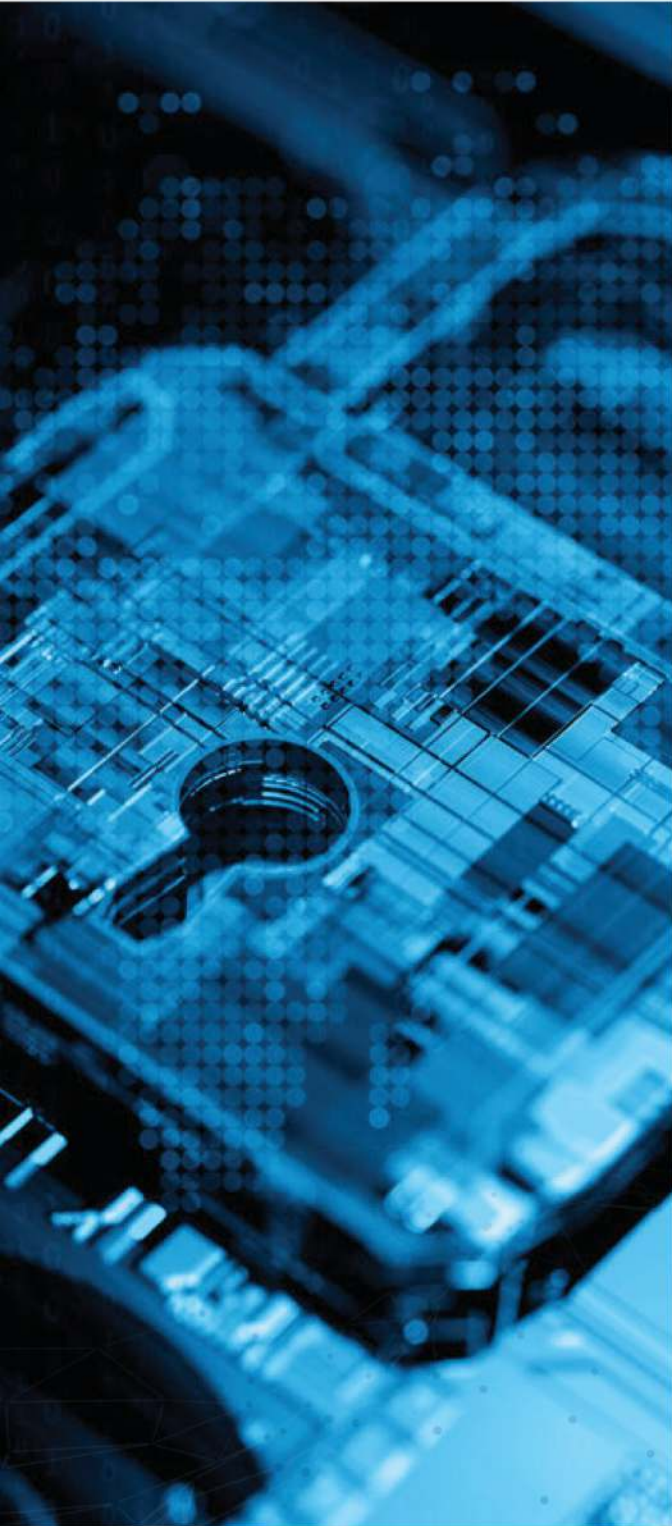
to organisations. The shortage of cyber security professionals will leave organisations vulnerable and exposed to untold dangers from cyberspace.

Insider threats also remain a significant cyber security risk to organisations. Insiders with access to critical information systems and data pose a significant threats to any organisations. There have been numerous cases of intellectual property theft and the leaking of sensitive information that have caused substantial financial and reputational damage.

There were also incidents where these insiders, either employees or vendors, unknowingly became victims of elaborate cybercrime schemes such as through watering hole attacks, social engineering ploys, malware and ransomware infections, propagation mechanism by inserting infected USB devices into the internal networks or arbitrarily clicking on links found in emails or while browsing the Internet.

The government via its relevant agencies and initiatives will have to approach organisations and institutions on best cyber security practices. More efforts have to be made to encourage






necessary controls over system and data access by employees and vendors. The implementation of a proper Bring Your Own Device (BYOD) policy should be deployed by organisations and institutions. Again, awareness also plays an important role here in mitigating incidents due to insider threats, especially for those at the management tier.

Additionally, the correct posture and approach are needed in dealing with the selection of third parties/vendors, planning, development and implementation of ICT projects, especially those that involve or intended for critical establishments such as an Industrial Control System (ICS) for CNII agency. Security-by-Design should be the flagship approach in ICT project development in order to ensure that the end products and systems are free of vulnerabilities and not susceptible to cyber threats. This can only be achieved through continuous testing, authentication safeguards and adherence to best practices.

Malaysia has also been facing threats of terrorism and violent extremism. Terrorists and violent extremists have been using various web services and social media as a breeding ground to entice new




recruits, followers and supporters to their causes. Continuous efforts have been made to curb such threats and there have been successful convictions in recent years. Yet the ease of developing a new website or forum for any agenda presents a growing challenge to law enforcement agencies.

These issues are complex due to the varying interpretation of what would and should be considered as amounting to terrorism or violent extremism. There has been a dire need of manpower and expertise to monitor and correctly identify web contents that would fall under this category. There are also other obstacles including this content which is usually hosted by providers that are beyond our jurisdiction. The lack of awareness among the general public concerning these types of resources reduces the incidents of timely reporting of this content.

Content-related issues, on the other hand, bring a new level of complexity to the challenges of cyberspace. Some issues

concerning pornography and harmful content such as online gambling, information on illegal substances, instructions to make firearms, and misleading and false information, require a coordinated and swift effort and commitment by all parties, which in this case would be agencies and institutions that are directly responsible for network accessibilities. Removal or restriction of access to content that is deemed as harmful by Malaysian law must be pursued.

There is also the issue of differing perspectives on content that may be perceived as either hate speech or seditious, or an appropriate expression of free speech. This is often the case for politically-motivated postings on blogs and social media. While there have been successful convictions from time to time, the creation and spreading of content of this nature does not seem to be lessening, and if anything, they seem to flourish correspondingly to the actual situation of the counterpart issues in the real world.

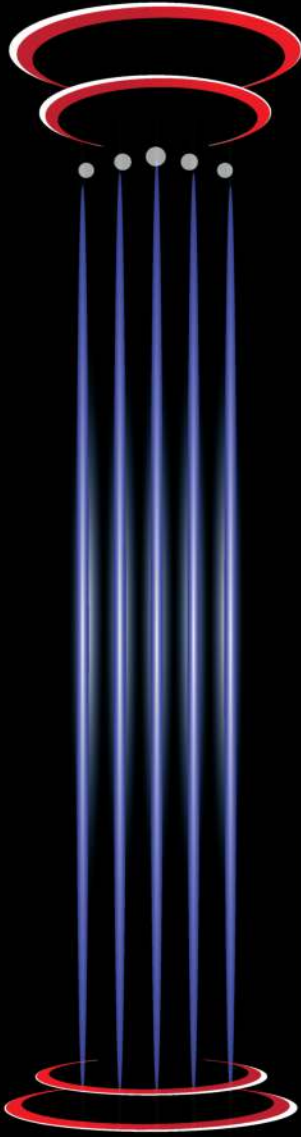


Concerns over the misuse of user personal data are increasing at all levels of society. Citizens are now more vigilant on how and what personal information is shared. The Personal Data Protection Act 2010 has also helped to clarify what would be considered as encroaching user privacy by entities collecting user information. Greater effort is needed to take strong action against those that do not act appropriately to protect personal data.

