Science and Technology Trends
Governance Systems for Cybersecurity

National Cybersecurity Governance and Implementation of Malaysia for the Critical National Information Infrastructure

Mohd Shamir Bin Hashim

1. The Policy on Cybersecurity

1.1. Background

In 2005, the Malaysian Government realized the interdependency of ICT infrastructures, mainly through the Internet, brings great benefits and enables the country to turn knowledge into value for the benefit of the people. However, this same interdependency means that the country's modern industrialized society is now increasingly vulnerable to cyber threats that have potential devastating impacts. The interdependent and borderless nature of the Internet increases the number of attack vectors and makes bringing cyber criminals to justice an ever more challenging task.

The increasing pervasiveness, connectivity and globalization of information technology and the dynamic nature of cyber threats means that countries must adopt an integrated approach to protect their Critical National Information Infrastructures (CNII) including efforts to focus resources, strengthening the law enforcement, improving coordination, enhancing research and development, facilitating information sharing, and encouraging greater public and private cooperation. This approach is in a form of a cybersecurity policy which focuses on protecting the country's CNII.

1.2. Policy Domains

In coming up with a cybersecurity policy, the following domains were considered.

1) Legislation − identify and review the existing laws and regulations governing cybersecurity and to perform analysis to confirm compliance to international laws;
2) Institutional − review existing institutional arrangements and identify the roles and responsibilities that coordinate national security efforts in protecting the CNII against cyber threats;
3) Technology − review existing information security requirement against international standards and best practices and identify deployment of security controls and safeguards to CNII;

CyberSecurity Malaysia, Level 5, Sapura@Mines, No. 7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia
E-mail: shamir@cybersecurity.my

4) Public and Private Cooperation − review and analyze the current level of coordination of cooperation and partnership arrangements between the public and private sector in mitigating attacks and cyber threats to the CNII;
5) International Engagement − analyze the available international security implementation models and determine the feasibility to implement it locally.

1.3. The Critical National Information Infrastructure

The policy is developed to cater for the protection of the CNII. Therefore, there is a need to have a definition of CNII for the country. A series of discussion sessions were conducted involving the relevant stakeholders from the ministries, academic institutions, the industry, and government agencies to decide on a definition of Malaysian CNII. As a result, the CNII of Malaysia is defined as those information infrastructures that are very important to the nation that significant disruption to which, would have severe impact on the national economic strength, image, defense and security, government capabilities to function, and public health and safety.

In addition to the definition, the CNII of Malaysia is categorized into ten (10) sectors which are:

National Defence & Security	Water
Banking & Finance	Health services
Information & Communication	Government
Energy	Emergency services
Transportation	Food & Agriculture

2. The National Cybersecurity Policy

The proposed cybersecurity policy for Malaysia was presented to the Cabinet of Ministers in 2006. The proposal was accepted for implementation and is named The National Cyber Security Policy (NCSP).

The NCSP seeks to address the cyber threat risks to the CNII of Malaysia. It recognizes the critical and highly interdependent nature of the country's information infrastructure and aims to develop and establish a comprehensive program and a series of frameworks to ensure the effectiveness of information security controls over vital assets and that the CNII are protected to a level that commensurate the risks faced.

2.1. Policy Vision

The vision of the NCSP is:

''Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well-being and wealth creation.''

This vision is in line with the need in reaching a developed nation status and aligned with the culture and values of the Malaysia. Continuous promotion and communication of the vision created short term objectives and encouraged individual entities within the CNII to focus on cybersecurity resources in a manner that is compatible and aligned with the NCSP vision.

Promoting stability means reducing risk of disruption to critical services. A secure, resilient and self reliant CNII will reduce the level of disruption to critical services and will help prevent hostile cyber attacks from outside of Malaysia. Meanwhile, promoting social well-being is about having a greater availability of services through the increased use of new technologies.

2.2. Key Policy Pillars

The NCSP has eight (8) Policy Thrust (PT) that covers the aspect of national cybersecurity, which are as follows.

