Cyber Crime Legislations

Raj Kumar

Cyber Crime Legislations

- International Conventions
- National frameworks
- Loop holes and need to update
- Examples of best practices from the region

Cyber Crime Legislations

- The term “cybercrime” is used to cover a wide variety of criminal conduct.
- As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime.
- One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences:
  - offences against the confidentiality, integrity and availability of computer data and systems;
  - computer-related offences;
  - content-related offences;
  - copyright-related offences.

Convention on Cyber Crime

- Also known as the Budapest Convention on Cyber Crime, drawn up by the Council of Europe, France
- The first international treaty on Internet and computer networks related crimes
- Addresses:
  - infringements of copyright
  - computer-related fraud
  - child pornography
  - hate crimes
  - violations of network security
  - illegal access and interception
  - Data and system interference
  - Misuse of device
  - Computer related forgery
- Has powers and procedures for conducting search of computer networks and lawful interception.
- International Treaty seeking to address computer and internet crime by
  - Harmonising national and domestic criminal laws related to cyber crime
  - Improving investigation techniques and procedures
  - Increasing cooperation among countries
- As of Dec 2016, 52 states have ratified the convention

National Frameworks - EU

- **EU Network and Information Security (NIS) Directive:**

  In January 2016, EU Parliament approved NIS Directive, proposed in 2013 EU Cyber Security Strategy. Expect formal approval by Council of Ministers, then EU countries must implement into national law within 21 months.

- PRIVACY – **Proposed EU General Data Protection Regulation**
  Extraterritorial Application and Enforcement. New law would apply to any company that controls or processes the personal data of Europeans through the offering of goods and services – *even if company has no physical presence in Europe.*
  - *Fines* of up to 4% of company's annual global revenue or *€20 million* for violations

U.S. Cybersecurity Laws

Cybersecurity legal parameters arise from multiple layers and sources:

Federal law

Computer Fraud and Abuse Act prohibits unauthorized computer access, interference, obtaining data

Electronic Communications Privacy Act governs interception, access to data

State law -- fills gaps in federal law, but can set *de facto* national standards

- Example: Massachusetts data breach requirement triggered by a (1) substantial risk of
- identity theft or fraud (2) OR acquisition or use for an unauthorized purpose
- Companies handling sensitive personal data must have Written Information Security Policy; encryption of personal data transmitted externally; and specific minimum "administrative, technical, and physical" security controls.

U.S. Cybersecurity Laws – Critical Infrastructure and Information Sharing

Enhancing cybersecurity for "critical infrastructure" has been a key focus of the Obama administration.

- February 2013: **Executive Order 13636**
- Identifies 16 critical infrastructure areas
- Regulators directed to review existing authorities and act to improve cybersecurity among regulated entities
- February 2014: NIST releases **Cybersecurity Framework** and **CI Cyber Community** ("C³")

Cybersecurity Act of 2015:

Information-Sharing through DHS Portal. Establishes a *voluntary* framework for confidential, two-way sharing of cyber threat information between private sector and U.S. government, via a Department of Homeland Security portal; offers protection from liability for sharing.

U.S. Cybersecurity Laws – Protecting Personal Information

Companies have generally applicable legal obligations to protect personal information.

- Data Security**: Massachusetts data security law** requires specific affirmative acts
- Data Breach Notification**:** State laws generally require alerts to state regulators and impacted
- individuals if breach involving personal data.

Companies may not make “deceptive” data security claims or engage in “unfair” data security practices. Policed by Federal Trade Commission and state regulators.

In certain sectors, specific laws impose additional layer of security duties for certain categories of sensitive personal data.

- Financial Services: **Gramm-Leach-Bliley Act** (Nonpublic Personal Information, “NPI”)
- Healthcare: **HIPAA** (Protected Health Information, “PHI” and “ePHI”)
- Telecommunications Carriers:

Canada Cybersecurity Laws

Criminal Code

- Prohibits “fraudulently and without color of right” obtaining “any computer service;” or willful “mischief” to interfere with computer use or tamper with data.
- Prohibits interception, access to electronic communications, but exceptions for consent
- (“express or implied”) or to protect the network.