On the technological side, threats due to vulnerabilities and cyber-attacks are consistently increasing. This is very much due to lack of awareness among users, both in government institutions and business entities; and among individuals. Good cyber hygiene habits - such as creating complex passwords, consistently backing up data, regularly updating and upgrading software and hardware, and limiting privileged access to critical systems - are still lacking among public and private sector users.

All things considered, we believe that it is rather fair to assume that the prevailing issues and challenges in Malaysia's cyber security landscape can be attributed to, first and foremost, awareness and education. Technological solutions and controls can only do so much – it is the netizens themselves that need to have a basic grasp of cyber security essentials and related legislation and regulations so that they can at least avoid the most common pitfalls, particularly while navigating cyberspace.





**STRATEGIC
PILLARS**

STRATEGIC PILLARS

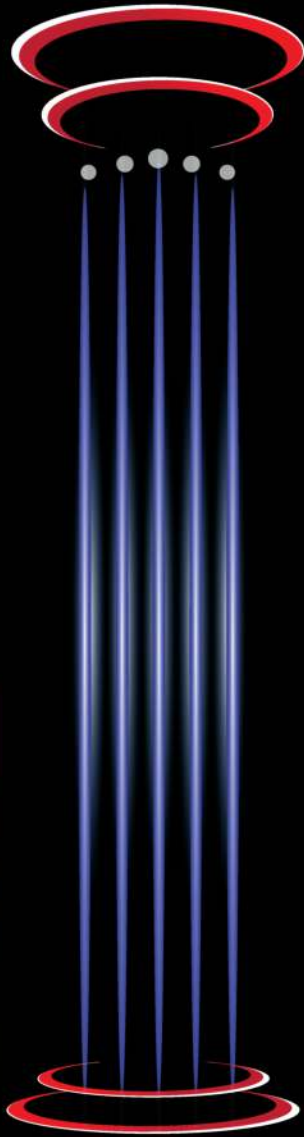
Malaysia Cyber Security Strategy outlines our key objectives, categorised into five strategic Pillars that will govern all aspects of cyber security planning and implementation in Malaysia until 2024. The Strategy is focused on the three overriding success factors for interrelated and interdependent organisational change, namely People, Process and Technology.

For this purpose, *People* represents the need for knowledge, skill and expertise enhancements as well as capacity and capability building among the human capital of the digital era. *Process* covers the development and strengthening, and implementation and maintenance of laws, regulations, procedures and guidelines to effectively govern our cyberspace. *Technology* covers the technology required for effective cyber security implementation.

The Strategy also describes a number of action plans aimed at increasing cyber security in various sectors of the government, businesses and society. These action plans will be measured accordingly to assess their effectiveness.

The five Pillars outlined in this Strategy have been identified as crucial for achieving Malaysia's goals of protecting government and CNII networks, system and data, as well as businesses and citizens, while at the same time combatting cybercrime.



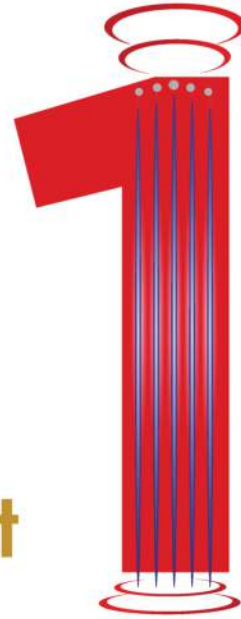


1

EFFECTIVE
GOVERNANCE
AND MANAGEMENT



Effective Governance and Management



Experience has taught Malaysia that the most important measure to safeguard cyberspace is effective governance and management. The management of cyber security risks should evolve simultaneously with the evolution of threats, alongside the adoption of digital in doing business. Ideally, we need a national standard on governance and management, which allows for shared responsibility and cross-sectional integration to optimise the efforts in dealing with any issues, threats or breaches.





To improve national resilience against cyber threats, an active cyber defence approach which ranges from Advanced Persistent Threat to cybercrimes and content-related threats is needed. This approach will include both the defensive and offensive capabilities to effectively mitigate cyber threats, focusing on the capability to detect, analyse, and act upon any cyber threats within our cyber defence ecosystem.

In the quest to achieve greater resilience, Malaysia needs a functional governance and management system that is agile, adoptable and ready to cater

for the challenges of the digital era (and beyond). It has to have the necessary framework and action plans in place, creating a partnership within the ecosystem that will foster close collaborations among stakeholders, including relevant government entities, law enforcement agencies, businesses and industry leaders. Such partnerships will be made possible through the establishment of appropriate platforms for information sharing, strategy-building and resource sharing to form a strong national cyber workforce to manage the ever evolving and ever increasing cyber-related issues and incidents.

This Pillar aims to create effective governance and management through three strategic initiatives, specifically by:



This Pillar aims to achieve the ability to defend our networks, data and systems from cyber threats and subsequently respond to threats effectively in a well-coordinated and concerted manner. Equally imperative is the ability to predict and detect, investigate and disrupt hostile actions against the government, businesses and citizens of Malaysia. To achieve this, the government shall play the crucial role of ensuring that all action plans are properly implemented by the intended entities.

In order to enhance the national cyber security governance framework, we will strengthen governance structures by

clearly defining the roles and responsibilities of all parties within the ecosystem. This can be accomplished by reviewing the current roles and responsibilities held by the existing cyber security stakeholders in Malaysia.

Recognising the critical and highly interdependent nature of CNII organisations from both the government and private sectors in managing cyber security risks and incident responses, the government will continue to clarify the roles and responsibilities of the respective organisations as technologies evolve to ensure the CNII are protected to a level that commensurates with the risks faced.

We will also identify and bridge gaps in responsibilities and coordination among agencies and sector leads in managing incident response by enhancing threat information sharing platforms. At present, there are various cyber security stakeholders in Malaysia in the form of law enforcement agencies and other government bodies with varying degrees of roles, jurisdiction, competence and functions in the cyber security governance value chain. Agencies such as the MCMC, MDEC and CyberSecurity Malaysia focus on regulating the communications and multimedia industry, driving the digital economy and providing ICT security specialist services, respectively. Others like the Royal Malaysia Police and the Central Bank of Malaysia lean more towards law enforcement. Whereas parent institutions such as the Ministry of Communications and Multimedia Malaysia and the Ministry of International Trade and Industry oversee the bigger picture and implementation of policies. For the purpose of improving the national cyber security ecosystem, all these resources must be pulled together and work side by side via a multi-agency coordination protocol with streamlined processes and procedures, and a well-defined scope of authority and accountability.

To achieve this agenda, the government has established NACSA to serve as the central agency for cyber security in Malaysia. At the moment, development and enhancement efforts are now in place to equip NACSA with the necessary capabilities to provide leadership and guidance to all cyber security organisations that will fall under its coordination. In this respect, NACSA will be directly responsible in overseeing the establishment and operations of various information sharing platforms among the various stakeholders. It will also be at the forefront in the identification and management of risks and vulnerabilities that are of significance and concern to the national cyber security ecosystem. Subsequently, NACSA will be the focal point for the implementation of proactive measures to protect the government and CNII agencies' networks, systems and data and to improve inter-agency coordination to combat cybercrime.

The NC4 will be the main hub of all other Cyber Operation Centres in Malaysia. NC4's capability to predict, detect, deter and respond will be further intensified, strengthened and enhanced to address cyber-security related issues.

