MALAYSIA'S NATIONAL CYBER SECURITY POLICY
Towards an Integrated Approach for Cyber Security and Critical Information Infrastructure Protection (CIIP)

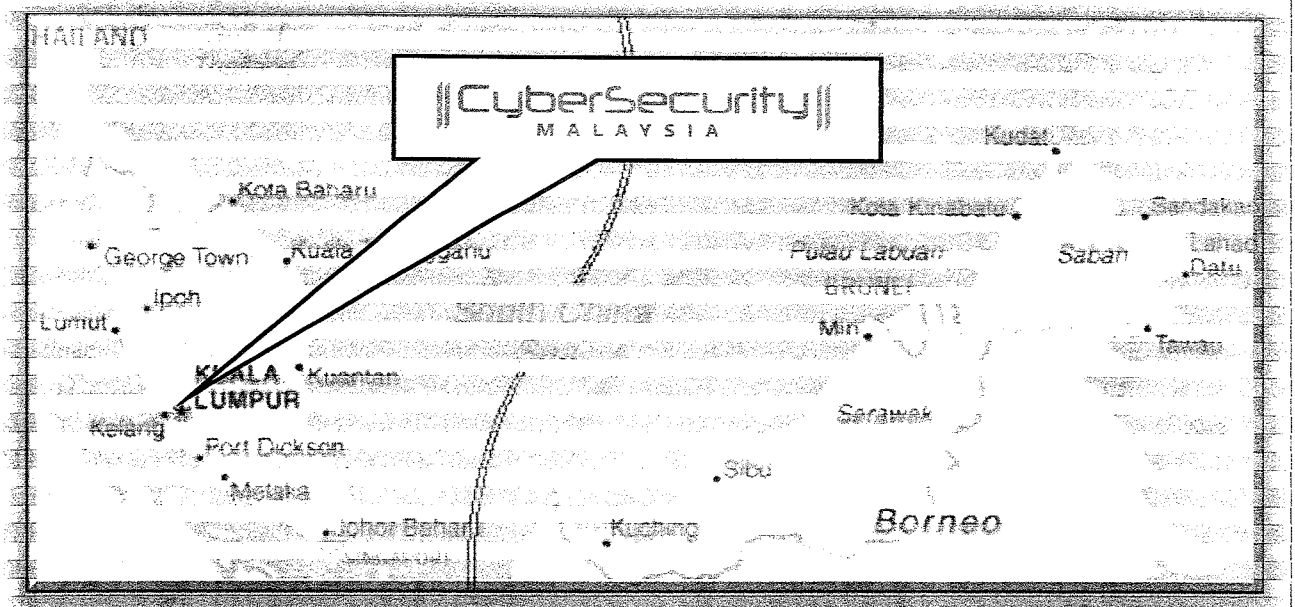
FAZLAN ABDULLAH
POLICY IMPLEMENTATION COORDINATION
CyberSecurity Malaysia
An agency under the Ministry of Science, Technology & Innovation
fazlan@cybersecurity.my

18 November 2009

CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

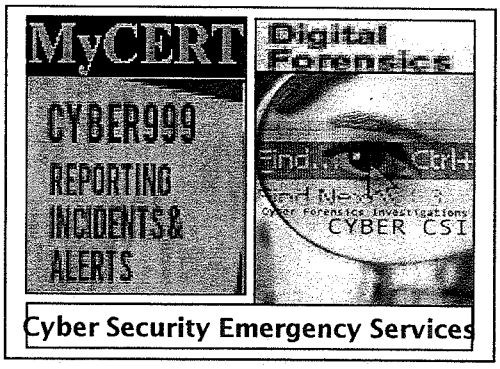
THE BRAND LAUREATE
CyberSecurity Malaysia
Best in Corporate Branding
Internet Security

Securing Our Cyberspace

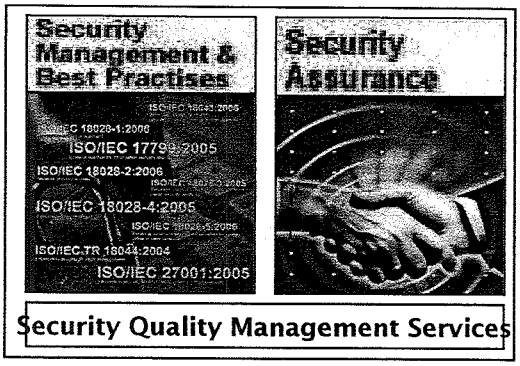


- **An agency under the Ministry of Science, Technology and Innovation of Malaysia**
- **Started operations in year 1997 and funded by the Malaysian Government**
- **We are the co-secretariat to the Malaysia's National Cyber Security Policy, together with the Ministry of Science, Technology and Innovation of Malaysia.**