2.2.1. Effective Governance

The interdependent nature of the CNII means that cybersecurity incidents can cascade to other sectors. The Malaysian Government has made significant progress in securing the CNII since the adoption of the NCSP but there are still challenges to be confronted. Initially, the Ministry of Science, Technology and Innovation Malaysia, the developer of the NCSP, took the task of implementing the policy. At that point, cybersecurity protection programs were not systematically coordinated across the government machineries resulting to confusion and misunderstanding among agencies regarding their roles and responsibilities. In the absence of coordination, ministries and agencies focus on their own missions and not on the overarching national needs.

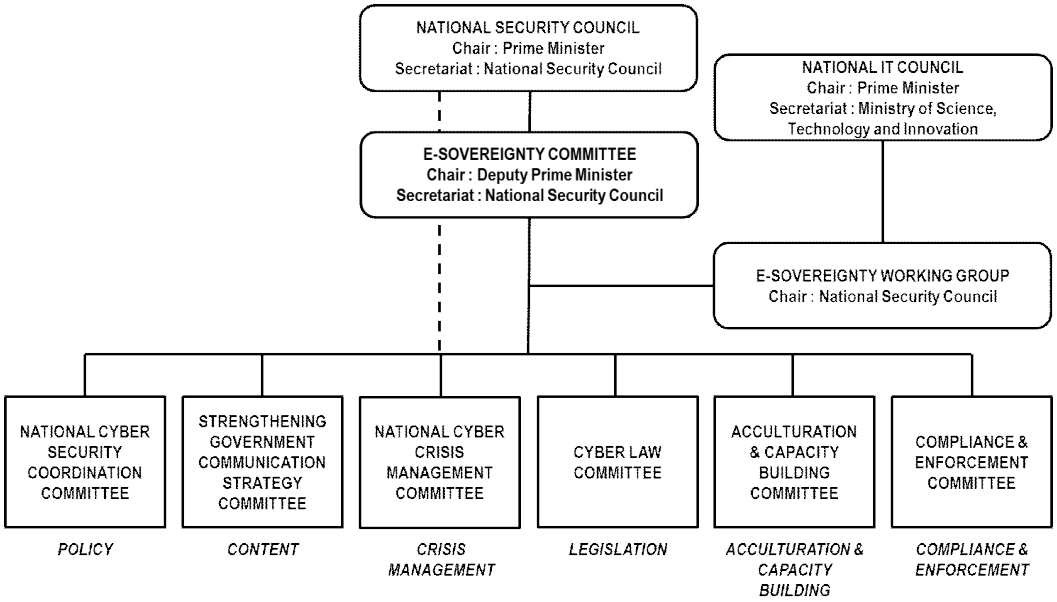
The policy identified the need for a single information security coordination body to be established. CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation, was given this task to provide a strong platform for strengthening the nation's cybersecurity efforts and improving the public and private cooperation across the CNII. To date, the agency has raised the profile of cybersecurity and continued to vigorously promote the 'culture of security' within the country.

In 2011, as cybersecurity grew in importance, the custodian of the NCSP, was transferred from the Ministry of Science, Technology and Innovation Malaysia to the National Security Council Malaysia under the Prime Minister's Department. This further facilitates the coordination in implementing the initiatives of cybersecurity across multiple ministries and agencies. However, CyberSecurity Malaysia remains as the organization implementing the policy.

The CNII organizations in Malaysia are a combination of public and private entities which are governed by their respective regulators. Therefore, under this policy thrust, there is a need for a public-private cooperation framework covering incident response, reporting structure, focal point for cybersecurity protection-related, research and development (R&D) and cybersecurity awareness efforts.

Cybersecurity effective governance for Malaysia is done by the e-sovereignty Committee under the purview of the National Security Council. Figure 1 shows the structure of the committee.

Figure 1. Malaysia e-Sovereignty Committee



2.2.2. Legislative & Regulatory Framework

The NCSP is to ensure the confidentiality, integrity and availability of information and non-repudiation of communication in accordance with its vision. It is intended to create trust and confidence within the Malaysian CNII. The legal system is important and must be adequate and adaptable to ensure the advancement in information technology benefits the people and the country, and to ensure that the CNII is securely protected from cyber attacks. Therefore, the laws and regulations are defined, and categorized to penalized cyber crimes so as to deter future malice and to provide the country with the appropriate level of compliance.