Even though the government has led many initiatives to improve the current cyber security landscape, it requires the cooperation and collaboration of all stakeholders to achieve the mission to secure our cyberspace and provide a safer environment for all Malaysians. An embedded and sustainable approach is needed whereby citizens, industry and other partners in the society and government, play their full part in securing the networks, services and data. Therefore, efforts will also be taken to enhance collaboration and build trust among government and CNII agencies, businesses and partners through information sharing and Public-Private Partnerships.

To facilitate this, we will provide the engagement programmes and information sharing platforms, such as conducting conferences, seminars, workshops and dialogues where all the stakeholders,

including Chief Executive Officers, Chief Financial Officers, Chief Information Officers, Chief Security Officers and Chief Information Security Officers could share their knowledge, thoughts, experiences and proposals. Such collaboration would pave the way for an appropriate and systematic sharing mechanism and platform on actionable cyber threat information, enhancements of cyber security coordination and the promotion of analytical and technical exchanges between subject matter experts.

A change management plan will also be prepared and subsequently introduced to organisations that are involved to streamline changes and improvements that are required to be in place to support the envisioned governance structure. Also, in order to provide the necessary mechanism and structure for effective



coordination, information and media management, we will be working towards establishing the National Communication Plan. This Plan is necessary to describe the requirements of an information channel that is both capable and quick to accommodate for information sharing during a cyber crisis or incident and will also serve as the main reference to explain the roles and responsibilities of all related agencies with regards to media management.

These are especially crucial given the rapid advancements of the digital age that foresee the expansions of e-government initiatives, e-commerce transactions and digital economy in our daily lives. This is with the inclusion of Artificial Intelligence and machine learning in modern systems, the increasing application of IoT in devices and peripherals, and the extensive use of complex Industrial Control Systems. All of which inadvertently would open up even more avenue for potentials risks and threats to security, safety and privacy.

In essence, Pillar 1 initiatives will cover the protection of the CNII sectors, with support and guidance for businesses and individuals to mitigate cyber threats. Recognising the importance of digital economy, the government will include Trade, Industry and Economy as

one of the CNII sectors. Focus will be made on the development of sector specific guidelines and frameworks, such as maritime and aviation to accommodate current cyber security needs and address the emerging threats, with a key attention on the convergence of Information Technology (IT) and Operational Technology (OT) systems.

Hence, a government-led Technical Working Group will be established to spearhead an in-depth study on laws, rules and regulations as well as standards and best practices in cyber security that have to be adhered to by the CNII agencies. The government will also create a training platform to assist participating organisations in complying with cyber security standards.

The government will work together with private sector entities to promote understanding of cyber security risks, encourage a more informed risk management decisions, and advocate investments in appropriate security measures. This will serve as an effective platform of cooperation between various public and private sectors thus ensuring that business entities and organisations, as well as citizens, adopt the security-centric norms, behaviour and practices that are required to stay safe in cyberspace.

CNII: 11 SECTORS



**National Defence
and Security**

**Banking and
Finance**



**Information and
Communication**



Energy



Transportation



Water



Health Services



Government



**Emergency
Services**



**Agriculture
and Plantation**



**Trade, Industry
and Economy**



We will establish a data leakage protection mechanism through the adoption and implementation of policies, procedures and guidelines related to data protection, public key infrastructure and electronic information management. This will be realised through the development of data leakage protection policy and guidelines as well as the execution of the National Cryptography Policy, which outlines the methods and strategic approach in the use and creation of cryptographic algorithms and cryptography products to protect information that are of national interest.

Management of vendors that deal with government and CNII agencies will also be improved to minimise data privacy and security risks. Awareness initiatives will be conducted on supply chain threats. Supply chain security management will be integrated into agency procurement and risk management process. Vendors, products and services shall be assessed to identify those with high risk and mitigated accordingly. Third parties that are awarded with government projects, especially on ICT, will be required to adhere to information security standards and practices such as the International Organization for Standardization and the International Electrotechnical Commission's ISO/IEC 27001:2013 and ISO/IEC 27002:2013 as well as having the necessary cyber security and information security experts in place.

Management of the Computer Emergency Response Teams (CERTs) will also be improved and strengthened through the enhancement and restructuring of National Cyber Security Incident Response Team (CSIRT), Sector CSIRT and Organisation CSIRT. These CSIRTs will be provided with the necessary capabilities and capacity to handle, mitigate and recover from cyber crisis and incidents. Furthermore, cyber incident reporting will be made mandatory for all government and CNII agencies, while businesses will be encouraged to report them. We will also develop a Vulnerability Assessment Implementation Plan and conduct periodic risk and vulnerability assessment on all critical ICT services. We will

measure the National Readiness Level through periodically-conducted studies.

The government will draw on its capabilities to develop and apply active cyber defence measures to enhance the levels of cyber security readiness across national and government networks. Cyber security courses, content and syllabuses will be developed for government training programmes and for specific target groups that will be identified based on their roles and responsibilities. All existing training platforms will be utilised to establish main training centres that can cater for these target groups and properly meet their needs and requirements in capacity and capability building efforts.





Cyber security incident management will also be enhanced through the revision of the National Cyber Crisis Management Plan (NCCMP) and its reporting mechanism by the first quarter of 2021. Cyber exercises at the organisational, sectoral and national levels will be implemented according to the Cyber Exercise Implementation Plan, of which the findings will greatly contribute to the preparation of the Cyber Readiness Report, planned to be delivered by end of 2021.

Combatting terrorists and violent extremists' use of the Internet will continue to be a priority area, with the main objectives of: raising awareness among the public; and preventing radicalisation and terrorist recruitment and fundraising activities through digital platforms such as social media and web portals. The Southeast Asia Regional Centre for Counter-

Terrorism (SEARCCT) and the Royal Malaysia Police will continue to play their role in monitoring violent extremist activities in cyberspace. An integrated information sharing platform shall be developed to facilitate flow of information between agencies and towards the general public.

Ultimately, under this Pillar, it is expected that a new national cyber security governance structure with a clear division of power and responsibilities is built based on the foundations and principles set forth by the National Security Council's Directive. The implementation of the Malaysia Cyber Security Strategy will be supervised through an annual evaluation process, after which a Malaysia Cyber Security Strategy landscape report will be prepared and presented to the stakeholders for milestone reviews and further deliberations.

SUMMARY

PILLAR 1: Effective Governance and Management

STRATEGY 1 Enhancing National Cyber Security Governance and Ecosystem

- To strengthen governance and ecosystem in cyber security
- To enhance collaboration and building trust among government agencies, CNII agencies, businesses and partners through information sharing and effective Public-Private Partnership
- To establish and implement National Communication Mechanism for effective coordination, information sharing and media management

STRATEGY 2 Improving Organisation Management and Business Operation (Government, CNII and Business)

- To embed cyber security in business operation
- To enhance holistic cyber security controls in supply chain environment
- To comply to International Standard (ISMS, BCMS or equivalent) and Best Practices
- To promote the use of certified ICT security products
- To implement S-SDLC for critical Information System Development
- To establish Data Leakage Protection Mechanism
- To improve CERT Management
- To develop Vulnerability Assessment (VA) Implementation Plan and conduct periodic risk and VA on all critical ICT services
- To measure National Readiness Level through periodical study
- To enhance Industrial Control System (ICS) Protection

STRATEGY 3 Strengthening Cyber Security Incident Management and Active Cyber Defence

- To strengthen capacity and capability in Incident Management
- To develop capacity in combating terrorist/extremist use of Internet
- To enhance national readiness towards bigger scale and targeted cyber attacks