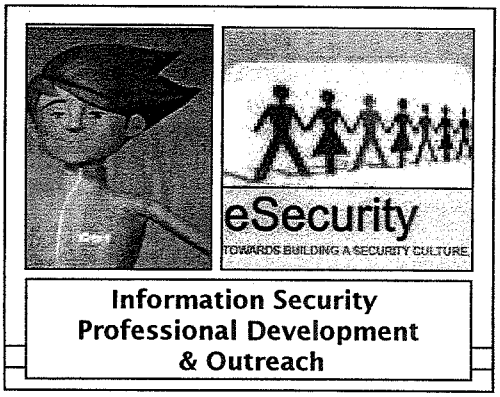
CyberSecurity Malaysia
Core Services



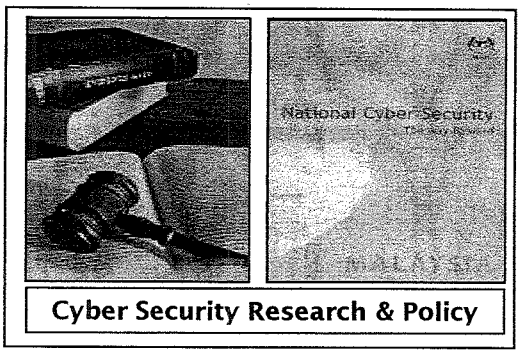
Cyber Security Emergency Services



Security Quality Management Services



Information Security
Professional Development
& Outreach



Cyber Security Research & Policy

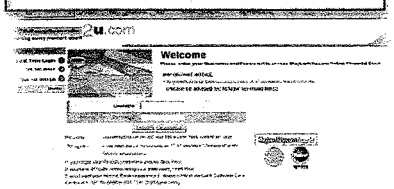
CYBER THREATS
- Malaysia

Technology Related Threats

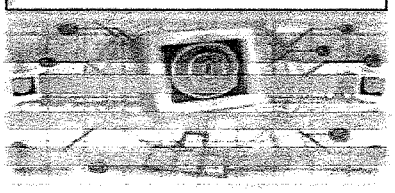
Hack Threat

Intrusion

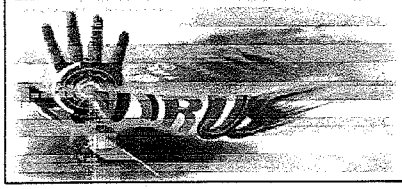
Fraud



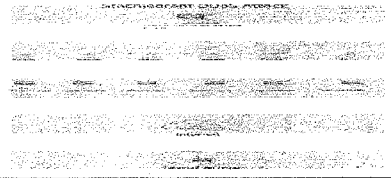
Harassment



Malicious Code

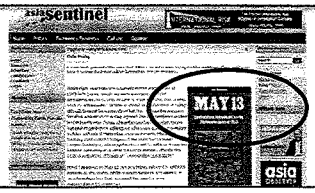


Denial of Service Attack



Cyber Content Related Threats

Threats to National Security



Sedition / Defamation

Online Porn

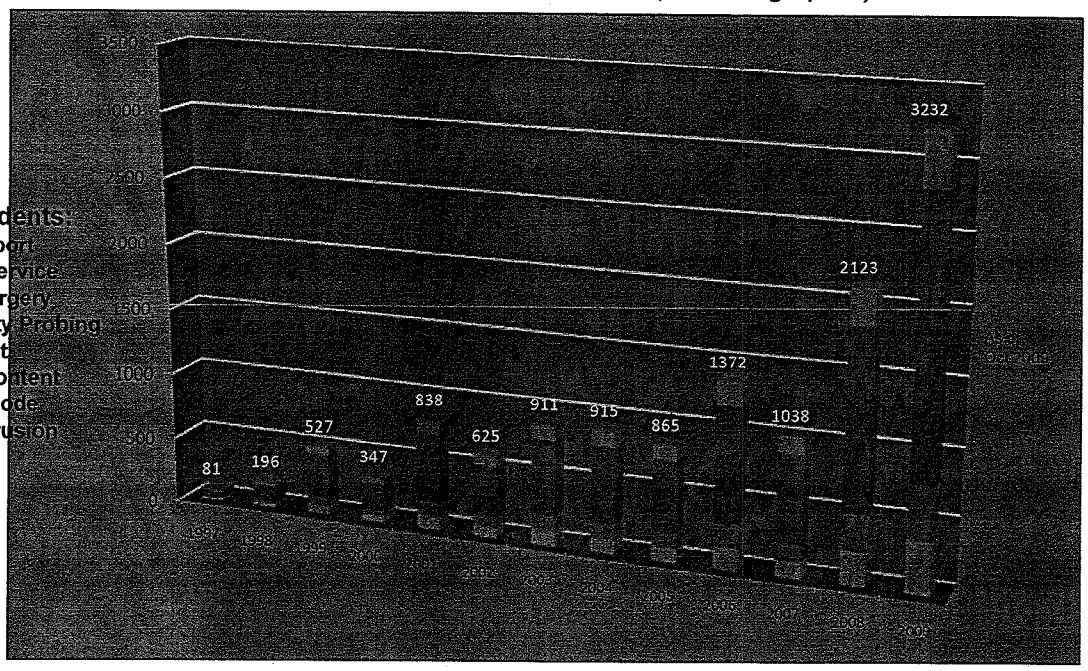
Hate Speech

Securing Our Cyberspace

CYBER SECURITY INCIDENTS - MyCERT

CyberSecurity MALAYSIA

- A total of 12,982 security incidents were referred since 1997 (excluding spam)