The laws and regulations must be enhanced in order for enforcement agencies to effectively detect and address problems and threats from cyber attacks and interruption to the information systems; both with preventive and corrective measures to effectively address legal challenges surrounding the information security protection. To achieve this, it is imperative for Malaysia to create an enabling environment through continuous reviews and coordination of the country's legislative and regulatory frameworks in line with global standards and approved best practices.

CyberSecurity Malaysia in 2011 conducted 'A Study on the Legal Issues of Cyber Activities in Malaysia', under the guidance of the Attorney's General Chambers, on the existing laws of Malaysia related to the cyber environment such as the Computer Crimes Act, the Communication and Multimedia Act and the Digital Signature Act. These also include some of the conventional laws that also have implication on the cyber environment such as the Penal Code, the Internal Security Act, the Sedition Act, the Defamation Act, and the Evidence Act. The outcome of the study is recommendations on improvement that need to be made to the existing laws. With the recommendations, the Attorney General's Chambers worked with the respective ministries to make the necessary amendments.

However, presently such legislative and regulatory initiatives should not only be a national agenda, but also as part of an international framework in curbing cyber threats to the global community. Crimes in cyber space transcends traditional boundaries that restrict the movement of conventional criminals. In the realm of information and communications technology, criminal action in one country can affect other countries due to the interconnectivity and interdependence of borderless networks.

2.2.3. Cybersecurity Technology Framework

The cybersecurity technology framework defined clear security controls to be implemented and enforced. Security controls such as management, technical and operational controls help to put the necessary measures in place for security implementation. In addition, the security controls applied to a particular information system shall be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a breach in security due to the loss of confidentiality, integrity, or availability.

Previously the need for equipment and systems were based on individual requirements and not based on a baseline or standards approved by the government. Thus for most cases, cybersecurity controls were determined at a later stage and had proven to be expensive and damaging to the network.

This policy thrust provides a reference point for formulating the standard cybersecurity baseline for the protection of CNII. The key objectives of formulating the standard cybersecurity baseline are to establish a standard to be used by CNII; and to ensure all procurement or in-house development of CNII cybersecurity-related products and systems comply with the security requirements of the baseline.

Cybersecurity-related products and systems encompasses a broad range of hardware, application software, security practices, security architecture and designs, physical security measures, as well as policies and procedures that protect the confidentiality, integrity, and availability of information residing within and across the CNII elements. This policy thrust defined the security controls that are needed. Security such as management, technical and operational controls provided some assurance that security measures are in place.

Base on the requirement of this thrust, it was recommended that all CNII entities of Malaysia adopt the MS ISO/IEC 27001-2007 Information Security Management System (ISMS) as a security baseline and to obtain the certification. After much deliberation, the Malaysian Government agreed to this proposal and issued an instruction in February 2010 that all Malaysian CNIIs are to be ISMS certified within three years.

Another initiative under this thrust is the establishment of the Malaysia Common Criteria Evaluation and Certification Scheme (MyCC). CyberSecurity Malaysia has become a member of the Common Criteria Recognition Arrangement (CCRA) since 2007. The CC scheme implements a security evaluation/certification program that will enable users to procure technology with greater confidence. This kind of evaluation will reduce the need for the individual CNII entities to perform their own testing. This improved competitiveness, technology deployment and decrease the risk faced by implementers of the technology.

2.2.4. Culture of Security and Capacity Building

The advancement of the wireless and broadband technologies has contributed significantly to the increasing participation of the interconnected community. As a result of this mounting interconnectivity and interdependency, information systems and networks are now exposed to a growing number and variety of threats and vulnerabilities. This raises the need for a greater awareness and understanding of cybersecurity issues and the need to develop a culture of cybersecurity, which encompasses on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within the information systems and networks.