- Protection of Critical Infrastructure through Active Cyber Defence
- Strengthen Incident Management
- Cyber Risk Framework
- Effective Coordination
- Policy, Guidelines, Compliance
- Information Sharing
- Clear Roles & Responsibilities
- Supply Chain Security
- Technology Security
- Protection of SMEs
- Industries Involvement

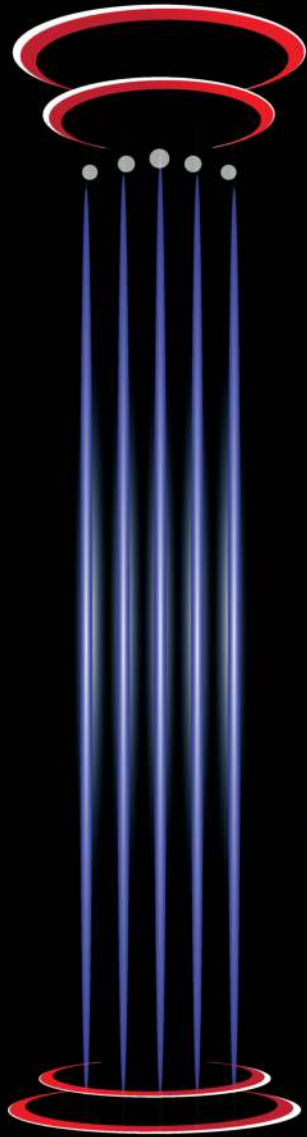


CYBER SECURITY ECOSYSTEM





***NATIONAL CYBER
WORKFORCE***



2

STRENGTHENING
LEGISLATIVE FRAMEWORK
AND ENFORCEMENT



Strengthening Legislative Framework and Enforcement

Malaysia has a comprehensive set of cyber related laws in South East Asia. Since the 1990s, Malaysia has introduced numerous laws to cater for the advent of digital age and the full spectrum of cyber issues.

EXISTING LAWS FOR CYBERCRIME AND CYBER SECURITY ISSUES IN MALAYSIA

Criminal Procedure Code	Penal Code
Sedition Act 1948	Evidence Act 1950
Defamation Act 1957	Prevention of Crime Act 1959
Official Secrets Act 1972	Trade Marks Act 1976
Patents Act 1983	Copyright Act 1987
Direct Sales and Anti-Pyramid Scheme Act 1993	Computer Crimes Act 1997
Digital Signature Act 1997	Telemedicine Act 1997
Communications and Multimedia Act 1998	Consumer Protection Act 1999
Optical Discs Act 2000	Child Act 2001
Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001	Film Censorship Act 2002
Mutual Assistance in Criminal Matters Act 2002	Electronic Commerce Act 2006
Capital Market and Services Act 2007	Electronic Government Activities Act 2007
Personal Data Protection Act 2010	Security Offences (Special Measures) Act 2012
Financial Services Act 2013	Islamic Financial Services Act 2013
Prevention of Terrorism Act 2015	National Security Council Act 2016
Sexual Offences Against Children Act 2017	

The Computer Crimes Act 1997 was enacted in 1997 to address crimes directed at computers and ICTs. This act covers offences such as unauthorised access to computer material and unauthorised modification of computer contents.

As technology evolves at a rapid pace, Malaysia recognises that there are areas in the laws which need to be reviewed to

accommodate new technologies and to reflect new realities, especially in the cyber security domain. The emergence of new cyber threats pose new challenges. Consequently, Malaysia may need to consider mechanisms to enable existing laws to be applied in cyberspace, and, only if required, enact new laws.

This Pillar aims to strengthen cyber security legislation and enforcement through two strategic initiatives, specifically by:



The first order of this Pillar is to study and review all the existing laws and regulations that have been used to deal with cybercrime and cyber security cases. Findings of said efforts will not only pave the way for us to appropriately update the existing legislation and regulation but will also help us introduce a new law in cyber security, if deemed necessary.

Malaysia is fully aware that cybercrime requires a coordinated and cooperative international response. The cross-border nature of cybercrime creates challenges in bringing cyber criminals justice. Recognising that effective regional and international cooperation is crucial in combating cybercrime, Malaysia will continue enhancing regional and international co-operation through existing bilateral



and multilateral cooperation platforms. Malaysia is also striving to strengthen and harmonise domestic legislation with international conventions and treaties.

Malaysia recognises that the challenge presented by cybercrime also requires a coordinated and an integrated national approach. Law enforcement agencies need to work together to address the threats. Malaysia will be taking steps to enhance the capacity and capability of law enforcement agencies to tackle cybercrime by developing and implementing the

National Cybercrime Enforcement Plan (NCCEP). Under this Plan, efforts will be taken to increase the knowledge and skill of judiciary members, prosecutors, law enforcement officers and legal practitioners so as to prepare them for the intricacies of cybercrimes in the digital era.

An expert group will also be established to identify gaps and required improvements in cybercrime enforcement. Furthermore, we also need to foster better collaboration between government agencies and key stakeholders including telecommunication companies,

industries, Internet service providers as well as content providers both at national and international levels. Law enforcement agencies will be equipped with the latest tools and capability for the identification of criminals / malicious parties; and the identification, collection, acquisition and preservation of digital evidence. Digital forensic labs will be enhanced to address the growing complexity of cybercrime investigation.

We will also ensure that the tools and technology, as well as capability enhancements for each law enforcement agency are accredited, directly related and the best available to accommodate the type of cybercrime cases that they handle. A national working group on capacity building and joint collaboration with various training institutions will be established in order to develop specific modules of training and the mechanisms to assess the effectiveness of such training.

The Plan also calls for a clear and streamlined coordination process among central and enforcement agencies. For this purpose, a Cybercrime Coordination Centre will be established. The Centre will focus on ensuring an integrated

and coordinated approach in addressing cybercrime.

This approach is timely since fighting cybercrime requires concerted efforts. In order to achieve effective investigation and successful prosecution of cybercrime, a team of experts, consisting of investigating officers and forensic experts, should be established at the initial stage of the investigation to address and advise on specific issues arising during the investigation process. The Centre will also serve as a central information sharing mechanism between law enforcement agencies to increase efficiency and to minimise delay in investigation.

Such endeavours follows the study on the requirements for the establishment of more cyber courts. The first cyber court was established in September 2016, and was aimed at addressing the increasing number of civil and criminal cyber cases. The dedicated cyber court will ensure that cyber cases receive priority with adequate levels of expertise, which will translate into efficiency in disposal of cyber cases. The government will also examine the feasibility and viability of establishing a specific unit that



combines elements from all of the various government agencies that have been dealing with cyber security cases and incidents under one roof in order to streamline our actions and reactions.

A comprehensive Standard Operating Procedure (SOP) also needs to be developed and endorsed to serve as a guide for law enforcement agencies in investigating cybercrime. This is particularly important as cybercrime have expanded well beyond the virtual domains and now even interconnected with other type of criminal activities such as human trafficking, drug smuggling and illicit recruitment whereby ICT tools are used as an information, communication and coordination platform.

Other than fostering collaborations between local law enforcement agencies, the Plan will also explore the possibility of furthering cooperation with foreign counterparts. This could include cross-border secondments or visiting experts' programmes. It is hoped that through these efforts, more can be shared between like-minded national agencies and experts in dealing with cyber security issues and challenges that are common to all and borderless in nature.

