Malaysia’s Approach to Network Security

Bistamam Siru Abdul Rahman,
General Manager,
Industry Development Division,
Malaysian Communications and Multimedia Commission

Background

- MCMC is a statutory body established under the Malaysian Communications and Multimedia Commission Act 1998 to regulate and nurture the communications and multimedia industry in Malaysia in accordance with the national policy objectives set out in the Communications and Multimedia Act 1998 (CMA).
- The MCMC is also charged with overseeing the new regulatory framework for the converging industries of telecommunications, broadcast and online activities.
- The 10th National Policy Objective, as stated in the CMA, requires the Commission to ensure information security and the integrity and reliability of the network for the country

Laws and Policies

S. 3 (2) (j) CMA
"to ensure information security and network reliability and integrity

Communications and Multimedia Act 1998 (CMA)

Computer Crimes Act 1997

Digital Signature Act 1998

Under the CMA, the Commission is entrusted to ensure information security and the reliability and integrity of the network.

Legal issues relating to network security are addressed in the Communications and Multimedia Act and the Computer Crimes Act 1998. For example, fraudulent use of network, improper use of network facilities/services and interception of communications are addressed in the CMA. Under the Computer Crimes Act, acts such as unauthorized access to computer material and with intent to commit or facilitate commission of further offence, unauthorized modification of contents of any computer and wrongful communication is addressed.

Present Approach

Public

Private

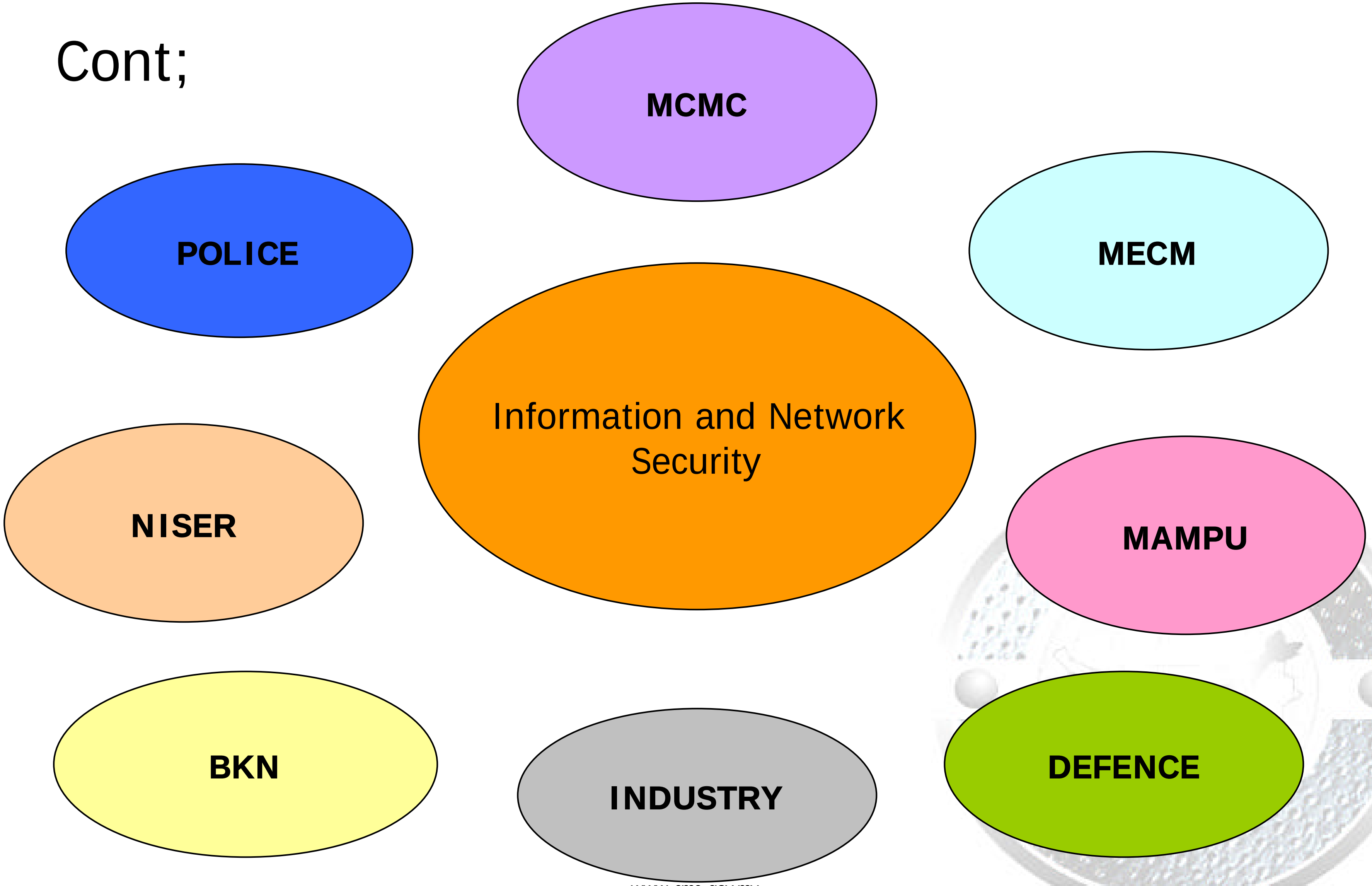
Presently, matters relating to information and network security in the public sector is under the administration of the **Malaysian Administrative Modernization and Management Planning Unit (MAMPU)** Within MAMPU, there is the ICT Security Division. They recently launched the Malaysian Public Sector Management Of Information & Communications Technology Security Handbook (MyMIS) They also operate the G-CERT. However, MAMPU does not have any enforcement powers.

