



Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

Information and Network Security Issues in the Communications and Multimedia Industry

TOH SWEE HOE

Malaysian Communications and Multimedia
Commission [MCMC]

HackInTheBox Conference, KL

2004



Agenda

- A. Background
 - Malaysian regulatory framework
 - Market environment
- B. Security Issues/Challenges
- C. Initiatives in safe and secure networking
- D. Stakeholders to meet the challenges



A. Background

[Regulatory Framework]

1. Establishment of MCMC
2. Scope of responsibility
3. National Policy Objectives under the Communications and Multimedia Act (CMA) 1998
4. Convergence
5. Licensing under the CMA 1998



Establishment of MCMC as the industry's regulator

- A statutory corporation
 - Established by the Malaysian Communications and Multimedia Commission Act 1998 (MCMCA)
 - Effective from 1 November 1998
- Operational autonomy but subject to policy directives from Minister



Scope of Responsibility

- To regulate according to the :
 - Communications and Multimedia Act 1998 (CMA)
 - Postal Services Act 1991 (PSA)
 - Digital Signature Act 1997 (DSA)
- Covers telecoms, broadcasters and ISPs; postal and courier services; and digital certification authorities



National Policy Objectives under CMA

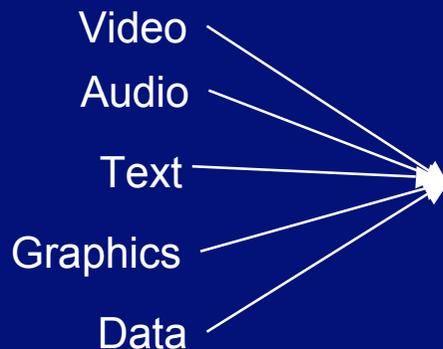
1. Creating a global hub
2. Building a civil society
3. Nurturing local content and culture
4. Ensuring long-term benefits for end-users
5. Nurturing user confidence
6. Promoting access and equity
7. Creating a robust applications environment
8. Facilitate efficient allocation of resources
9. Developing industry capabilities
10. Promoting secure and safe networking



Convergence

Technology convergence

Evolution into common digital platforms for delivery of audio-visual content and applications



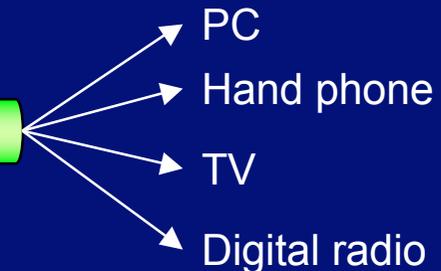
Converged market for communications and multimedia services

Convergence regulator needed to facilitate seamless evolution from separate markets to converged markets



Service convergence

Services delivered over non-traditional access equipment, e.g. radio over PC, e-mails over TV, video over hand phones





Types and Categories of Service Provider Licences

Types of Licence	Individual	Class
Content Applications Service Provider	X	
Applications Service Provider	X	X
Network Service Provider	X	X
Network Facility Provider	X	X



A. Background [Market environment]

- Communications market in Malaysia
- General Market Trends in Malaysia - Internet
- ISP Consumer Satisfaction Index
- E-Security Survey 2003



Malaysia's Communications Market

Penetration Rate (per 100)	2001	2002	2003	2004
Cellular	30.8%	36.9%	43.9%	48.5%
Internet Dial-up	8.8%	10.5%	11.4%	12.4%
Fixed Line	19.6%	18.8%	18.1%	17.8%



General Market Trends : Internet

Dial Up Subscriptions by ISP

Total subscribers	:	Q1, 2004 - 3.139 m
Growth rate	:	8.7 %
Penetration	:	12.4 %
Major ISPs	:	TMNet (57.5%), Jaring (23.5%) Time.Net (17.3 %)

Broadband users	:	Q2, 2004 - 174,018
Penetration	:	0.68 %



ISP Consumer Satisfaction Index

- There has been 6 “waves” of surveys from Feb 2001 to November 2003
- ISPs concerned - TM Net and JARING
- During the last wave, the average score of the two ISPs (from 10) among Individuals were 7.59 while the Commercial sector scored the two ISPs an average of 7.34



E-Security Survey

- During the E-Security Awareness Program in 2003, MCMC conducted a survey in Kota Bharu, Kelantan, Kota Kinabalu, Sabah and Johor Bharu, Johor.
- The survey was conducted to gauge the level of understanding of E-Security issues in those states.
- Some sampling of the results:
 - Knowledge of what a virus is - 90% of those surveyed know what a computer virus is.
 - Anti-Virus software - 85% have installed anti-virus software on their computers



E-Security Survey

- Infected by virus - 70% of those surveyed have had their computers infected by viruses.
- Trust of the Internet - Only 16% are comfortable with the level of security the Internet offers.
- Internet Security - 87.5% of those surveyed quoted security issues as a concern when they are connected to the Internet
- Awareness campaigns - Only 12.6% of those surveyed felt that there is sufficient information for ordinary users on E-Security.