SUMMARY

PILLAR 2: Strengthening Legislative Framework and Enforcement

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

- To enhance and review current legal frameworks to address cybercrime
- To study the need to introduce a new law on cyber security

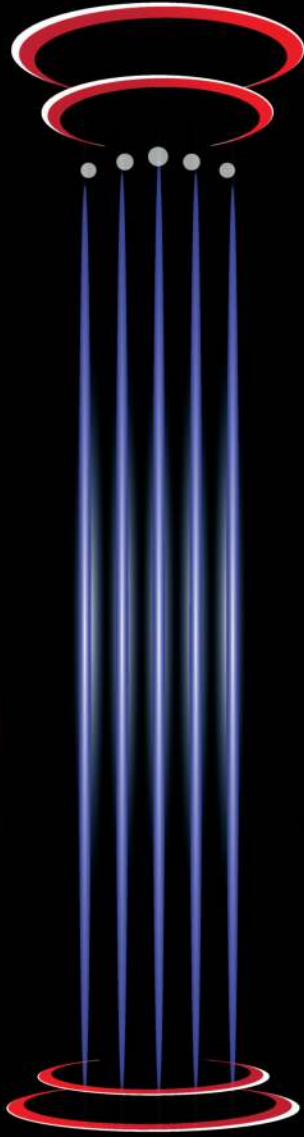
STRATEGY 5 Enhancing the Capacity and Capability of Cybercrime Enforcement

- To strengthen cybercrime enforcement capacity and capability in managing cybercrime, advanced threats and organised syndicates



- Enhancing regional and international cooperation through existing bilateral and multilateral cooperation
- Strengthen cybercrime enforcement capacity & capability in managing cybercrime, advanced threats and organised syndicates
- Review existing laws
- Cyber Security Act





3

CATALYSING

**WORLD CLASS INNOVATION,
TECHNOLOGY, R&D
AND INDUSTRY**



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



To ensure self-reliance and encourage economic growth, the government plans to spur innovative cyber security technology research and development (R&D) by local industry players through the development of the National Cyber Security Research and Development Roadmap and creating a conducive domestic environment for innovation and R&D. The key objective of the Roadmap is to spearhead innovation in the areas of cyber security, safety and privacy protection.



Towards this end, we will establish a R&D collaboration platform between the government, academia and industry with the objective of generating local innovations and scaling-up existing cyber security technology solutions. This will not only address current cyber security challenges, but also drive local industry to compete and thrive at the global level.

MIMOS Berhad is well positioned to spearhead this initiative since it has been very active and productive in driving R&D in Cyber security, together with partners from the academia, industry and government, for more than

two decades. Key areas of R&D include:

- Privacy enhancing technology;
- Digital signature;
- Digital identity;
- Entity authentication;
- Encryption algorithm; and
- Cyber physical security

Technologies developed have been incorporated into various systems to provide higher security posture, for example Malaysian Health Data Warehouse, Government Online Services Gateway, National Cyber Coordination and Command Centre, and the National Digital ID Proof-of-Concept.

Appropriately, this Pillar aims to catalyse world class innovation, technology, R&D and industry in building and strengthening the cyber security innovation ecosystem in Malaysia through two strategic initiatives, specifically by:



Spurring the National Cyber Security R&D Programme



Promoting a competitive local industry and technology

The National Cyber Security Research and Development Roadmap, which will take into consideration of the maturity of R&D initiatives, will be formulated after identifying the priority areas and the prevailing gaps. The Roadmap will outline short-term, medium-term and long-term planning to address security challenges and opportunities brought forward by current and emerging technologies.

The Roadmap will be further supported by the establishment of a shared Centre of Excellence. Specialised programmes will be established to produce more local talent and contribute towards a sustainable and vibrant R&D community. Collaborations will also be fostered between universities, educational institutions, industries and key government stakeholder to help design, create and introduce more industry-oriented courses and specialisations and thereby increase the number of marketable university graduate students in cyber security-related fields of study.





To promote the creation of local technologies and a competitive local industry, we plan to nurture existing companies and create new ventures, supported by the Public-Private Partnership establishment of a Cyber Security Start-Up Hub. The Hub will help to understand and address local cyber security challenges so that companies or start-ups could in turn develop solutions and services that are relevant and ready to serve local needs and subsequently scale up to meet global requirements. The Hub will also provide incentives and appropriate platforms for companies to share information. The Hub will assist companies with marketing their products locally and globally. A national programme will facilitate adoption of locally developed cyber security products, solutions and services within critical national infrastructure.

There will also be a notable expansion of funding, through additional government grants and incentives, to help promote the acceptance and adoption of locally developed cyber security products, solutions and services by CNII organisations, including government agencies and private sector organisations.

SUMMARY

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


STRATEGY **6** Spurring National Cyber Security R&D Programme

- To stimulate and encourage cross discipline research and collaboration

STRATEGY **7** Promoting a Competitive Local Industry and Technology

- To stimulate the creation of new local cyber security ventures through the establishment of cyber security start-up / ideation hub
- Promote the use of local ICT security products and services and support the growth and expansion of the local cyber security industry
- To strengthen academic centres of excellence in universities through collaboration with academia, educational institutes and industry

RESEARCH & DEVELOPMENT ROADMAP



Stimulate and Encourage Cross Discipline Research and Collaboration



Spearheading Innovation in the Areas of Cyber Security

SHARED CENTRE OF EXCELLENCE




Collaboration Platform Government-Academia-Industry



Creating a Conducive Environment for Innovation and R&D

LOCAL INDUSTRY DEVELOPMENT

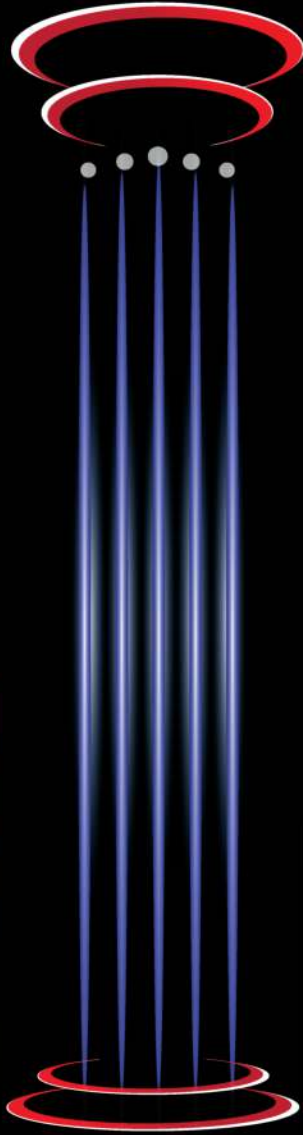


Promote the use of local ICT security products and services and support the growth and expansion of the local cyber security industry

Stimulate the creation of new local cyber security ventures through the establishment of cyber security start-up/ideation hub