Personal Information Protection & Electronic Documents Act (PIPEDA) (2005)

- Reasonable administrative, technical, physical measures to protect personal data.
- Enforcement
  - Entities: Office of the Privacy Commissioner of Canada enforces **PIPEDA**
  - Risk: high degree of privacy enforcement, deemed “adequate” country by EU

United Kingdom Cybersecurity Laws

Computer Misuse Act of 1990 (Amended in 2006)

- Prohibits hacking, unauthorised access to computer systems, and purposefully spreading malware.
- Enforcement
- UK ICO can issue an Enforcement Notice for breach of the data protection principles

UK Data Protection Act of 1998. (This will change **GDPR** in 2018.)

- Staysure.com.uk (2015): Fine of £175,000 on holiday insurance company for inadequate security systems and policy, causing breach of credit card data of 90,000+ customers
- Worldview Limited (2014): Fine of £7,500 for vulnerability in company's website, enabling hackers to access payment card data of 3,500+ customers

French Cybersecurity Laws

French Data Protection Act

- Omnibus privacy, data protection, and cybersecurity framework law enforcement
- In May 2015, the CNIL issued a summary of its inspection program for 2015.
- 2014: CNIL (Commission Nationale de l'Informatique et des Libertés) conducted 421 inspections
- 2015: CNIL planned to conduct 550 inspections
- Optical Center (2015): Fined €50,000 by the CNIL for inadequate security of customers' personal data (vulnerable customer login site, weak passwords).

German Cybersecurity Laws

Federal Data Protection Act (BDSG)

IT Security Act (ITSG) (2015) -- critical infrastructure operators must:

- Establish and Implement a minimum set of security measures;
- Verify implementation by conducting security audits;
- Report incidents to Federal Office for Information Security (BSI).

Telecommunications Act (2014*)* contains sector-specific data security provisions.

- For example, section 109 requires the use of technical safeguards to prevent unauthorized access.
- Enforcement:
  - Improper Data Processing Agreement (Bavarian DPA, 2015)
  - Imposed big fine on data controller for failure to adequately

Estonian Cybersecurity Laws

National Department of Critical Infrastructure Protection

- Coordinates IT security for 42 critical public and private services

Estonian Information Systems Authority (EISA)

- Assists and supervises public and private sector organizations with IT security.
- Responsible for encryption of electronic IDs issued to Estonian citizens and businesses.

Data Protection Inspectorate

- Allows the public to request info about collection of personal data; promotes transparency of institutions performing public functions.

National CERT (CERT-EE)

- Handles security incidents on the .ee domain (denial of service attacks, malware)

Chinese Cybersecurity Laws

No comprehensive cybersecurity law

Draft Cybersecurity Law (July 2015) would consolidate existing powers, including monitoring, and introduces concept of Critical Information Infrastructure

Antiterrorism Law (effective January 2016)
Requires telecom operators and Internet companies to provide "technical interfaces, decryption and other technical support and assistance" to China's government investigating terrorist activities, broadly defined. Omits controversial draft language requiring data localization and encryption key registration by foreign tech companies.

National Security Law (July 2015)
Government to ensure that key technologies and infrastructure, as well as information systems and data in important areas, are "safe and controllable", so as to "protect national sovereignty, security and development interests in the cyberspace."

Computer Information Network and Internet Security, Protection, and Management Regulations
Internet service providers must secure processing of data, educate Internet users on security.

Japanese Cybersecurity Laws

Criminal Code, and Act on the Prohibition of Unauthorized Computer Access (UCAL):
Prohibit computer fraud, malware, spyware, obstructing business by interfering, false data, unauthorized computer access.