MCMC
CMA

The Police
CCA
CMA

The National IT Council gave birth to NISER to address e-security Issues of the nation and as to act as Malaysia's CERT. NISER or the "National ICT Security and Emergency Response Center" offers research in vulnerability detection, intrusion detection and computer forensic technology. They offer their services to private and public entities. Like MAMPU's ICT Security Division, they do not Have any enforcement powers.

Cont;



MCMC

POLICE

MECM

Information and Network Security

NISER

MAMPU

BKN

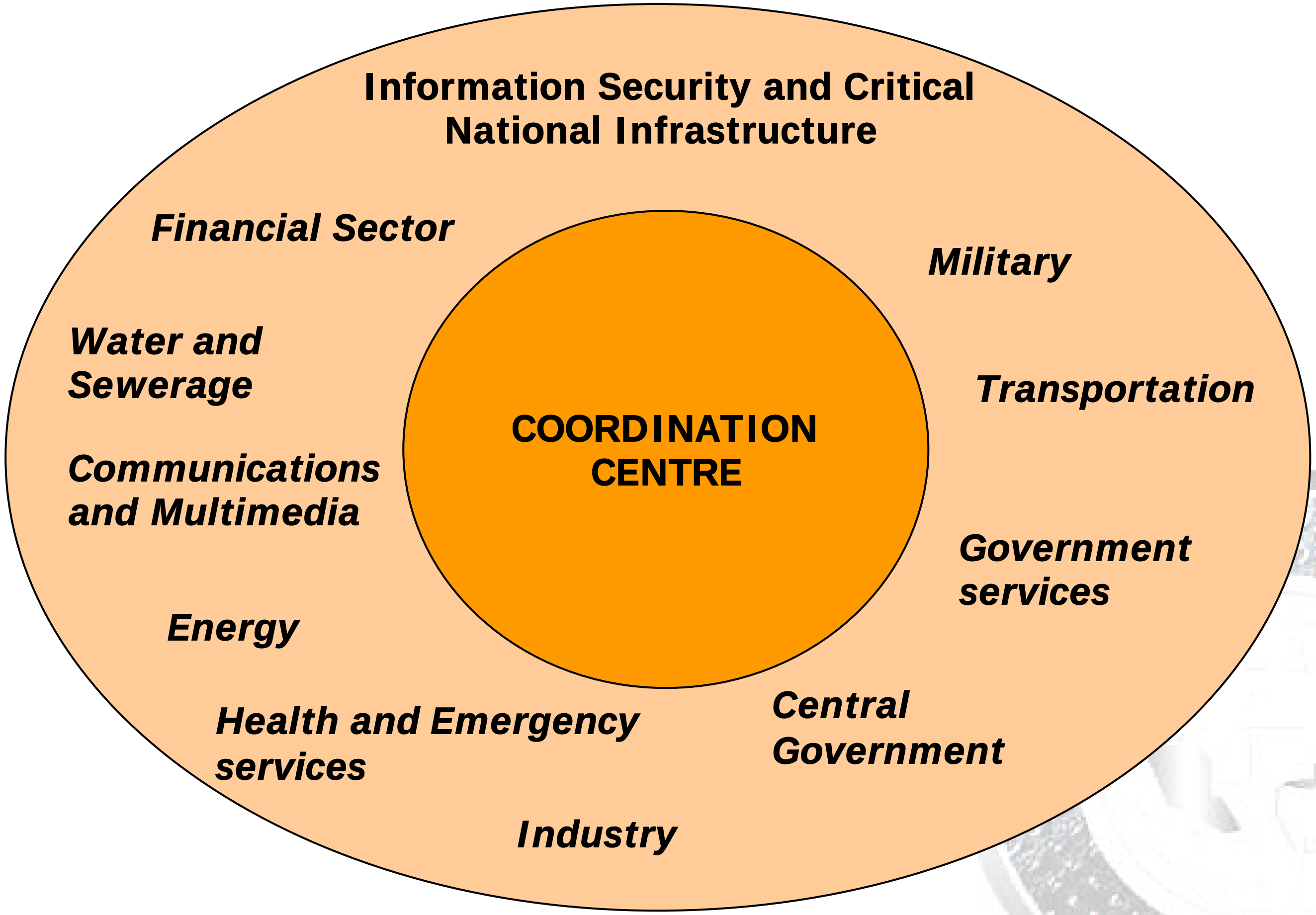
INDUSTRY

DEFENCE

Issues (from present approach)