Generate local innovations

- Scaling-up existing cyber security technology solutions
- Drive local industry

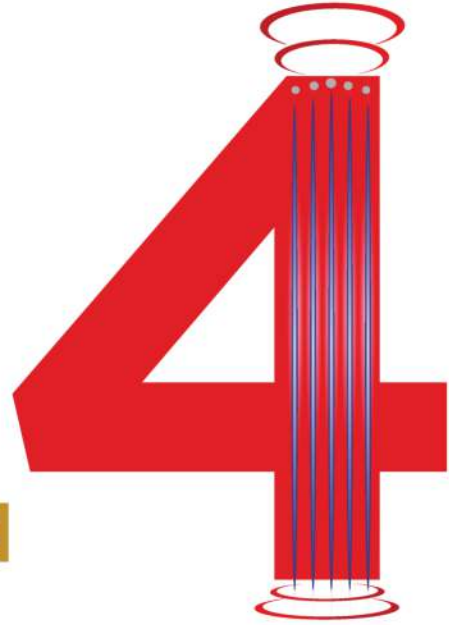


4

**ENHANCING
CAPACITY AND CAPABILITY
BUILDING, AWARENESS
AND EDUCATION**

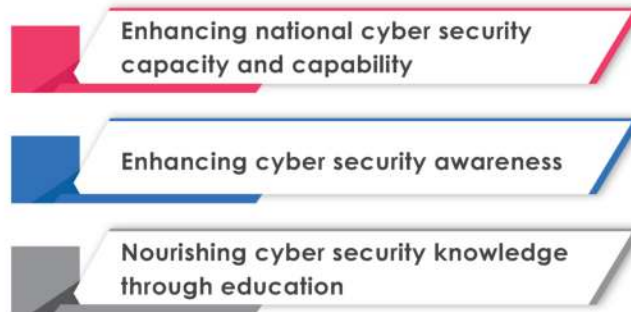


Enhancing Capacity and Capability Building, Awareness and Education



To meet the challenges of the rapidly changing nature of cyber threats, the government will develop and implement a comprehensive National Cyber Security Capacity and Capability Plan that will determine the areas of expertise and skill sets that will need to be continuously improved and enhanced at national, sectoral and organisational levels.

Correspondingly, this Pillar aims to enhance capacity and capability building, awareness and education through three strategic initiatives, specifically by:



The Plan will be implemented by building coherent cross-sector collaboration in strategic information sharing and security awareness initiatives, deepening the understanding of advanced threats, developing a culture that understands security risks in the context of business resiliency and expanding the capability to develop a safer and more resilient technology, as well as the ability to respond to advanced threats.

Malaysia has been developing and implementing cyber security capacity and capability through various ministries, agencies and CNII organisations. Enhancements of national cyber security capacity and capability will be focused on increasing the number of local skilled professionals through training and certification programmes to meet the demands

for skilled workforce in both the public and private sectors. Specialist skill development, on the other hand, requires pursuing good quality and established security professional certifications primarily in specific areas of cyber security domain, that are lacking in the country.

Meanwhile, awareness and education would require, among other things, the identification of necessary target audiences and content development approaches that can enable resource sharing and collaboration. The government, through its various agencies, will take up the crucial role of empowering all levels of society to understand cyber security-related risks and challenges, as well as the necessary defensive measures needed for safer Internet use.

The Malaysia Digital Economy Corporation, the lead agency for driving the digital economy in Malaysia, will spearhead efforts to increase the number of local skilled professionals, which will include talent development initiatives through new talent, up-skilling and re-skilling. The government will also provide additional funding and scholarships in order to encourage knowledge acquisition and enrichment among existing cyber security professionals. This will help develop a new generation of a cyber security professionals, with the necessary education and skills.

Currently, CyberSecurity Malaysia has started its efforts to increase the number of local cyber security professionals through the implementation of Global Accredited Cybersecurity Education (ACE) Scheme. It is a holistic professional certification scheme established indigenously to certify and recognise cyber security personnel in tandem with ISO/IEC 17024 on people certifications, ISO/IEC 9000 on processes and ISO/IEC 27001 on security management.



Enhance capacity at national sectoral organisation

New talent up-skilling and re-skilling



Realising that cyber security is about human interaction and attitude towards technology, we will need to inculcate the importance of adhering to cyber hygiene practices among government and CNII entities, businesses and the general public. Currently, there are various cyber security awareness initiatives undertaken by relevant agencies or organisations through various approaches and target groups.

To name a few;

- NACSA has published the *10 Easy Steps for Cyber Security Awareness* that outlines all of the most sensible practices in cyberspace;
- Malaysian Modernisation and Management Planning Unit (MAMPU) has been organising cyber security awareness programmes for 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 organised various programmes 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

Increase the number of local skilled professionals through training and certification programmes

Adhering to cyber hygiene practices

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 officer as part of its annual cyber security awareness programme;
- 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.





These commendable initiatives at the same time are experiencing challenges in terms of resources, coverage, approaches and target groups that have hindered the effectiveness of the implementation.

To enhance Malaysia's approach on cyber security awareness, the government will develop and implement the National Cyber Security Awareness Master Plan. Under the Plan, the National Cyber Security Awareness Governance structure will be established, which aims to develop an integrated and concerted cyber security awareness programme. The primary aim of the integrated programme is to reduce the number of cyber incidents by running cyber security awareness programmes and call for actions that are more organised, coordinated and able to reach a wider target audience among Malaysians.

The Plan will outline integrated initiatives on public-private driven collaboration and coordination, and the mobilisation of resources



to enable a wider outreach of programmes to kids, youth, adults/parents and organisations. Initiatives by various agencies will also be implemented in an integrated and coordinated manner to ensure a wider coverage and bigger impact. This will be crucial to educating citizens on the necessary knowledge to detect and avoid abuse, fraud and crime online, as well as to nurture accountable behaviour, thereby creating well-informed and responsible cyber citizens.

At the same time, we will also be working on establishing a creative content development programme mechanism that brings together all the stakeholders, from both the public and private sectors, to share their experience and best practices on creating awareness. It is hoped that a unified national brand of cyber security awareness programme can then be developed, one which streamlines the content of various awareness programmes based on the accepted security baseline framework. A corresponding

measurement mechanism will also be appropriately devised to evaluate the effectiveness of said programmes and to identify ways to improve them from time to time.

Cyber security will also become part of the syllabi at the primary, secondary and tertiary level of education. Given the increasing threats from cyberspace and the all-embracing nature of ICT and the Internet, especially among the younger generation of Malaysians, we believe that it is never too early to introduce and foster cyber security awareness. Our youth needs to be equipped with the necessary cyber security knowledge and tools to ensure safety and security.

In academia, there is a need to embed cyber security across taught courses under ICT and Computer Engineering programmes. As an example, cyber security requirements need to be taught in Software Programming (secure coding), Software and System Development Cycle (Secure SDLC), Database,





Operating Systems, Network, IT Administration and Management, as well as cross platform application development. This effort is in addition to the present dedicated cyber security related courses being taught in colleges and universities.

The same effort of introducing cyber security related issues across non-ICT or non-Engineering disciplines covering cyber law in Law, FinTech in Finance, security risk management of network ready medical devices in Health, among others, is necessary to enable graduates to stay relevant and to be able to grasp the impact of new technological developments.

Within the Public Service Department, there is a need to establish cyber security as a vertical (grade) in the government sector to enable specialisation in the various domains under information security and to enable retention of these trained personnel within their expertise by providing sufficient opportunities for career growth.