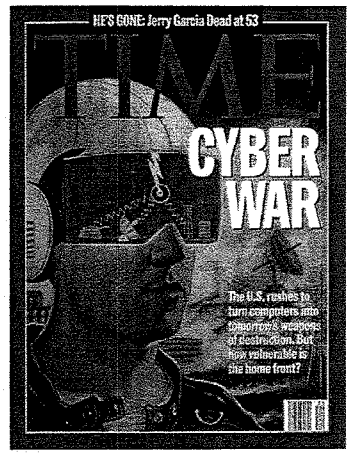


Type of incidents:
- Drones Report
- Denial of Service
- Fraud & Forgery
- Vulnerability Probing
- Harassment
- Indecent Content
- Malicious code
- System Intrusion

Securing Our Cyberspace

CYBER WARFARE

CyberSecurity MALAYSIA



Cyberwar

Internet and related technological means against political, economic, technological and information sovereignty and independence of a state.

Examples:
- Nation/government vs. terrorist/subversive groups
- Law Enforcement vs. organised crime
- Organisations vs. economic/industrial espionage

Tactics
- Cyber espionage
- Web vandalism
- Propaganda
- Gathering data
- Distributed Denial-of-Service Attacks
- Equipment disruption
- Attacking critical infrastructure
- Compromised Counterfeit Hardware

(source: http://en.wikipedia.org/wiki/Cyberwarfare)

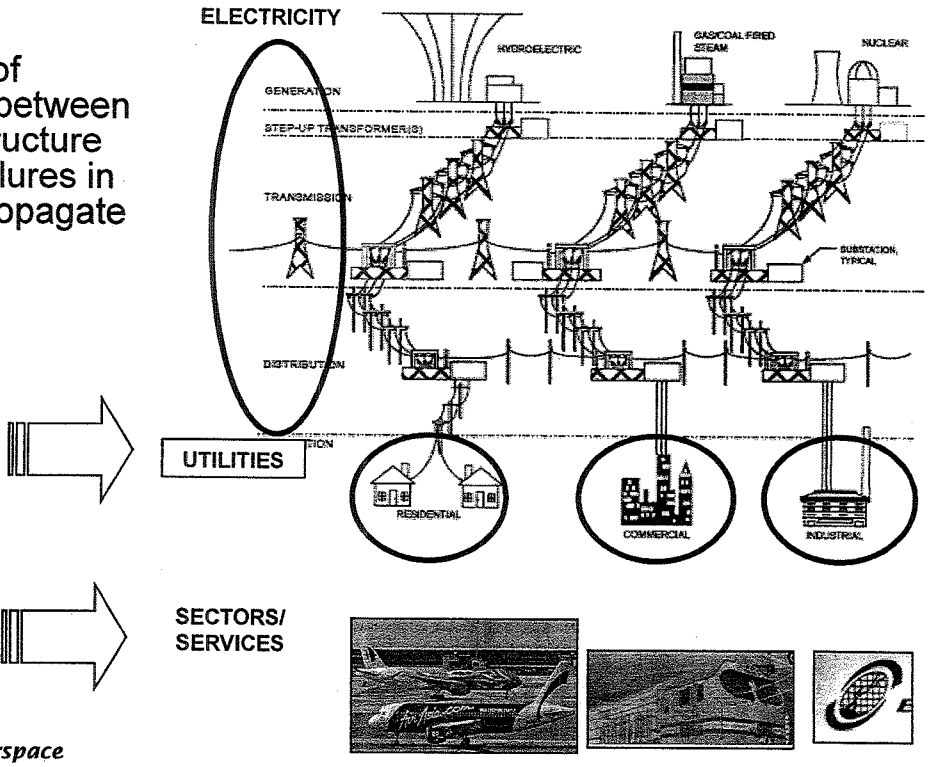
Securing Our Cyberspace

THREATS TO CRITIAL NATIONAL INFORMATION INFRASTRUCTURE (CNII)

CyberSecurity MALAYSIA

Interdependencies

The high degree of interdependency between our critical infrastructure sectors means failures in one sector can propagate into others.



E-SOVEREIGNTY AGENDA
- Malaysia's e-Sovereignty Foundation

CyberSecurity MALAYSIA

Source: NITC, 2003

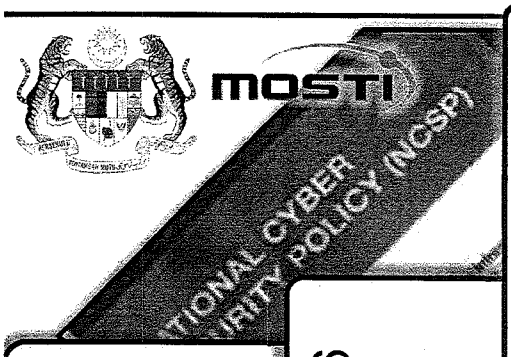
Self-Preservation
Preservation of identity (cultures, values, beliefs) and the sovereignty of the nation state (politics & economics)

Projection
Use of ICT to promote Malaysian image, wealth creation and worldview towards enhancing stature and sphere of influence

Protection
Enhancing security of the Critical National Information Infrastructures (CNII)

THE NATIONAL CYBER SECURITY POLICY (NCSP) - Objective

CyberSecurity MALAYSIA



2005 National Cyber Security Policy formulated by MOSTI

2006 NCSP Adoption and Implementation

2007 CyberSecurity MALAYSIA — CyberSecurity Malaysia launched by Prime Minister of Malaysia on 20 Aug 2007

- Malaysia's Ministry of Science, Technology & Innovation (MOSTI) carried out the study on the National Cyber Security Policy (NCSP) in 2005
- National IT Council (NITC) Meeting on 7 Apr 2006 agreed to implement NCSP and establishment of the Malaysia Cyber Security Centre to administer NCSP.
- NCSP was endorsed by the Cabinet in May 2006.
- CyberSecurity Malaysia launched by Prime Minister of Malaysia on 20 Aug 2007.

