SKMM Network Security Centre (SNSC)
-Protecting the Communication Front

ITU Regional Cybersecurity Forum for Asia-Pacific

23rd – 25th September 2009

Background

- Population -28.3 million
- Broadband penetration – 24.8%
- Mobile /Cellular penetration-100.8%
- Broadband technologies subscriptions

Year	Quarter	ADSL	SDSL	Satellite	Others	Mobile	Others
		FIXED ('000)				Wireless ('000)	
2009	1	1,337.7	8.2	5.1	5.6	474.9	61.2
	2	1,378.3	8.3	5.1	6.0	631.3	86.9

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

-National Cyber Security Policy

The Need

- 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.
  - Information revolution has changed all areas
  - Daily activities rely on interdependent network of technology infrastructure
  - Exploiting security flaws appears to be far easier, less expensive and more anonymous than ever before

NCSP

- Designed to facilitate Malaysia's move towards a knowledge-based economy (K-economy).
- Formulated based on a National Cyber Security Framework that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

NCSP Objective

- To address the risks to the Critical National Information Infrastructure (CNII)
- Recognizes the critical and highly interdependent nature of the CNII
- 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
- To ensure that the CNII are protected to a level that commensurate the risks faced.

CNII Sectors

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

The Eight Policy Thrusts

- THRUST 1: Effective Governance
- THRUST 2: Legislative & Regulatory Framework
- THRUST 3: Cyber Security Technology Framework
- THRUST 4: Culture of security and Capacity Building
- THRUST 5: Research & Development Towards Self-Reliance
- THRUST 6: Compliance and Enforcement
- THRUST 7: Cyber Security Emergency Readiness
- THRUST 8: International Cooperation

SKMM Network Security Centre (SNSC)

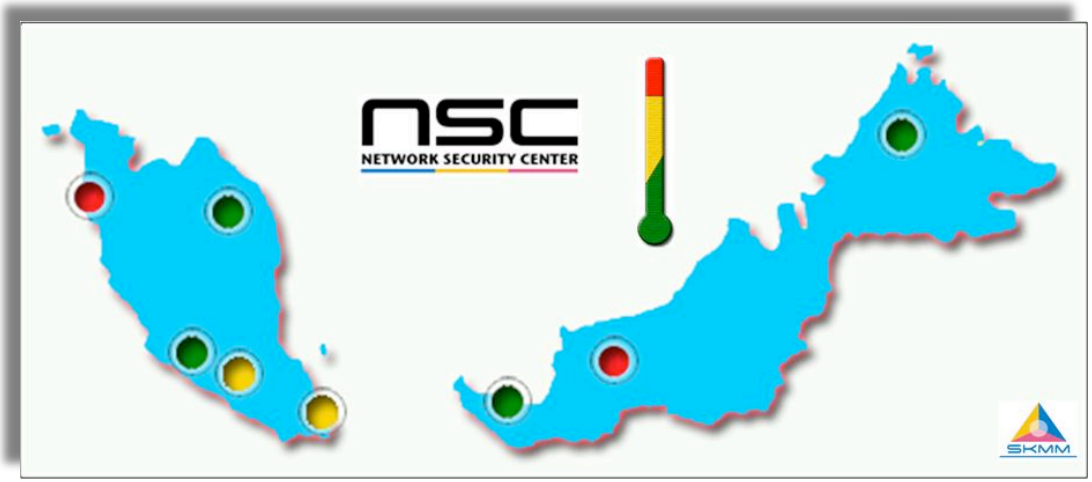
- A cyber security monitoring centre initiated by the Malaysian Communication and Multimedia Commission (SKMM)
- Inline with the NCSP and the 10th national policy objective of the Communication and Multimedia Act (CMA)
- To provide for supervision, monitoring and to provide for preventive early warning measures to all relevant stakeholders in Malaysia

Current Scenario in Malaysia

- ISPs are the gateways for Malaysian Internet
- There is a need to know what is the status of the Malaysian Network
- SNSC , the only national level monitoring that designed to analyze and react based on the real time sampling of the Malaysian Internet traffic.

SNSC-Internet Security Thermometer

- Serves as the national Internet network thermometer to provide overall understanding of macro cyber threat level with the involvement and cooperation of both public and private sectors.