There was a lack of cybersecurity outreach and awareness in both the public and private sectors coupled with the lack of initiatives that can drive and increase the level of cybersecurity awareness through training and education strategies across all elements of the CNII. CyberSecurity Malaysia conducted a study in 2010 titled the National Strategy for Cyber Security Acculturation and Capacity Building that focuses on the key aspect, which is the cybersecurity acculturation and capacity building that takes into consideration the interests of all parties that develop, own, provide, manage, service and use information systems and networks within the CNII.

The effort to promote a culture of security requires leadership and extensive involvement of well-planned and well-managed programs that was reduced into a systematic and strategic roadmaps and plans of action. This makes cybersecurity a concern and responsibility at all levels of government and business and for individuals who are involved in the CNII environment.

In achieving maximum success of the cybersecurity awareness and education programs, the initiatives and coordinated efforts are centralized to specialized organizations to drive and increase the level of cybersecurity awareness across all elements of the CNII. The cybersecurity acculturation programs also target the public by having plans to inculcate best practices, good habits

and behaviours, and safe use of the Internet. This includes the development of content, the approach and implementation plan of the acculturation.

The culture of security is promoted by qualified professionals from specialized organizations whom identify minimum requirements and qualifications for those who are involved in the cybersecurity knowledge transfer processes. The CyberSAFE program, which stands for Cyber Security and Awareness for Everyone (www.cybersafe.my) is a CyberSecurity Malaysia's main program in inculcating security awareness in the country. This program provides content for children, youth, parents and organizations.

This is the one thrust that gives focus on the human aspect of cybersecurity. The development of human resources is critical to the success of efforts to improve security. In order to achieve the vision of the policy, the public and private sectors must have personnel that are sufficiently and professionally trained in the technical and non-technical issues of cybersecurity.

2.2.5. Research & Development Towards Self Reliance

To effectively garner the output from research and development, the coordination of the research teams, ideas, thoughts and innovation are consolidated under the 'National R&D Roadmap for Self-reliance in Cyber Security' developed by MIMOS Berhad, another entity under the Ministry of Science, Technology and Innovation of Malaysia. The objective of the roadmap is to overcome the lack of cybersecurity coordination and prioritization at the national level, which caused the research agendas and programs not to be systematically managed. Therefore, together with another 22 organizations representing the academics, government, industry and researchers, a consortium was formed with the goal of aligning and integrating all R&D programs and projects related to cybersecurity. This is to avoid duplication of efforts and to encourage collaboration, where appropriate, between academia, industry and the government.

The R&D roadmap focuses on technologies to protect the country's CNII with the aim of achieving self-reliance in those technologies. It specifies the critical technologies that are essential for the operation of the CNII, which are areas that are deemed vital in times of peace and crisis. Determining the research areas is important to prevent uncoordinated research efforts where individual entities and research institutes focus on individual missions that do not meet the overarching national needs and priorities.

The R&D efforts are aimed at countering threats to the CNII by making improvements to the current capabilities and also by developing new ones. This is achieved by intensifying efforts to promote cybersecurity research at learning institutions and research centres to increase the size of cybersecurity research community, which will churn revolutionary ideas and world class intellectual properties. These home grown intellectual properties provide the environment for future creation and development of the original works and finally stimulate greater economic growth and entrepreneurial activities.

2.2.6. Compliance & Enforcement

Interdependencies across the CNII are complex and pervasive. For example, no telecommunications organization can operate without power, and modern financial services organizations cannot operate effectively without telecommunications. As the ten sectors of the CNII are inter linked and reliant upon each other, a weakness in one of the sectors can be translated into a weakness in all the other sectors.

The NCSP requires that cybersecurity systems across the CNII to be standardized. It was strengthened and monitored, and enforced base on international

standards. The policy also required the development of a standard cybersecurity risk assessment framework. It is therefore of vital importance that all the ten CNII sectors achieve a minimum level of cybersecurity and that this achievement is independently verified.

Therefore, there is a need for independent cybersecurity audits and other control mechanisms where the information was used to monitor compliance, set baselines and identify trends. This has assisted in identifying the CNII sectors that need help in meeting the security baseline. For this, a Working Group (WG) consisting of members from multiple ministries and CNII organizations along with CyberSecurity Malaysia, develop a risk assessment framework for the CNII to use in identifying risk within their respective IT systems. This has helped the entities to understand their own risk profile by using similar, acceptable and comparable techniques to identify risk. The uniformity in using the framework allowed the identification of trends, strength and weaknesses. Apart from allowing the identification of critical systems that need to be secured, it also provides assistance, focus resources and drive the research and development initiatives.