Act on the Protection of Personal Information (APPI): duty of companies to secure personal data they handle

Enforcement

- *Entities*: NO central data protection authority in Japan. APPI enforced by the ministry responsible for oversight of the sector containing the company at issue
- *Risk:*
- High risk if violations of Criminal Code, or UCAL
- Moderate risk if privacy violations

When relevant ministry learns of a company's violation, ministry first contacts company informally to discuss problem, changes. Low risk of formal enforcement, unless fail to implement those changes.

Benesse (2014): after, breach affected 35 million customers, the Ministry of Economy, Trade, and Industry directed company to change contracts with subs and own management and security controls.

South Korean Cybersecurity Laws

Act on the Protection of Information and Communications Infrastructure
Information and Communications Network Act - detailed security standards for service providers

Personal Information Protection Act (PIPA)

- One of strictest privacy regimes in world: breach damages awarded up to 3x actual harm claimed
- Imposes security requirements on entities handling personal data
- Breach Notification Required

PIPA and sectoral statutes require prompt notice of personal data breach to individuals and regulators
Enforcement

- *Risk*: high if privacy violations
- Google (2014): Fined ~$200K for harvesting sensitive personal data from wi-fi networks w/o consent

Indian Cybersecurity Laws

India's **Information Technology Act of 2000 (IT Act)** addresses the protection of electronic data and computer-related offenses (e.g., hacking and tampering with computer source documents)

Under 2008 amendments, **IT Act** does not criminalize hacking, but prohibits computer related fraud and tampering with computer source documents.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules – "Privacy Rules" . Together, **IT Act** and **Privacy Rules** impose cyber requirements on companies.

- "Reasonable Security Practices" interpreted as operation of documented, comprehensive information security program, policies, and procedures
- Parties can specify "reasonable security practices" in contract.

Singapore Cybersecurity Laws

Computer Misuse and Cybersecurity Act governs cybercrime.
Unauthorized access to or modification of computer material; Unauthorized use or interception of a computer service; **2013 Amendments** address cyber threats to *critical information infrastructure.* Minister of Home Affairs can direct companies to take pre-emptive measures necessary to prevent, detect, or counter any cyber threat to national security, essential services, or foreign relations of Singapore.

Personal Data Protection Act 2012 is Singapore's first comprehensive framework for personal data protection.

- Individuals and organizations must protect personal data with reasonable security arrangements to prevent unauthorized access or similar risks.

Australia Cybersecurity Laws

Telecommunications (Interception and Access) Act 1979

- May intercept data if one party consents OR if owner performing network security and informs employees
- Employer may monitor employee's personal data too, if sufficient nexus to EE record/relationship + inform employees

Privacy Act 1998 (amended 2014)

- Exemption for employer actions directly connected to employee record/relationship
- Reasonable steps to protect personal data (data breach policy, incident response plan)
- No general data breach notice mandate, but is required in health and financial sectors

Enforcement:

- *Entities:* Australian Information Commissioner and the Privacy Commissioner
- Makes determinations on alleged breaches of Privacy Act, enforceable by court
- *Risk:* higher since 2014, new power for Privacy Commissioner: penalties, enforceable order
- Maximum civil penalty for privacy violations: AU$ 1.7 million for companies
- Adobe (2015): AIC found Adobe's handling of customer password hints violated Privacy Act; recommended security changes

UAE Cybersecurity Laws

Cyber Crimes Law:
2012 Amendments expand scope of offenses, definition of privacy violations and monetary penalties and punishment

Offenses: Strict liability standard for unauthorized access to electronic sites and information; no intent required.