The policy 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

NCSP Objectives

- Address The Risks To The Critical National Information Infrastructure
- Ensure That Critical Infrastructure Are Protected To A Level That Is Commensurate With The Risks
- Develop And Establish A Comprehensive Program And A Series Of Frameworks

THE NATIONAL CYBER SECURITY POLICY - Vision & CNII Sectors

CyberSecurity MALAYSIA

VISION

'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'

DEFENCE & SECURITY
- Ministry of Defense, Military
- Ministry of Home Affairs, Police

TRANSPORTATION
- Ministry of Transport

BANKING & FINANCE
- Ministry of Finance
- Central Bank
- Securities Commission

HEALTH SERVICES
- Ministry of Health

EMERGENCY SERVICES
Ministry of Housing & Local Municipality

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Assets (real & virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on
- *National defense & security*
- *National economic strength*
- *National image*
- *Government capability to function*
- *Public health & safety*

ENERGY
- Energy Commission
- Electricity Co., Petroleum Company

INFORMATION & COMMUNICATIONS
- Ministry of Information, Communications & Culture
- Malaysia Communication & Multimedia Commission

GOVERNMENT
- Malaysia Administrative, Modernisation and Management Planning Unit

FOOD & AGRICULTURE
- Ministry of Agriculture

WATER
- National Water Service Commission

Securing Our Cyberspace

THE NATIONAL CYBER SECURITY POLICY
- Implementation Approach

CyberSecurity MALAYSIA

(0 – 1 YEAR) ADDRESSING IMMEDIATE CONCERNS

- Stop-gap measures to address fundamental vulnerabilities to the information security of the CNII.
- Creating a centralised security platform.
- Raising awareness of information security and its implications.

(0 – 3 YEARS) BUILDING INFRASTRUCTURE & HUMAN CAPACITY

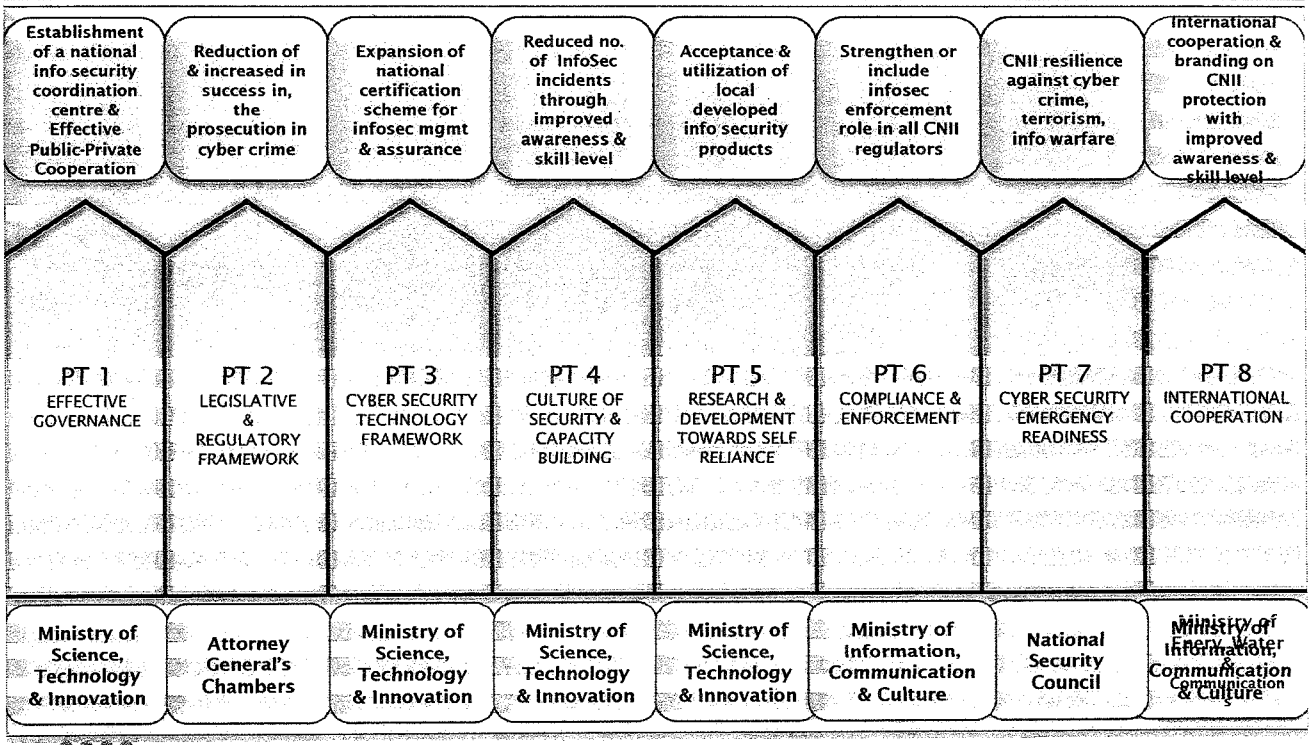
- Setting-up the necessary systems, processes, standards and institutional arrangements (mechanisms) .
- Building capacity amongst researchers and info security professionals.