The Government of Malaysia has imposed the requirement for all CNII organizations to be ISO/IEC 27001 Information Security Management System (ISMS) certified. The National Security Council of Malaysia has identified about 200 of the country's CNII and spearheads the task of ensuring these organizations get the required certification. The ISO/IEC 27001 ISMS is the cybersecurity baseline for the CNII Malaysia.

The Chief Government Security Office under the Prime Minister's Department of Malaysia has an Inspectorate Team, and together with CyberSecurity Malaysia conduct periodic security audit on the country's vital points which covers the CNII sectors. This is to ensure that the security requirement dictated by NCSP is fulfilled and maintained.

2.2.7. Cybersecurity Emergency Readiness

The cybersecurity incident response, warning and alert systems are critical tools in combating cyber attacks. Although is it difficult to establish with any accuracy the actual loss resulting from these attacks, the trend shows that such attacks are increasing in frequency, sophistication and scale. Therefore, vigilant monitoring and effective incident response is very important.

During the initial stage of implementing the NCSP, effective cybersecurity monitoring is not prevalent among the CNII entities. In addition to incident response and monitoring, the absence of business continuity management was seen as another critical factor hindering the country towards having a resilient and secure CNII.

The Computer Emergency Response Teams (CERT) or the Computer Security Incident Response Team (CSIRT) is an instrumental set up in mitigating cyber threats and incidents. There are a few CERTs in Malaysia but the two prominent ones are the Government CERT (GCERT) and the Malaysian CERT (MyCERT). The GCERT is hosted by the Malaysian Administrative Modernisation and Management Planning Unit of the Prime Minister's Department, and having the public sector as its jurisdiction. Meanwhile, MyCERT is hosted by CyberSecurity Malaysia having jurisdiction over the country and is consider the national CERT.

Previously the CERT's operate effectively within their own sectors, and it was found that there was a lack of coordination between CERTs due to their defined jurisdiction and this resulted in less information sharing and less effective incident response. Therefore, the lack of coordination was improved to ensure effective coordination, standardization and consistency in order to address national cyber threats and attacks, by strengthening the cooperation between CERTs and relevant parties. Proper mechanisms were identified and put in place,

and enforced for effective national cyber incident reporting.

The National Security Council of Malaysia has developed the National Cyber Crisis Management Plan (NCCMP) outlining national strategies in mitigating and responding to cyber incidents and attacks emphasising on the public and private collaboration and coordination. Tied to this plan are the national cyber drills co-organized annually by the National Security Council and CyberSecurity Malaysia. The main objective of these drills is to test the procedures and processes stated in the NCCMP. Through these drills, all shortcomings are identified and rectified to ensure continuous improvement to the NCCMP. The drills also observe the reactions of the participating CNIIs and the flow of information. It is critical to ensure that all cybersecurity related information gathered be disseminated to all the relevant CNII sectors as and when needed. Therefore, vulnerability advisories and threat warnings can and should reach everyone in a timely and efficient manner.

Additional to the drills, CNII organizations were strongly requested to develop document on comprehensive business continuity and disaster recovery plans as part of an effective business continuity management strategy. For the continuous efficiency of emergency readiness, periodic vulnerability assessments programs was also conducted to identify security flaws and recommended remedial actions.

2.2.8. International Cooperation

The global community has recognized that cyber threats are not affected by the geographical factors and the physical boundaries of countries. Therefore there is a serious need for international collaboration among countries for information security initiatives such as sharing information, research, best practices, overcoming challenges and formulating international policy. Under this policy thrust, Malaysia, through CyberSecurity Malaysia, maintain active participation on relevant international information security bodies and panels, and also in all relevant international information security events, conferences and forums. In addition, CyberSecurity Malaysia hosted international information security events to enhance the strategic position of the country.