Penalties: Increase with perceived sensitivity of data accessed or disclosed. Many violations entail imprisonment or deportation.
No comprehensive data protection law

Telecommunications Regulatory Authority
- Oversees telecommunications, information technology, and Internet regulation

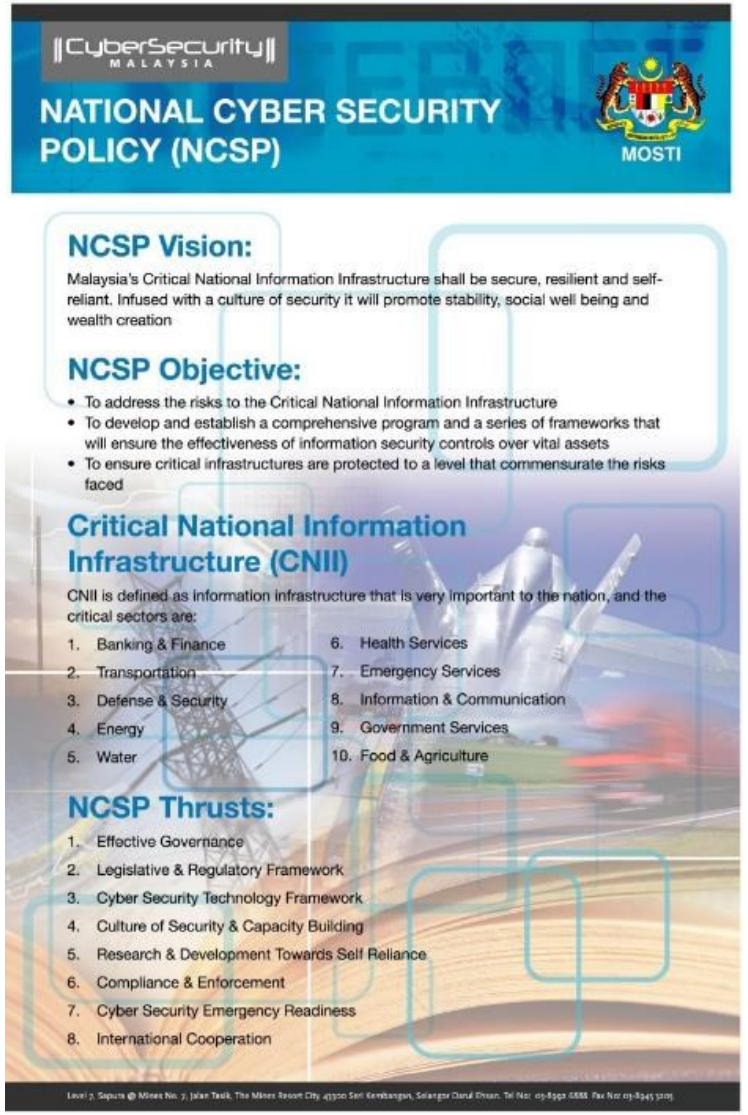
National CERT (aeCERT)
- Provides incident response support and cybersecurity awareness training

Loopholes and the need to update

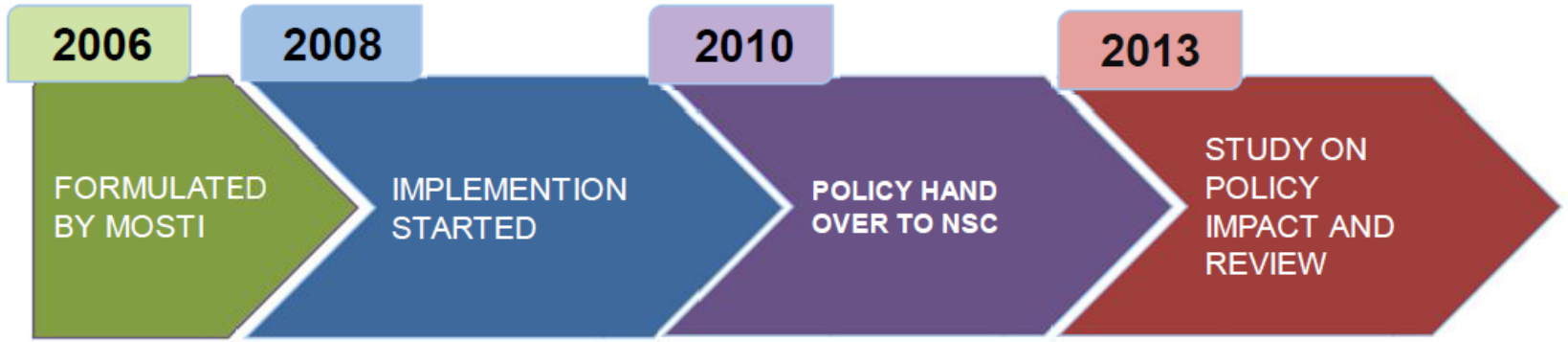
- The rapid growth of the Internet and sophistication of cybercrime continues to **outpace the ability of the legal system to respond.** The **attribution problem** makes policing and accountability particularly difficult.
- Cyber **assets are distributed** between the public sector and private sector, and the private sector is comprised of a wide range of disparate entities.
- There is a **lack of international coordination** on cyber issues. As a result, there is no centralized international cyber threat **information sharing** or common computer **incident response** teams.
- **Different values** among countries; different levels of **preparedness**; different degrees of **interest and risks**.
- Companies and governments face overlapping and **conflicting sets of laws**:
- Harmonization vs. divergence of regional and national laws
- **Personal data laws and system/infrastructure obligations are not integrated or reconciled**