(0 – 5 YEARS & 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 Info Security.

THE NATIONAL CYBER SECURITY POLICY
- Policy Thrust

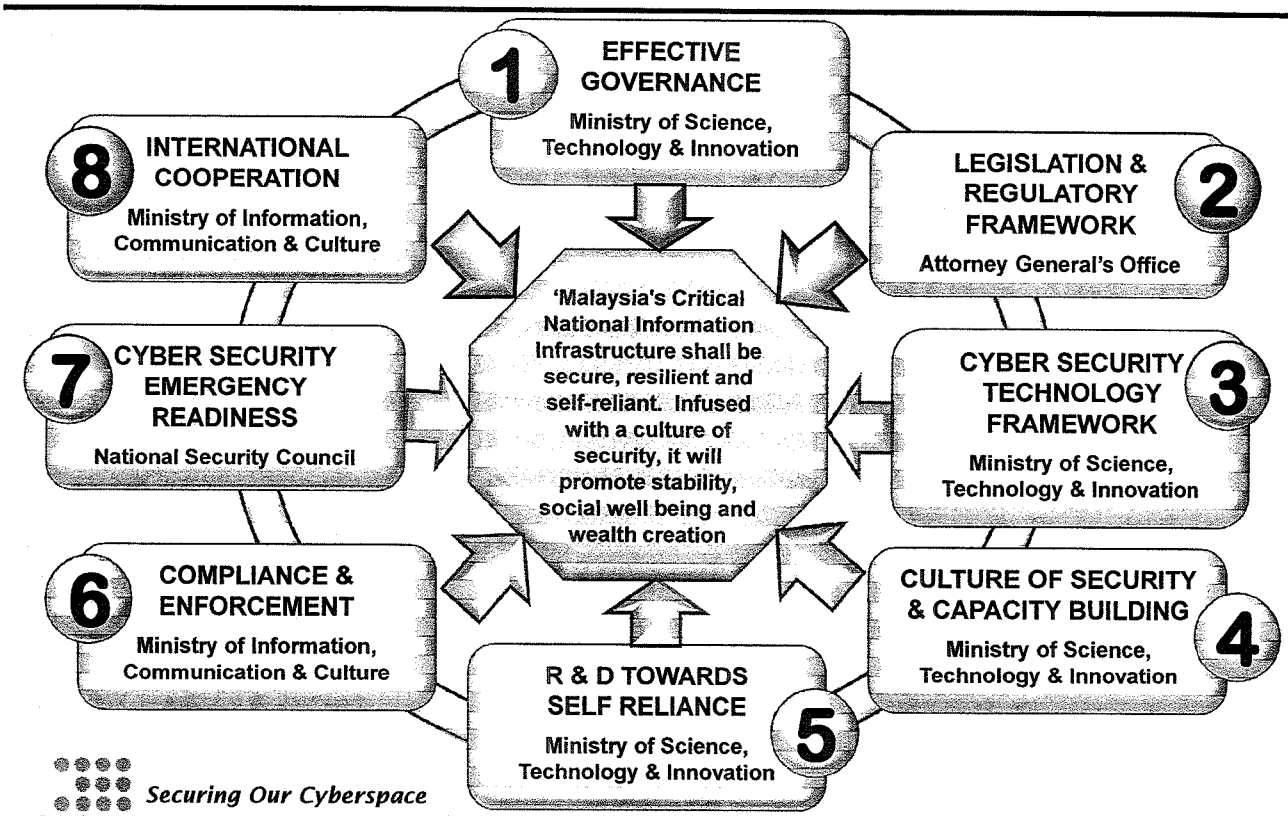
CyberSecurity MALAYSIA



PT – Policy Thrust

Securing Our Cyberspace

THE NATIONAL CYBER SECURITY POLICY - Policy Thrust



Securing Our Cyberspace

PT 1: EFFECTIVE GOVERNANCE - Structure

Establishment of a national info security coordination center

National IT Council
Chair: Prime Minister

National Cyber Security Advisory Committee (NaCSAC)
Chair: Chief Secretary

National Cyber Security Coordination Committee (NC3)
Chair: Secretary General, Ministry of Science, Technology & Innovation