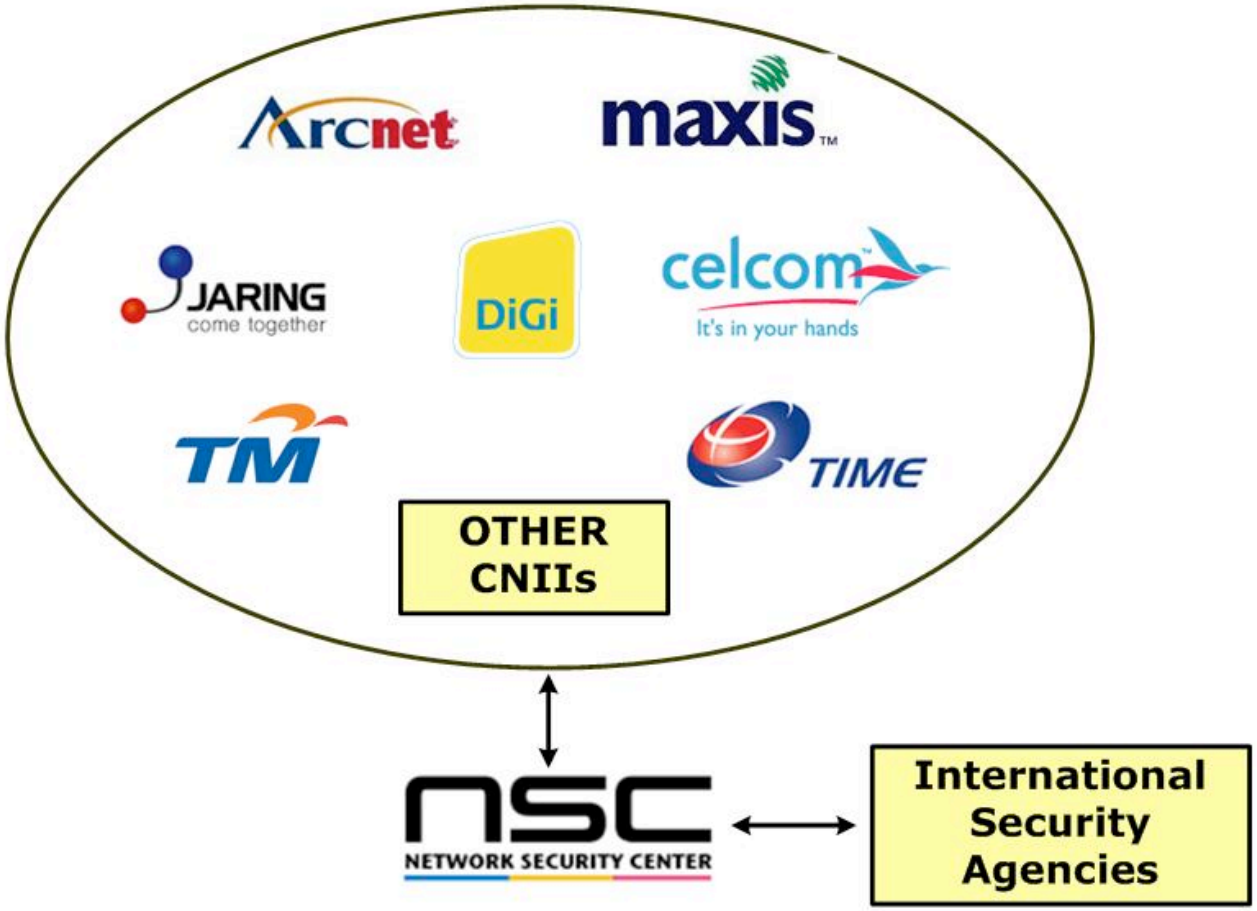
Mission Statement

- To reduce the probability of cyber security risks from crystallizing by **disseminating early warnings** and share information among the stakeholders thus minimizing any adverse impact to the overall Malaysian communications and multimedia industry

Main activities

- Network Threat Monitoring and Management
  - Recommends threat level for Malaysian network
  - Monitor the criticality of threats coming into the local network
- Incident Management, Network Forensic, Recovery and Advisory
  - Analyze network – forensic
  - Provide early warning, handling, advisory and coordination during incidences
- Vulnerability Management
  - Network auditing activities to ensure continuous security

The Bigger Picture



Detect & Protect

Armed with seven (7) Databases based on world wide references which are updated real time

- Threat Mgt. Database
- Vulnerability Database
- Malware Database
- Port Database
- Pattern Database
- Incident Analysis Database
- Early Warning Database

Way Forward

- Provide wider coverage by adding more sensors in other parts of the Malaysian Network
- Increase collaboration works with other local and international cyber security agencies, i.e. IMPACT,ACMA and etc
- Complement SNSC with Honey-Net network feeds to improve visibility on malware distributions.
- Support National Cyber Security Coordination Centre proposed under NCSP (National Security Council Purview)

Thank You

Saravanan Kulanthaivelu (saravanan@cmc.gov.my)
Security, Trust and Governance Department,
Monitoring and Enforcement Division,
Malaysian Communications and Multimedia Commission
63000 Cyberjaya, Selangor Darul Ehsan
MALAYSIA
Tel: 603.8688 8180
Fax: 603.8688 1003