SUMMARY

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

STRATEGY 8 Enhancing National Cyber Security Capacity and Capability Building

- To develop National Cyber Security Capacity and Capability Building Plan
- To develop a comprehensive plan to build adequate tools and technology through an integrated approach

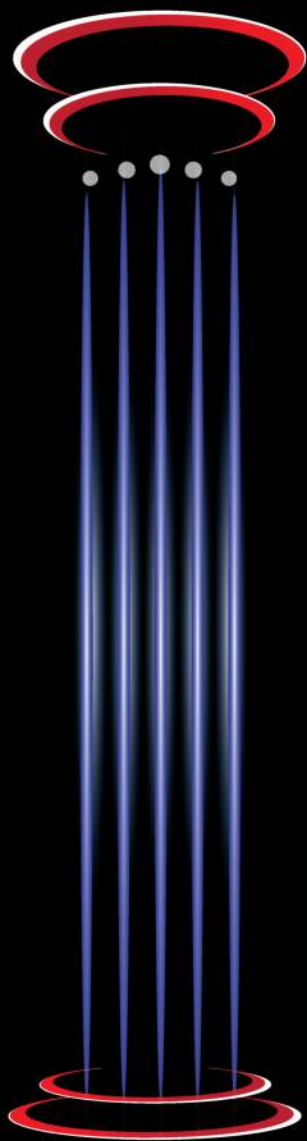
STRATEGY 9 Enhancing Cyber Security Awareness

- To improve cyber security awareness programme implementation approach through the implementation of the National Cyber Security Awareness Master Plan

STRATEGY 10 Nourishing Cyber Security Knowledge Through Education

- To develop cyber security subject as one of the syllabi at the primary, secondary and tertiary level through collaboration with Ministry of Education





5


STRENGTHENING
GLOBAL COLLABORATION



Strengthening Global Collaboration



In the digital age, no nation or economy can remain in a silo in combating cyber threats. Global collaborations, including information and knowledge sharing, as well as international cooperation and enforcement, are crucial to effectively counter evolving cyber threats. The nature of the Internet – which is ambiguous and anonymous – may contribute to the misperception, misinterpretation and misrepresentation of cyber threats or attacks, leading to potential escalation or tension between states. As such, it is imperative to instil trust and transparency between states through close international cooperation on cyber issues.



International engagement is also pivotal to combat cross-border threats and attacks involving multiple jurisdictions. Strong international engagement plays important roles in addressing the challenge, particularly in expediting cross-border enforcement activities.

Fostering global collaboration is thus a key component of this strategy. Malaysia needs to engage with other trusted international entities to strengthen cooperation that is mutually beneficial, while

respecting state boundaries and sovereignty.

While establishing or enhancing cooperation will significantly strengthen relationships, Malaysia is also committed to adhering to the international commitments and obligations with regard to cyber security (where appropriate), be it at regional, sub-regional or multilateral level. Malaysia also recognises the need to build capacity in cyber diplomacy.

For that reason, this Pillar aims to strengthen global collaboration through two strategic initiatives specifically by:



Strengthening international collaboration and cooperation in cyber security affairs



Demonstrating Malaysia's commitment in promoting a secure, stable and peaceful cyberspace to uphold international security

The primary element in accomplishing the first strategic initiative is through embedding cyber security as a key priority in our foreign policy. The development of a cyber security international engagement plan will be the next step – it will enable Malaysia to enhance and coordinate its international engagement across government. A dedicated working group will be established to develop this plan.

Having a comprehensive plan will only be beneficial if the government machinery responsible for implementation is well equipped with appropriate skills and knowledge. Hence, the relevant government agencies will work together to embed cyber security as one of the elements in our diplomatic and international affairs capacity building programme. The aim is to ensure that our diplomats around the globe have a clear understanding of key cyber security issues and knowledge of our national context.





Malaysia will continue to foster bilateral relations in cyber security with other nations and identified international organisations or industry players through the creation of official collaboration instruments either by Memorandum of Understandings, joint statements or legal instruments. The efforts will be followed through with practical collaborations such as knowledge sharing and transfers, joint R&D, technology transfers, information exchange and training, policy dialogues, jointly organised programme, and discussions on harmonisation of legislation.

Malaysia will also continue to actively participate and contribute in regional, sub-regional and multilateral cyber security collaboration efforts through the United Nations (UN), the Association of South East Asian Nations (ASEAN) and its dialogue partners, the Asia-Pacific Economic Cooperation (APEC), the Commonwealth, the Organisation of Islamic Cooperation (OIC), the Global

Forum on Cyber Expertise (GFCE), the Asia-Pacific Computer Emergency Response Team (APCERT), the Forum of Incident Response and Security Teams (FIRST), the Council of Europe, and other international entities. Malaysia will innovate proposals on international cyber security cooperation tailored to the interest of the respective fora in collaboration with the identified partners. Concurrently, we will also promote international collaboration in both the public and private sectors, and establish strategic alliances with international partners and entities that share our vision. Malaysia will also strive to be at the forefront of international discussions by driving, chairing and hosting regional and international cyber security fora as well as conferences.

We will intensify our efforts to disrupt the business model and infrastructure of organised crime

through greater cross-border collaboration. We will learn from the successes and failures of others in policing and enforcing cyber security such as in dealing with infringements of copyright, computer-related fraud, child pornography, online gambling and violations of network security to help improve cyber security measures. Intelligence from trusted international partners on issues with implications to the nation, especially on critical national infrastructure, will be constantly monitored and responded to accordingly. Malaysia will also engage the international platforms, primarily in international standards development and ratification of treaties, to ensure that any new international cyber security norms being developed does not contradict our national interest.





To demonstrate Malaysia's commitment in promoting a secure, stable and peaceful cyberspace with the aim of upholding international security as per the second strategic initiative, we will shape a concerted national position on key international cyber security issues particularly with regard to norms, rules and principles of responsible states' behaviour, how international law applies in cyberspace, as well as Confidence Building Measures (CBMs). With regard to CBMs, Malaysia aims to intensify efforts in driving CBMs within ASEAN in collaboration with identified

dialogue partners with a view to elevate trust and confidence between states in cyberspace.

In taking the steps toward realizing Malaysia's commitments in international cooperation, we will also constantly review and assess the effectiveness of efforts and investments that have been made thus far.

In the long run, we aspire to be recognised and seen as a country that promotes and upholds international stability in cyberspace based on the existing international agreements on all of these matters.

SUMMARY

Pillar 5: Strengthening Global Collaboration

STRATEGY 11 Strengthening International Collaboration and Cooperation in Cyber Security Affairs

- To address cyber security as a priority in foreign policy
- To align domestic and International cyber security efforts
- To recognise cyber security as one of the elements in diplomatic and international affairs
- To actively participate and contribute in key international cyber fora and strategically collaborate with international partners
- To identify and establish formal and informal bilateral cooperation in cyber security

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

- To shape a concerted national position on the operationalisation of norms, rules and principles of responsible behaviour of states and how international law applies in cyberspace
- To continue efforts in driving regional Confidence Building Measures (CBMs)

Shape a concerted national position on norms, rules and principles of responsible behaviour of states and how international law applies in cyberspace

Shape a concerted national position on norms, rules and principles of responsible behaviour of states and how international law applies in cyberspace

Continue efforts in driving regional Confidence Building Measures(CBMs)

Address cyber security as a priority in foreign policy

Actively participate and contribute in key international cyber fora and strategically collaborate with international partners

Align domestic and international cyber security efforts

Identify and establish formal & informal cooperation in cyber security

Recognise cyber security as one of the elements in diplomatic and international affairs





MALAYSIA CYBER SECURITY STRATEGY 2020-2024

CONCLUSION

CONCLUSION



Malaysia has committed to providing a cyberspace that is secure, trusted and resilient, and also encourages economic prosperity and supports social well-being. We are confident that this can be accomplished by strengthening our capabilities to predict, detect, deter and respond to cyber threats.



In the face of constantly changing cyber threats, Malaysia needs to be prepared, more than ever, to protect its national security and sovereignty. Although the global community agrees on the importance of cyber threats, there are still continuing discussions at the regional and international levels as to how to effectively combat them. There will always be questions on how far a nation can or should go in responding to what it perceives as a threat to its national security and sovereignty, and the complexities surrounding such a situation when the cyber incidents are cross-border in nature.

The Malaysian government will strive to meet its responsibilities and lead the national response; however, businesses, organisations and individual citizens also have to play their roles and take reasonable cyber hygiene measures to protect themselves and ensure that they are cyber resilient and able to continue

operating in the event of a cyber incident.

