MOSTI

National Cyber Security

National Security Vision

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

Background

The alarming rise of premeditated attacks with potentially catastrophic effects to interdependent networks and information systems across the globe has demanded that significant attention is paid to critical information infrastructure protection initiatives.

For many years Governments have been protecting strategically critical infrastructures, however in recent times the information revolution has transformed all areas of life. The way business is transacted, government operates, and national defence is conducted has changed. These activities now rely on an interdependent network of information technology infrastructures and this increases our risk to a wide range of new vulnerabilities and threats to the nation's critical infrastructures. These new cyber threats are in many ways significantly different from the more traditional risks that Governments have been used to addressing. Exploiting security flaws appears now to be far easier, less expensive and more anonymous than ever before.

The increasing pervasiveness, connectivity and globalization of information technology coupled with the rapidly changing, dynamic nature of cyber threats and our commitment to the use of ICT for socio-economic development brings about the critical need to protect the critical information infrastructures to provide greater control. This means that Governments, including the Malaysian government, must adopt an integrated approach to protect these infrastructures from cyber threats.

The National Cyber Security Policy

This National Cyber Security Policy has been designed to facilitate Malaysia's move towards a knowledge-based economy (K-economy). The Policy was formulated based on a National Cyber Security Framework that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

The National Cyber Security Policy seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are:
National Defence and Security

- **Banking and Finance**
- **Information and Communications**
- **Energy**
- **Transportation**
- **Water**
- **Health Services**
- **Government**
- **Emergency services**
- **Food and Agriculture**

The Policy recognizes 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. It has been developed to ensure that the CNII are protected to a level that commensurate the risks faced.

The Eight Policy Thrusts

THRUST 1: *Effective Governance*
Centralise coordination of national cyber security initiatives
Promote effective cooperation between public and private sectors
Establish formal and encourage informal information sharing exchanges

THRUST 2: *Legislative & Regulatory Framework*
Review and enhance Malaysia's cyber laws to address the dynamic nature of cyber security threats
Establish progressive capacity building programmes for national law enforcement agencies
Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions

THRUST 3: *Cyber Security Technology Framework*
Develop a national cyber security technology framework that specifies cyber security requirement controls and baselines for CNII elements
Implement an evaluation/certification programme for cyber security product and systems

THRUST 4: Culture of security and Capacity Building
Develop, foster and maintain a national culture of security
Standardise and coordinate cyber security awareness and education programmes across all elements of the CNII
Establish an effective mechanism for cyber security knowledge dissemination at the national level
Identify minimum requirements and qualifications for information security professionals

THRUST 5: *Research & Development Towards Self-Reliance*
Formalise the coordination and prioritization of cyber security research and development activities
Enlarge and strengthen the cyber security research community
Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development
Nurture the growth of cyber security industry

THRUST 6: *Compliance and Enforcement*
Standardise cyber security systems across all elements of the CNII
Strengthen tho monitoring and enforcement of standards
Develop a standard cyber security risk assessment framework

THRUST 7: *Cyber Security Emergency Readiness*
Strengthen the national computer emergency response teams (CERTs)
Develop effective cyber security incident reporting mechanisms
Encourage all elements of the CNII to monitor cyber security events
Develop a standard business continuity management framework
Disseminate vulnerability advisories and threat warnings in atimely manner
Encourage all elements of the CNII to perform periodic vulnerability assessment programmes

THRUST 8: *International Cooperation*
Encourage active participation in all relevant international cyber security bodies, panels and multi-national agencies
Promote active participation in all relevant international cyber security by hosting an annual international cyber security conference

Implementation Approach

Phase I (0 - 1 year)	**Addressing Immediate Concerns**	- Stop-gap measures to address fundamental vulnerabilities to the cyber security of the CNII - Creating a centralize platform for security mechanism - Raising awareness of cyber security and its implications
Phase II (0 - 3 years)	**Building the Infrastructure**	- Setting-up the necessary systems, process, standards and institutional arrangements (mechanisms) - Building capacity amongst researches and information security professionals
Phase III (0 - 5 years and beyond)	**Developing Self-Reliance**	- Developing self-reliance in terms of technology as well as professionals - Monitoring the mechanisms for compliance - Evaluating and improving the mechanisms - Creating the culture of cyber security

The successful implementation of the eight policy thrust as contained within the National Cyber Security relies on a coordinated and focused approach. The key feature of the Policy implementation is:

Establishment Of The Malaysia Cyber Security Centre

The Malaysia Cyber Security Centre is envisioned to become a one-stop coordination centre for national cyber security initiatives by adopting a coordinated and focused approach, with the key objective of strengthening the country's cyber security arena.
The centre will be under the purview of the Ministry of Science, Technology and Innovation (MOSTI), and overseen by the National IT Council for policy direction and the National Security Council in times of national crisis.

The key functions of the Malaysia Cyber Security Center are :

- **National Cyber Security Policy Implementation**
  Defines, communicates and updates (when necessary) the national cyber security programmes to all the CNII.

- **National Coordination**
  Closely coordinates cyber security initiatives of various key Agencies and organisations in Malaysia.

- **Outreach**
  Promote and facilities formal and informal mechanism for information sharing across the CNII. This includes promoting cyber security awareness, training and education programmes to grow the competency of information security professionals and the industry as a whole.

- **Compliance Monitoring**
  Facilities the monitoring of compliance to cyber security policies and standards across the CNII.

- **Risk Assessment**
  Assesses and identifies cyber security threats exploiting vulnerabilities and risks across the CNII.

Conclusion

Today's unrelenting march towards an IT centric infrastructure with increasingly complex interdependencies, increasingly frequent cyber attacks and dynamic risk profile has required governments to review traditional protection mechanisms. 21st century infrastructure protection programmes will need to consider a host of virtual as well as physical threats.

Key to the success of any protection programme is effective governance and coordination. The National Cyber Security Policy focuses particular attention upon this area. The establishment of a single coordinating body will help tp provide additional levels of organization, clarity and accountability. It will enhance the operations of current organisations who will continue to perform their duties and enhance the security of the CNII.

Alongside clear and effective governance, the National Cyber Security Policy provides mechanisms for improving the trust and cooperation between the public and private sectors, improving cyber security skills and capacity, and focuses on enhancing existing skills and capacity, and focuses on enhancing research and development initiatives and practices with the aim towards self-reliance. It also maps out emergency readiness initiatives and dictates a programme of compliance and assurance across the whole of the CNII

The National Cyber Security Policy also reaches out to Malaysia's international partners and describes methods whereby Malaysia can share cyber security knowledge with the region and the wider world. It propels Malaysia towards greater international recognition in this field.

Taken as a whole, the National Cyber Security Policy aims to improve trust and cooperation in the CNII both at home and abroad, for the benefit of the people of Malaysia.

Prepared by:

Ministry of Science, Technology And Innovation
ICT Policy Division.
Level 5, Block C5,
Federal Government Adminstrative Centre,
62662 Putrajaya
MALAYSIA.
Tel: 603-88858000
www.mosti.gov.my