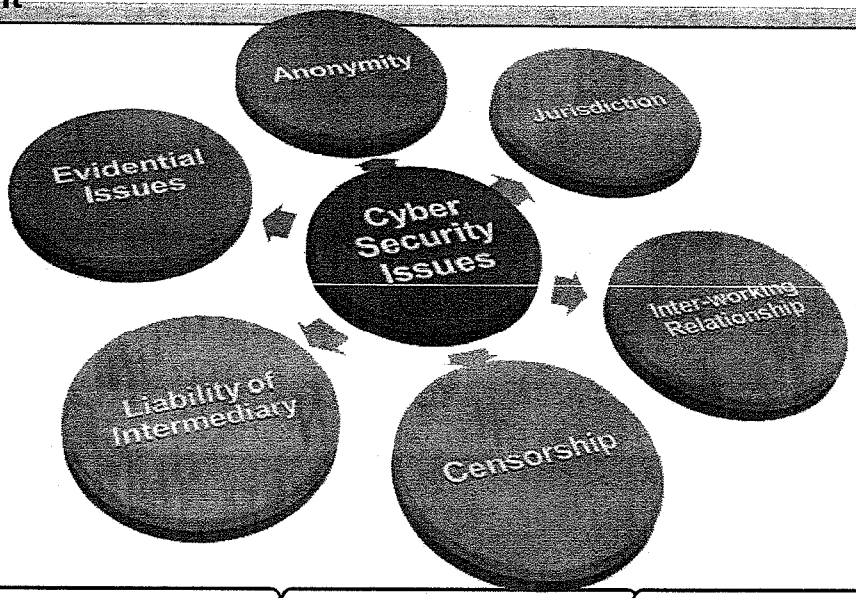
National Cyber Security Policy Working Group
| PT1 | PT2 | PT3 | PT4 | PT5 | PT6 | PT7 | PT8 |

Securing Our Cyberspace

PT 2: LEGISLATIVE & REGULATORY FRAMEWORK - Cyber Security Issues

CyberSecurity MALAYSIA

A Study on the laws of Malaysia to accommodate legal challenges in the Cyber Environment



Identification of issues and challenges faced in the cyber environment	Assessment of current legislative framework	Recommendation of type of amendments to the law

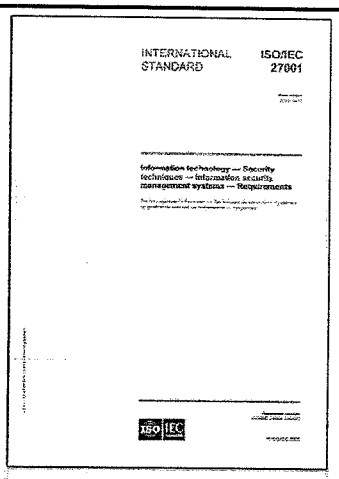
PT 2: LEGISLATIVE & REGULATORY FRAMEWORK - Cyber Laws Reviews Recommendations

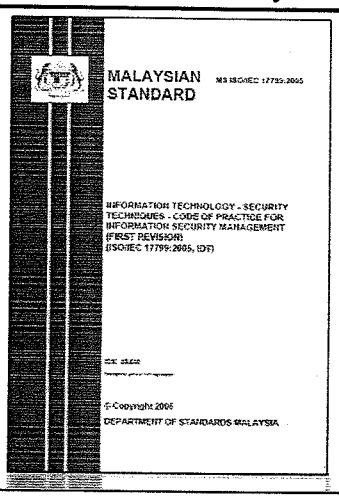
CyberSecurity MALAYSIA

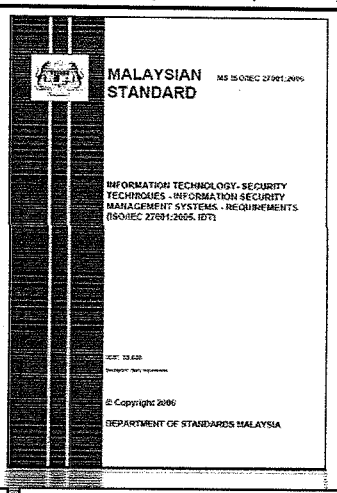
1. Improve the Laws
2. Awareness & Education
3. Enhance policies relating to cyber security
4. Evolving technology – Amendments to the law quickly but will be insufficient. Playing "catch-up" all the time
5. Jurisdictional benchmarking – constantly monitor law developments particularly Singapore, UK and Australia

PT 3: CYBER SECURITY TECHNOLOGY FRAMEWORK - Standards

To increase the robustness of the CNII sectors by complying to international standards:
MS ISO/IEC 27001:2006 Information Security Management System (ISMS)







The International Standards

MS ISO/IEC 27001:2006 | **MS ISO/IEC 17799:2005**

Adopted as Malaysian Standards

Securing Our Cyberspace

Expansion of national certification scheme for infosec mgmt & assuarance

PT 3: CYBER SECURITY TECHNOLOGY FRAMEWORK - Product Certification

Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme

MISSION
"to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products"

Malaysia was accepted as Common Criteria Recognition Arrangement (CCRA) Certificate Consuming Participant on 28 March 2007

Austria	India
Czech Republic	Turkey
Denmark	Italy
Findand	Malaysia
Greece	Pakistan
Hungary	Singapore

Securing Our Cyberspace

PT 4: CULTURE OF CYBER SECURITY & CAPACITY BUILDING – Cyber Security Acculturation Strategy Plan

The *Strategy* - to ensure the awareness programs, inclusive of the training and outreach activities are done effectively and reach the target audience with the right timing and depth accordingly