Examples of the best practices from the region – Malaysia National Cyber Security Policy (NCSP)

The policy recognises the critical and highly interdependent nature of the Critical National Information Infrastructure **(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.



Malaysia's NCSP Introduction



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

Objective

i. Address the risks to the **Critical National Information Infrastructure (CNII)**
ii. To ensure that critical infrastructure are protected to a level that is commensurate with the risks
iii. To develop and establish a comprehensive program and a series of frameworks

NCSP Implementation Plan

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

10 Critical Sectors

8 Policy Thrusts

No.	Policy Thrust	Thrust Driver
1	Effective Governance	National Security Council
2	Legislative & Regulatory Framework	Attorney General's Chambers
3	Cyber Security Technology Framework	Ministry of Science, Technology & Innovation
4	Culture of Security & Capacity Building	Ministry of Science, Technology & Innovation
5	R & D Towards Self-reliance	Ministry of Science, Technology & Innovation
6	Compliance & Enforcement	Ministry of Communications and Multimedia
7	Cyber Security Emergency Readiness	National Security Council
8	International Cooperation	Ministry of Communications and Multimedia

PT 1: Effective Governance

Thrust driver : National Security Council

Objectives:

- To have a centralised coordination of the national cyber security initiatives;
- To promote effective cooperation between the public and the private sectors; and
- To establish and encourage informal information sharing exchanges.

PT 2: Legistlative & Regulatory Framework

Thrust driver: Attorney General's Chambers

Objectives:

- Review and enhance Malaysia's cyber laws to address the dynamic nature of cybersecurity 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

PT 2: Legislative & Regulatory Framework : Malaysia's Cyber Law

Digital Signature Act 1997

TeleMedicine Act 1997

Copyright Act (Amendments) 1997

The Communications and Multimedia Act 1998

Computer Crime Act 1997

Consumer Protection Act 1999

Chapter VIA, Offences Relating to Terrorism, Penal Code (Amendment) Act 2007

Evidence (Amendment) (No. 2) Act 2012

CELEBRATING 25 YEARS OF ACHIEVEMENTS

PT 3: Cybersecurity Technology Framework

- Thrust driver: Ministry of Science, Technology & Innovation (MOSTI)

- Objectives:
  - 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

PT 3: Cybersecurity Technology Framework

- Thrust driver: Ministry of Science, Technology & Innovation (MOSTI)

- Objectives:
  - 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

PT 3: Cybersecurity Technology Framework

The International Standard

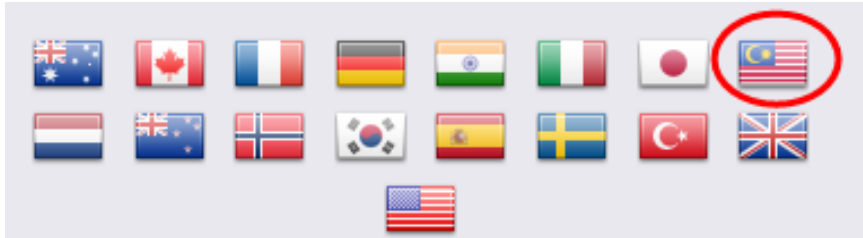
MS ISO/IEC 17799:2005 | MS ISO/IEC 27001:2007