a) Coordination
b) Awareness
c) Implementation of policies
d) Information-sharing

Future Plans



Information Security and Critical National Infrastructure

COORDINATION CENTRE

Financial Sector

Military

Water and Sewerage

Transportation

Communications and Multimedia

Government services

Energy

Central Government

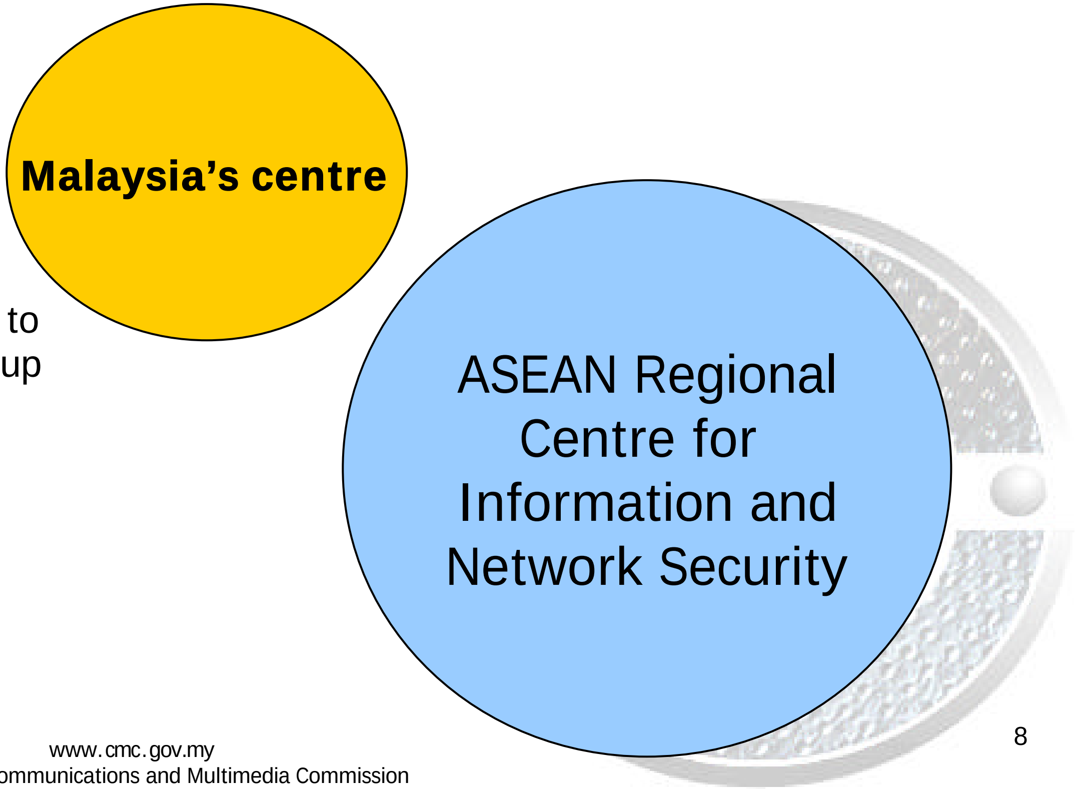
Health and Emergency services

Industry

The Way Forward

Setting up of a centralized body that will act as a stop agency for all, private and public bodies.

Malaysia will host a workshop on Information/Network Security and the Protection of Critical National Infrastructure in June. We have invited 6 organizations from Japan, S.Korea, Australia, New Zealand, UK and Canada to KL for them to share their experiences. It is hope Malaysia would be able to learn as much as possible to help us in setting up our local centralized body. Apart from the local participants, Malaysia has also extended invitations to other ASEAN countries to participate in order for ASEAN to also plan a regional centre of some sort for the benefit of ASEAN.



Malaysia's centre

ASEAN Regional Centre for Information and Network Security

Pointers for Slide # 2

Briefly explains what MCMC is and its relation/relevance to Information and Network Security. MCMC is also the Regulatory Authority for all of the ISPs operating in Malaysia.

Apart from regulating and nurturing the communication and Multimedia industry in accordance with the CMA, the MCMC is also the “Controller” for the Certification Authorities under the Digital Signature Act 1998.