Acculturation:

- Types of contents for cyber security awareness materials
- Cooperation, communication and coordination plan
- Assess the current state of cyber security culture within the CNII elements' and formulate recommendations

Capacity Building:

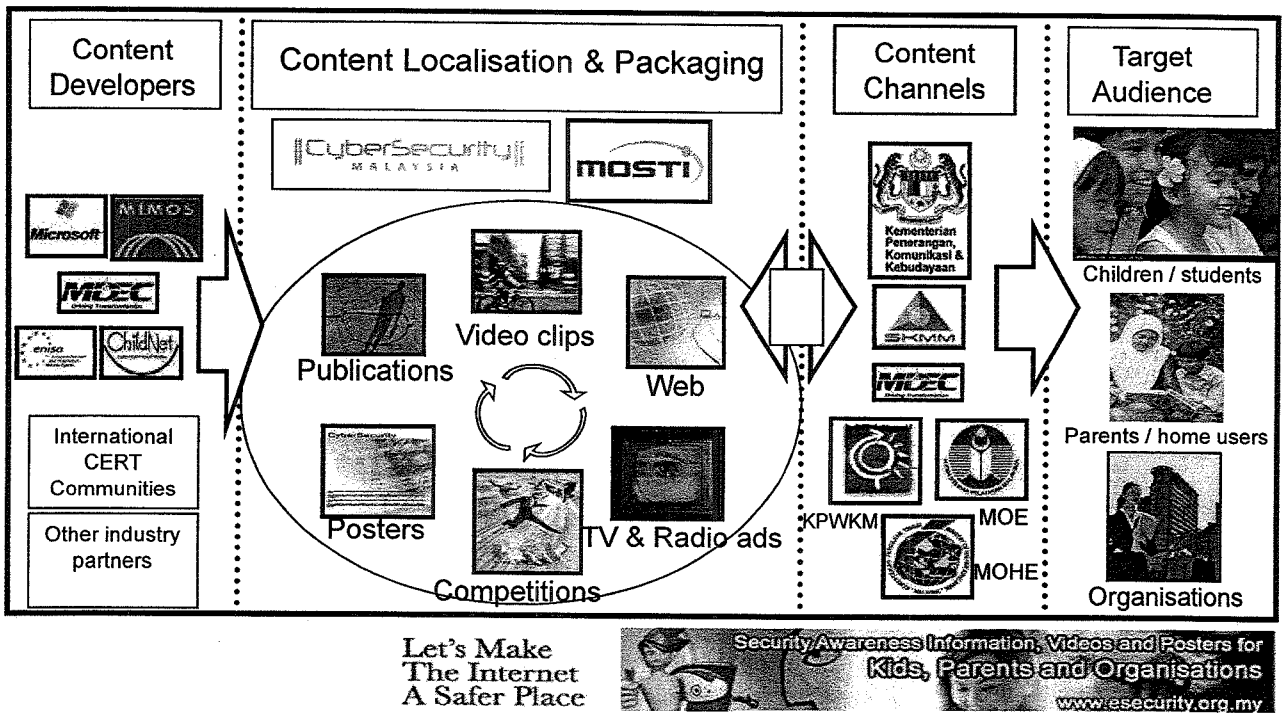
- Minimum requirements and qualifications for information security professionals.
- A plan for CNII entities to increase the number of certified security professionals within their respective organisations.

PT 4: CULTURE OF CYBER SECURITY & CAPACITY BUILDING – Capacity Building

	Associate Business Continuity Professional (ABCP) Certified Functional Continuity Professional (CFCP) Certified Business Continuity Vendor (CBCV) Certified Business Continuity Professional (CBCP)
	Certified Information Systems Security Professional (CISSP) Systems Security Certified Practitioner (SSCP)
	Certified Information Systems Auditor (CISA) Certified Information Security Manager (CISM) Certified in the Governance of Enterprise IT (CGEIT)
	Professional in Critical Infrastructure Protection (PCIP)

Reduce no of Infosec incidents through improved awareness & skill level

PT 4: CULTURE OF CYBER SECURITY & CAPACITY BUILDING - Awareness



PT 4: CULTURE OF CYBER SECURITY & CAPACITY BUILDING – Awareness Materials

PT 5: RESEARCH & DEVELOPMENT TOWARDS SELF RELIANCE - R & D Roadmap

CyberSecurity MALAYSIA

Development of the National R&D Roadmap for Self Reliance in Cyber Security Technologies is facilitated by MIMOS

Acceptance & utilization of local developed info security products

- To Identify Technologies That Are Relevant and Desirable by the CNII
- To Promote Collaboration with International Centres of Excellence
- To Provide Domain Competency Development
- To Nurture the Growth of Local Cyber Security Industry
- To Update the National R&D Roadmap