Adopted as Malaysian Standards

ITU 1992 2017 CELEBRATING 25 YEARS OF ACHIEVEMENTS

PT 3: Cybersecurity Technology Framework : Common Criteria Recognition Agreement (CCRA)

- **Certificate Authorizing Members:**
  - Participants that represent a compliant Certification Body
  - Mutually recognizes certified products/systems produced by the Certificate Authorising Participants based on ISO/IEC 15408
  - Malaysia has been a certificate consuming member and has been audited to become a Certificate Authorizing Member a member of CCRA since 2007



- **Certificate Consuming Members:**
  - Participants that have a national interest in recognising CC certificates produced by the Certificate Authorising Participants based on ISO/IEC 15408

CELEBRATING 25 YEARS OF ACHIEVEMENTS

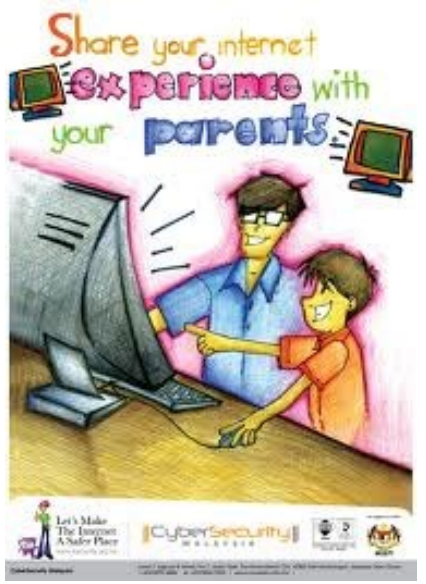
PT 4: Culture of Security and Capacity Building

- **Cybersecurity acculturation**
  - A plan to inculcate best practices, good habits and behaviours on good and safe use of Internet
  - Include content, approach and implementation plan for acculturation

- **Capacity building**
  - A plan to get organisations and individuals towards building a pool of information security professionals
  - Include content for skills areas, approach and implementation plan

PT 4: Culture of Security and Capacity Building : Cybersecurity Awareness

- Awareness posters
- CyberSAFE awareness newsletter
- INFOSEC Knowledge Sharing
- Radio Advertisements



www.cybersafe.my

CELEBRATING 25 YEARS OF ACHIEVEMENTS

PT 4: Culture of Security and Capacity Building : Capacity Building

- Help nurture the information security workforce with the required knowledge and skills by providing information security competency and capability courses and certifications.

- This is accomplished through strategic collaborations with reputable organizations in Malaysia and international
- accreditation institutions.

- Malaysia requires sufficient skilled people to deal with sophisticated cyber threats & uncertainty of cyber space.

(ISC)²®

ISACA®
Trust in, and value from, information systems

DRI International

ITU-D 1992 2017 CELEBRATING 25 YEARS OF ACHIEVEMENTS

PT 5: Research and Development towards Self-Reliance

Thrust driver: Ministry of Science, Technology & Innovation (MOSTI)

- **Issues:**
  - Lack of cybersecurity coordination and prioritization at the national level.
  - This has caused research agendas and programs not to be systemcatically managed.
  - Important priorities overlooked.
  - Need of a central entity to coordinate and prioritise the current and future R&D.

- **Solution:**
  - Malaysian Institute of Microelectronic Systems (MIMOS) – the national R&D centre in ICT under MOSTI, to align and integrate R&D programs to avoid duplication.

MIMOS
National R&D Centre in ICT

CELEBRATING 25 YEARS OF ACHIEVEMENTS

PT 5: Research and Development towards Self-Reliance

MIMOS :

Consortium of 22 organisations, representing academic, government, industry and researchers.