NACSA will play its part in providing cyber security guidance and coordination while keeping pace with existing and emerging cyber threats and the development of new technologies. All the necessary steps will be taken to ensure ease of access and sharing of threat information among government entities, businesses and the general public. NACSA will also provide advice on the risks and the actions necessary to mitigate them.

However, the effort to develop such competencies has to be supported by a structured governance that provides the means, funding and facility required to cultivate a competent workforce, maintain the appropriate standards, policies and best practices, and implement the most effective approach and solutions to address cyber security issues.

The main duty of the government is and will always be to defend the nation, its economy and prosperity as well as its citizens from threat and harm by internal and external factors, be it from cyberspace or otherwise. It is therefore pertinent for Malaysia to set the rules, standards and expectations over all elements and entities under its control and responsibility in order to ensure a safe and secure cyberspace; and to collaborate with trusted parties from the international community that share the same objective and aspiration.

For all these to be realised, there has to be a sense of inclusiveness, first and foremost, among all the stakeholders at the national level. Securing the national cyberspace will indeed require a collective effort. All roles and functions within the cyber security ecosystem that are outlined by the strategies are eventually connected and interdependent with one another, which clearly show that cooperation will always be a key aspect in ensuring success, security and peace.

To support the national interest, Malaysia needs a class of competency, capability and awareness that can truly safeguard the national cyberspace, its critical sectors, businesses and most importantly the well-being of its citizens, not only from external threats but also those from within. It is also important to highlight that while we will always uphold the right to a free cyberspace, we also acknowledge that constraints and controls are still needed at some levels of access and provision to ensure that our intrinsic values as a multi-racial nation and society are protected and kept intact.

In the long run, this can significantly assist in ensuring uniformity in the adoption and implementation of standards, policies and guidelines among all cyber security stakeholders in Malaysia. Again, we should remind ourselves that any strategy or planning will only be as good as the people behind it. Therefore, for the next five years, everybody must pull together or face the risk of getting left behind in the digital era.

ACKNOWLEDGEMENT

In the journey of the development of the Malaysia Cyber Security Strategy (MCSS), an extensive deliberations, engagements and dialogues with a range of stakeholders has been carried out to gather inputs, feedbacks and insight from their point of view. A series of workshops, seminars and conferences has been conducted which involved government ministries and agencies, CNII agencies, enforcement agencies, industry, businesses, academia, non-government organisations as well as the public.

On the other hand, Academy of Sciences Malaysia (ASM) has conducted an exercise to understand the issues and challenges that affect the national infrastructures, businesses and the well-being of citizens, as well as to identify the gaps in cyber security in Malaysia. As a result, ASM has produce an advisory report which outline the relevant strategies and specific recommendations towards ensuring a safe and secure national cyber environment. The advisory report also being used as a reference in developing the Malaysia Cyber Security Strategy.

On that note, the Government would like to express an appreciation to everyone for their commitment, contribution and efforts towards the completion of MCSS.



A token of appreciation to:

Ministry of International Trade and Industry
Ministry of Defence
Ministry of Finance
Ministry of Education
Ministry of Transport
Ministry of Women, Family and Community Development
Ministry of Higher Education
Ministry of Home Affairs
Ministry of Communications and Multimedia Malaysia
Ministry of Foreign Affairs
Ministry of Science, Technology and Innovation
Ministry of Health
Ministry of Domestic Trade and Consumer Affairs
Ministry of Youth and Sports
Attorney General's Chambers
The Office of Chief Government Security Officer
Malaysian Administrative Modernisation and Management Planning Unit
Economic Planning Unit, Prime Minister's Department
Implementation Coordination Unit, Prime Minister's Department
Public Service Department
Royal Malaysia Police
Department of Personal Data Protection
Department of National Unity and National Integration
Department of Islamic Development Malaysia
Department of Federal Territory Islamic Affairs
Defence Intelligence Staff Division, Ministry of Defence
Southeast Asia Regional Centre for Counter Terrorism
Council of Trust for the People
Central Bank of Malaysia
Malaysian Communications and Multimedia Commission
Securities Commission Malaysia
National Water Services Commission
Energy Commission
Companies Commission of Malaysia
Malaysian Aviation Commission
Bursa Malaysia
Inland Revenue Board of Malaysia
Intellectual Property Corporation of Malaysia
Technology Depository Agency Berhad

Malaysian Industry-Government Group for High Technology
Malaysia Digital Economy Corporation Sdn Bhd
SME Corporation Malaysia
MIMOS Berhad
CyberSecurity Malaysia
Communications and Multimedia Content Forum of Malaysia
Academy of Sciences Malaysia
Malaysia Airlines Berhad
Telekom Malaysia Berhad
GITN Sdn Berhad
Malayan Banking Berhad
Malaysian Social Institute
Science & Technology Research Institute for Defence
Institute for Youth Research Malaysia
Institute of Strategic and International Studies Malaysia
Retirement Trust Fund
Muslim Youth Movement of Malaysia
International Islamic University Malaysia
National Defence University of Malaysia
Technology University of Malaysia
Technical University of Malaysia Malacca
Association of Banks in Malaysia
Association of Islamic Banking Institutions Malaysia
National Tech Association of Malaysia
Childline Malaysia
Generasi Gemilang Foundation
Microsoft Malaysia
Mudah.my Sdn Bhd
Pos Digicert Sdn Bhd
DiGi Telecommunications Sdn Bhd
Commercial Circle Sdn Bhd
Cyber Intelligence Sdn. Bhd
Firmus Sdn Bhd
Informology Sdn Bhd
LGMS / LE Global Services Sdn Bhd
NanoSec
Netbytesec Sdn Bhd
OWASP
Phoenix Pinnacle Sdn Bhd
Rawsec
Techforte Sdn Bhd

ABBREVIATIONS

AGC	Attorney General's Chambers
AI	Artificial Intelligence
APCERT	Asia-Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ASEAN	Association of South East Asian Nations
BYOD	Bring Your Own Device
CBMs	Confidence Building Measures
CERT	Computer Emergency Response Team
CGSO	Chief Government Security Office
CMCF	Communications and Multimedia Forum of Malaysia
CNII	Critical National Information Infrastructure
CSIRT	Cyber Security Incident Response Team
FIRST	Forum of Incident Response and Security Teams
GFCE	Global Forum on Cyber Expertise
ICS	Industrial Control System
ICT	Information and Communications Technology
IoT	Internet of Things
IT	Information Technology
MAMPU	Malaysian Modernisation and Management Planning Unit
MCMC	Malaysian Communications and Multimedia Commission
MCSS	Malaysia Cyber Security Strategy
MDEC	Malaysia Digital Economy Corporation
MOE	Ministry of Education
MOH	Ministry of Health
MWFCD	Ministry of Women, Family and Community Development
NACSA	National Cyber Security Agency
NC4	National Cyber Coordination and Command Centre
NCCEP	National Cybercrime Enforcement Plan
NCCMP	National Cyber Crisis Management Plan
NCSP	National Cyber Security Policy
NSC	National Security Council
OIC	Organisation of Islamic Cooperation
OT	Operational Technology
R&D	Research and Development
SEARCCCT	Southeast Asia Regional Centre for Counter-Terrorism
SOP	Standard Operating Procedures
UN	United Nations
UNICEF	United Nations Children's Fund



NATIONAL SECURITY COUNCIL

Prime Minister's Department

Level LG & G, West Wing
Perdana Putra Building
Federal Government Administrative Centre
62502 Putrajaya
MALAYSIA