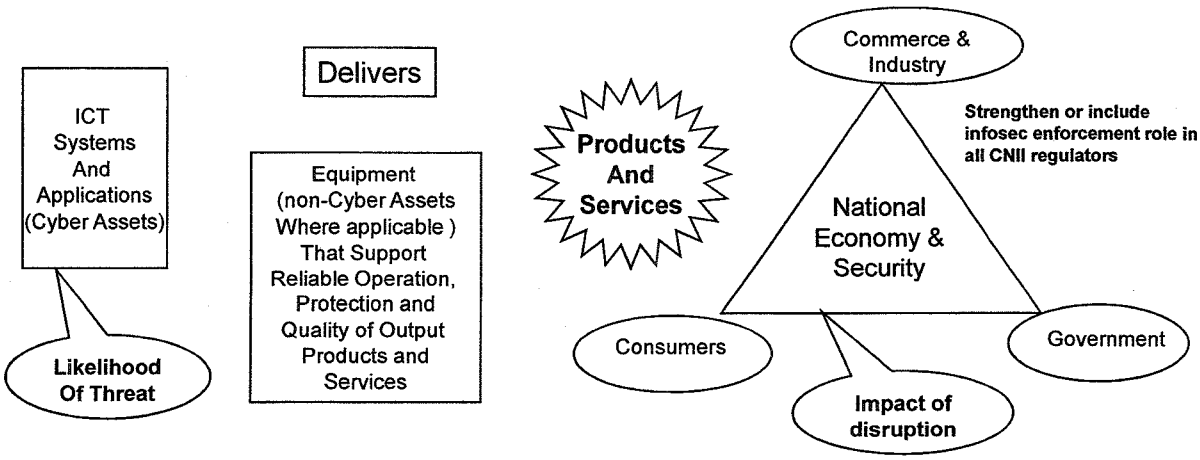
Securing Our Cyberspace

PT 6: COMPLIANCE & ENFORCEMENT - Risk Assessment

CyberSecurity MALAYSIA

Risk Assessment Focus in NCSP :

Risk Assessment (in NCSP-PT6 context) looks at the **likelihood** of threats exploiting vulnerabilities to **Cyber Assets** disrupting/compromising delivery of **Products and Services** and the **consequence or impact** of the disruption/compromises of the **Products and Services to the Nation**, Commerce, Industry, Government, Consumers and other beneficiaries . Inventorise list of critical products/services, identify cyber readiness, inventorise & monitor compliance to infosecurity standards

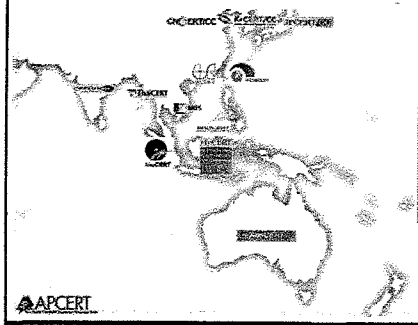


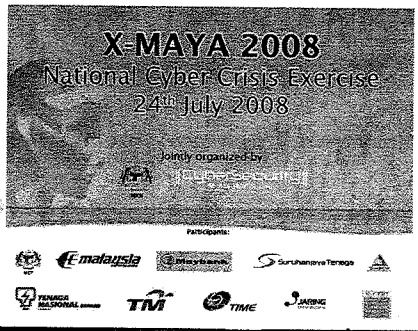
THE NATIONAL CYBER SECURITY POLICY
- Cyber Security Emergency Readiness

CyberSecurity MALAYSIA

NATIONAL CYBER CRISIS MANAGEMENT PLAN

A **framework** that outlines the **strategy** for cyber attacks mitigation and response among Malaysia's Critical National Information Infrastructure (CNII) through **public and private collaboration and coordination**





National Security Council (NSC)
Chair : YAB Prime Minister

National Cyber Crisis Management Committee (NCCMC)
Chair: YAB Deputy Prime Minister

National Cyber Crisis Management Working Group (NCCMWG)
Chair : Secretary of National Security Council

National Cyber Coordination and Control Centre (NC4)

CNII resilience against cyber crime, terrorism, info warfare

Increase the level of preparedness of the country against cyber attacks	Enhance the capability to handle cyber related issues	Provide coordinated response in handling cyber attacks	Minimize the impact to society and economic activities

PT 8: INTERNATIONAL COOPERATION
- Strategic framework

CyberSecurity MALAYSIA

Intl branding on CNII protection with improved awareness & skill level

LEADERSHIP
Explore opportunities at international cyber security platforms where Malaysia can *vie for positions* to play a leadership role to *project Malaysia's image and promote Malaysia's interests*

PRIORITIZE
Evaluate *Malaysia's interests* at international cyber security platforms and act on elements where Malaysia can *get tangible benefits and voice third world interests*

ENGAGE
Participate in relevant cyber security meetings and events *to promote Malaysia's positions and interests* in the said meetings and events

COLLABORATION

MEMBER

FIRST

OIC-CERT

APCERT

MoU with IPA, Japan

ISC²

APEC SPSG

ITU-D

ARF Cyber Security

APECTEL

MoU with AusCERT

Way Forward

- Closer Cooperation among APEC members, law enforcement agencies etc, to protect Cyberspace from Terrorist Use and Attacks.
- Strategic alliances provide assistance in anticipating and mitigating cyber attacks from abroad
- Sharing of information, best practices, tools, R&D and technologies in securing Cyberspace
- Need to keep up with/stay ahead of the cyber criminals in areas of people (skill set), process (management, underground criminal cooperation) & technology

THANK YOU