Key task is the development of the National R&D Roadmap for Self Reliance in Cybersecurity Technologies

CELEBRATING 25 YEARS OF ACHIEVEMENTS

PT 6: Compliance & Enforcement

- Issues:
  - Interdependencies across the CNII are complex such as no telecommunication organization can work without power and no financial institution can operate effectively without telecommunications.
  - A weakness in one sector can often translate into a weakness in all sectors.

- Solution:
  - The Thrust 6 working group has developed a risk assessment framework for the CNII to use in identifying risk within their respective IT systems.
  - This will help the entities to understand their own risk profile by using similar, acceptable and comparable techniques to identify risk.

- Thrust Driver: Ministry of Communication and Multimedia
  - The major information and communication regulator - Malaysian Communications and Multimedia Commission and CNII entities such as Telekom Malaysia, Maxis, Jaring to name a few are under t`he purview of this ministry.

PT 6: Compliance & Enforcement

Case for change:

- Cabinet mandate for CNII organizations to obtain ISMS certification within 3 years from the date of mandate 24 Feb 2010
- Low compliance to information security standards amongst CNII (only 50 CNIIs certified ISO27001 to date)
- Weak ecosystem of local industry to support the requirements of CNII e.g. Products certified under Common Criteria

Recommendation:

- Ensure mandatory compliance of ISMS Standards for CNII
- Capability and Awareness for CNIIs
- Facilitate Industry Development

Ensure Mandatory Compliance to Information Security Standards by CNII	• Study the need to introduce an Act to ensure mandatory compliance by CNII to ISMS Standards (ISO27001) and other selected info security standards.
Capability and Awareness Programmes for CNIIs	•ISMS (ISO/IEC-27001) training and workshops for CNIIs and regulatory bodies •CNII Information Security Standards Adoption Program
Facilitate Industry Development	•Products certification under ISO 15408 (Common Criteria EAL2) •Cyber Security Industry Directory •Cyber Security Trade Event to promote locally developed certified products under Common Criteria

PT 7: Cybersecurity Emergency Readiness

Issues:

- Many organizations within the CNII do not report cyber security incidents.
- Effective cyber security monitoring is not prevalent across the CNII.

Solution:

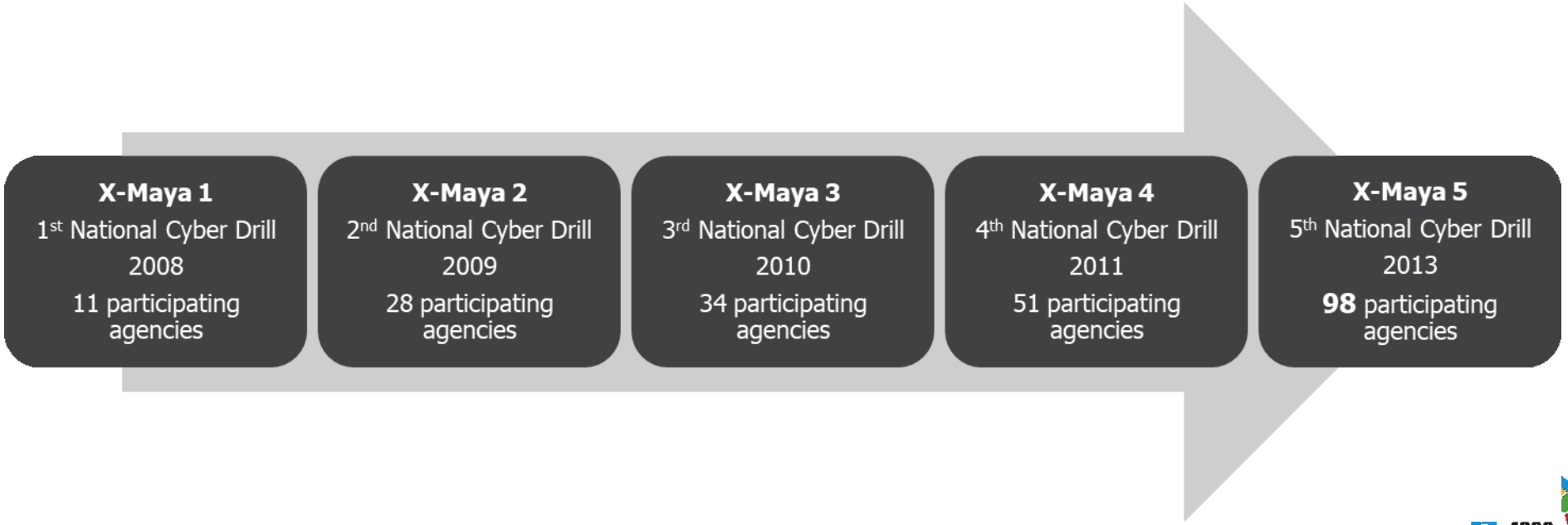
National Cyber Crisis Management Plan **(NCMP) -** A framework that outlines the strategy for cyber attacks mitigation and response among Malaysia's Critical National Information Infrastructure (CNII) through public and private collaboration and coordination.