CyberSecurity Malaysia is one of the co-founding members of the Asia Pacific Computer Emergency Response Team (APCERT) and has held the Chair and Secretariat position full term. Now the agency, as a member of the APCERT Steering Committee, holds the Deputy Chair position. On another major international initiative, CyberSecurity Malaysia spearhead the formation of the Organization of the Islamic Cooperation Computer Emergency Response Team (OIC-CERT)[2] holding the Chair and Secretariat position for full term. Just like the APCERT, the OIC-CERT is a collaborative platform of CERTs in mitigating cyber threats. However, while APCERT covers the Asia Pacific region and having members from 20 economies, the OIC-CERT have members from 21 Organization of the Islamic Cooperation (OIC) countries. Presently, CyberSecurity Malaysia has been appointed as the Permanent Secretariat of the OIC-CERT.

International cooperation in information security has strengthened the nation's capability, improves international recognition, highlights the existing achievements, and planned future activities. It has improved competitive advantage and strategic position, direction and initiatives in securing the CNII.

In addition to the mentioned multilateral engagement, Malaysia participated in various global information security platforms such as the Forum of Incident Response and Security Teams (FIRST), Anti-phishing Working Group (APWG), International Telecommunication Union (ITU), Asia-Pacific Economic

2 APCERT <www.apcert.org> , OIC-CERT <www.oic-cert.org>

Cooperation Telecommunications and Information (APEC TEL)[3]. The participation in international information security events, conferences and forums has enable Malaysia to increase the overall knowledge on information security, share best practices and identify common challenges as well as positioning Malaysia to becoming a leader in the field of information security. These events are excellent forums for knowledge sharing and helped increase the capacity of Malaysia's information security professionals.

The hosting of an annual international information security conference has help position Malaysia at the forefront of information security and establishes a reputation of thought leadership in this field. CyberSecurity Malaysia hosted the CyberSecurity Malaysia Award, Conference and Exhibition (CSM-ACE)[4].

This annual international conference hosted locally has increased the reputation, skills and capacity of Malaysia's own information security professionals. This event is also used to showcase home grown organizations and products giving the local information security industry an added advantage.

Increased international cooperation, activity and visibility by Malaysia in the field of information security have provided rapid expansion of local technologies in the security industry.

2.2.9. Lesson Learned

With the dependence on IT infrastructure resulting as the increase of cyber incidents, it is a right move for Malaysia to develop a national cybersecurity policy with a focus on enhancing the security, resilience and self-reliance of the country's CNII to promote stability, social well-being and wealth creation.

In implementing the policy, the keys to success were;

- Effective governance and coordination with the establishment of a single coordination centre which in this case is CyberSecurity Malaysia, which has created organization clarity and accountability;
- Improving the public private cooperation;
- Improving the information security skills and capacity;
- Enhancing the existing research & development initiatives toward self-reliance;
- Mapping out the emergency readiness;
- Dictating the program for compliance and assurance across the whole of CNII; and
- Reaching out to international partners.

References

Ministry of Science, Technology and Innovation, Malaysia, "National Cyber Security Policy: The Way Forward," Federal Government Administrative Centre. July 2006.

UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space" Office of Public Sector Information, Information Policy Team, June 2009.

United State, Executive Office of the President "Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure," United State, Executive Office of the President, May 2009.

Ministry of Science, Technology and Innovation. "National R&D Roadmap For Self-Reliance in Cyber Security Technologies." Unpublished.

ISACA and the IT Governance Institute. ISACA Overview. Retrieved April12, 2011. From <http://www.isaca.org/About-ISACA/History/Pages/default.aspx>

Hashim, M.S; "Malaysia's National Cyber Security Policy – The Country's Cyber Defence Initiatives'; IEEE; London, UK; June 2011

(ISC)². About (ISC)². Retrieved April 12, 2011. From <https://www.isc2.org/aboutus/default.aspx>

EC-Council. About us. Retrieved April 12, 2011. From <http://www.eccouncil.org/about_us.aspx>

3 FIRST <www.first.org>, APWG <www.antiphishing.org>, ITU <www.itu.int>, APEC TEL <www.apectelwg.org>

4 CSM-ACE <www.csm-ace.my>