The CMA is the only piece of regulation or law that identifies information security and the reliability and integrity of the network as a National Policy Objective. However, it does not elaborate on the process. Effectively, it is up to the organizations to fall into place.

Pointers for Slide # 3

In approaching Network Security, the participants may want to know what are the laws and policies in Malaysia that governs network security.

In Malaysia’s instance, the main statutes is the CMA and the Computer Crimes Act 1997. Within the two statutes, there are legal issues identified such as fraudulent use of network, improper use of network facilities/services and interception of communications are described in the CMA. In the CCA, acts such as unauthorized access, modification of contents and wrongful communication is addressed

Pointers for Slide # 4

Presently, approaches to network security has a "jurisdiction" flavor to it. Security issues in the public sector is administered by MAMPU (Malaysian Administrative Modernization and Management Planning Unit) Within MAMPU is the ICT Security Division. They also operate a CERT for the Government. They had also recently launched The Malaysian Public sector Management of Information and Communications Technology Security Handbook (myMIS). The handbook is a set of guidelines concerning compliance and adherence to best practices and measures leading to information and network security. A copy is available online at http://www.mampu.gov.my/ICT/MyMIS/MyMIS.htm All of the public sectors are asked to comply and adhere to the handbook while the private sector is encouraged. However, the ICT Security Division do not have any enforcement powers to enforce compliance.

Cont;

Whilst security issues within the public sector is “administered” by MAMPU, the National IT Council (NITC) was of the opinion that there was a need for a body that will be able to assist the private sector in dealing with security issues. Thus the NITC gave birth to the National ICT Security and Emergency Response Centre (NISER). NISER is also Malaysia’s CERT or MyCERT. They offer their services in respect of vulnerability detection, intrusion detection and forensic technology.

Presently, they offer their services to both public and private sectors. Like MAMPU, NISER do not have any enforcement powers.

Cont;

In this instance, only MCMC and the Police have any enforcement powers in matters relating to Information and Network Security. The MCMC is the body entrusted to implement and promote the Government's national policy objectives under the CMA. It has enforcement powers in relation to offences relating to network security in the CMA.

The Police has "sweeping" enforcement powers. They have jurisdiction over the CMA and also the CCA.

All complaints relating to network security matters will be passed to either the MCMC or/and the Police.

Pointers for Slide # 5

As it is, organizations in Malaysia lack the coordination process. This is a point of concern as it slows the development with regards to implementation of policies, information-sharing and creating awareness.

All of the organizations are “loosely” bound together and this is a disadvantage when the country needs to “react” to certain issues.

Pointers for Slide # 6

Presently, looking at the current situation, there are 4 main concerns that need to be tackled.

There is a basic lack of *coordination*. This is a concern when the country is to react or put into place, proactive measures. The lack of coordination results in *poor sharing of information*, *ineffective implementation of policies* and *a need for awareness program*.

However so, the MCMC is initiating continuous awareness program on security to consumers alike. The MCMC is also undertaking a network security audit for all of the ISPs

Pointers for Slide # 7

Future Plans:

There is an urgent need for bodies, sectors and stakeholders of the country’s Critical National Infrastructure to identify a centralized body which will coordinate and facilitate the issues concerning Information and Network Security, also the Protection of Critical Infrastructure.

The relevant bodies in Malaysia have met last March 8 to discuss the setting up of that “centralized body”. That centralized body will then function as Malaysia’s national body which will bind all of the critical sectors of Information and Network Security into a group to facilitate coordination process, dissemination of information and also as the nation’s centre of excellence in the field of “information and network security”.

Pointers for Slide # 8

To jump start the initiative to set Malaysia's own local central body for Information and Network Security, and the Protection of Critical Infrastructure, we have initiated a workshop where we have invited 6 organizations representing Japan, S.Korea, UK, Canada, New Zealand and Australia who are responsible for Information and Network Security, and the Protection of Critical Infrastructure in their own countries. The workshop will be from 10-11 June 2002.

Malaysia has also invited all ASEAN countries to participate in the workshop.

During the workshop, Malaysia hopes to learn as much as possible on the workings of each centre, how they operate, the lessons learnt and their experiences in dealing with matters such as jurisdiction,

Cont;

coordination and so forth.

We have also invited ASEAN members to participate. This is because During the last ASEAN Telecommunications Minister meeting in KL in July 2001, Malaysia mooted the idea of having a regional coordination centre/body for ASEAN on Information and Network Security.

This is to allow member countries of ASEAN to interact, exchange and share information and train its members on matters relating to information and network security.

Malaysia was chosen to spearhead this initiative for ASEAN and the workshop that we will be hosting in June 2002 will be the catalyst towards a new approach on network security, for Malaysia and also for ASEAN.