Thrust driver : National Security Council

PT 7: Cybersecurity Emergency Readiness

Cyber Drill : X-Maya

- Tied to the NCCMP, the cyber drill is to test the procedures and processes stated in the plan.
- The drill also observe the reaction of participating CNIIs and the flow of information.
- All kinks are iron out to ensure continuous improvement to the NCCMP.



PT 8: International Cooperation

Issues:

- No nation can act alone.
- The cyber environment does not conform to the physical boundaries of the countries thus successful cybersecurity initiatives require international cooperation.

Thrust driver: Ministry of Communications and Multimedia

PT 8: International Cooperation

Collaboration with:

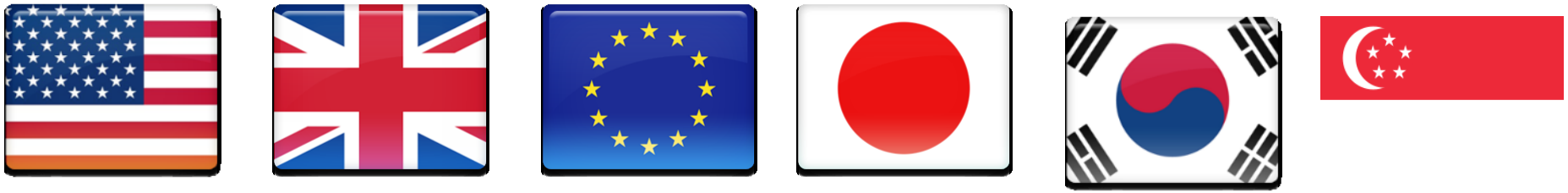
1. MoU with Japan CERT (JPCERT)
2. MoU with Information Technology Promotion Agency, Japan
3. MoU with Australian CERT (AusCERT)

Member of:

1. International Telecommunication Union (ITU)
2. Asia Pacific Computer Emergency Response Team (APCERT)
3. Organization of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT)
4. Forum of Incident Response and Security Teams (FIRST)
5. Security and Prosperity Steering Group (SPSG) under APEC Telecommunication and Information Working Group (APECTEL)
6. ASEAN Regional Forum (ARF) in Cyber Security

Other Strategic Initiatives

- In May 2009, **US** President Obama launched “CyberSpace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”
- In June 2009, **UK** Government published the first Cyber Security Strategy of the United Kingdom alongside the first annual update of the National Security Strategy.
- ENISA (**European** Network Information Security) founded “Dependability Roadmap” developed by IST.
- “Information Security Master Plan” developed by Ministry of Economics and Industry (2003) Security policy reinforced through e-**Japan** Strategy
- Security Policy in IT839 Strategy developed (2004) by Ministry of Information and Communication “Secure u-**Korea**”
- In 2016, Singapore launched their Singapore Cybersecurity Strategy



ITU : I Thank U