B. Security issues/challenges

- Service convergence
- Wireless
- Nomadic and mobile – roaming
- Applications/Network's openness to abuse
- Powerful intelligent user devices
- Knowledge/capacity to act
- User/Consumer confidence/thrust



Security Challenges [Service convergence]

Emergence of new converged services allows security breach to spread across network service boundaries

- VOIP Voice service via Internet Protocol (IP) , an application service of IP telephony
- SMS mobile/VoIP/PSTN callback services
- IP based video/audio streaming subscription over broadband wired and wireless services
- SIP/PC phones to PSTN/mobile



Security Challenges [Wireless]

1. Trends towards being wireless but always connected when:-
 - a. Mobile - Edge/GPRS/3G
 - b. Nomadic - WiFi Hotspots and Wi-Max MAN
 - c. Home - Wireless LAN
2. Being wireless opens communications to tapping/listening-in.



Security Challenges [abuse]

Intrusion, Viruses, Trojan Horses, Spam, Phishing,
Malicious Hacking
Spy ware, Identity Theft,
Piracy, Fraud, DoS, DDoS,
Malicious Emails etc



Security Challenges

1. In maintaining a service, two keys areas that must be secure are:
 - a. User authentication; and
 - b. Data confidentiality
2. Considering the issues in service convergence, being wireless, being mobile and nomadic, powerful user devices, and service openness to abuse, make the task of keeping network integrity for service/business continuity a big challenge



Security Challenges [Knowledge/Capacity]

Everyone faces the same challenges.
Addressing those same challenges require:

- Time
- Money
- Knowledge
- Staff
- Discipline



C. Initiatives for safe and secure networking



MCMC's initiatives – 1/2

1. Information and Network Security Policy for the Communications and Multimedia industry
2. Regulating SPAM
3. The Information Sharing Forum (ISF) for Information and Network Security
4. Information and Network Security Audits



MCMC's initiatives – 2/2

5. Awareness and Education
6. Capacity Building
7. International collaborative work
8. Others planned - Network Monitoring Centre and INS Portal



1. Information and Network Security Policy for the Communications and Multimedia industry

- The security policy will address the role and responsibilities of licensees under the Communications and Multimedia Act 1998 to ensure information security and the integrity and reliability of the network. It will also act as a guide for other parties relevant to the communications and multimedia industry
- Audits will be in the future based on the policies.



2. Regulating SPAM

- The MCMC have developed an action plan to address the problem that Spam poses. The action plans are multi-prong, which includes raising awareness, management by the ISPs, promoting technological solutions and would require the cooperation of all major stakeholders namely, the industry, consumers, service providers, the regulators and the international community.



2. Regulating SPAM

- The MCMC is also working together with the Consumer Forum of Malaysia (CfM) (www.cfm.org.my) to develop the IASP sub-code on Spam. Apart from the IASP sub-code on Spam, the MCMC is also working with the CfM to develop the Mobile Operator sub-code on Mobile Spam i.e. "sms", "texts".



2. Regulating SPAM

- During the last ASEAN Telecommunications Regulators' Council (ATRC) Meeting in Cambodia, it was decided that Malaysia will facilitate the ATRC's initiatives on anti-Spam activities. Malaysia via the MCMC intends to facilitate this process by first taking stock of the current anti-Spam activities found in the ATRC economies. A workshop is also planned in Q1, 2005 to further assist ATRC economies to implement best practices to eradicate Spam.



2. Regulating SPAM

- The Malaysian Communications and Multimedia Commission (MCMC) also regularly monitors for the blockage of local IP addresses by bodies such as *Spamhaus* where local ISPs affected are advised to take remedial steps to remove themselves from the list.



3. The Information Sharing Forum (ISF) for Information and Network Security

- On June 22, 2004, the MCMC together with 7 major IASPs in Malaysia, namely TM Net, JARING, Time.Net, Celcom.Net, Maxis.Net, DiGi.Net and NTT MSC together with NISER, the ICT Security Division of MAMPU and the Malaysian Technical Standards Committee set up the Information Sharing Forum or "ISF" to allow the relevant stakeholders an avenue to share information, expertise and experiences for the better of the network infrastructure in Malaysia.



3. The Information Sharing Forum (ISF) for Information and Network Security

- The ISF meets every month and is chaired by the MCMC. It also hosts a newsgroup where members interact and debate on issues before an ISF meeting.



3. The ISF on SPAM

- The ISF, which also consist of Internet Service Providers (ISPs) in Malaysia, also shares a “white-list” of IP addresses together with a “black-list” of known spammers. Apart from the list, the ISF is also preparing technical guidelines and a compendium of best practices that will serve as an anti-Spam toolkit. We hope to develop it before the proposed ATRC workshop on SPAM in Q1, 2005.



4. Information and Network Security Audits

- The MCMC also undertakes to conduct Information and Network Security Audits on CMA licensees.
- The audits are based on internationally accepted information and network security standards such as the BS 7799 (MS ISO 17799) and known best practices.
- In 2003, Information and Network Security audits was performed on ISPs
- During the said ISP audit, the ISPs were also subjected to several penetration tests on their network.



4. Information and Network Security Audits

- To conclude, audits are essential to ensure that organizations are equipped to deal with any security incidents.

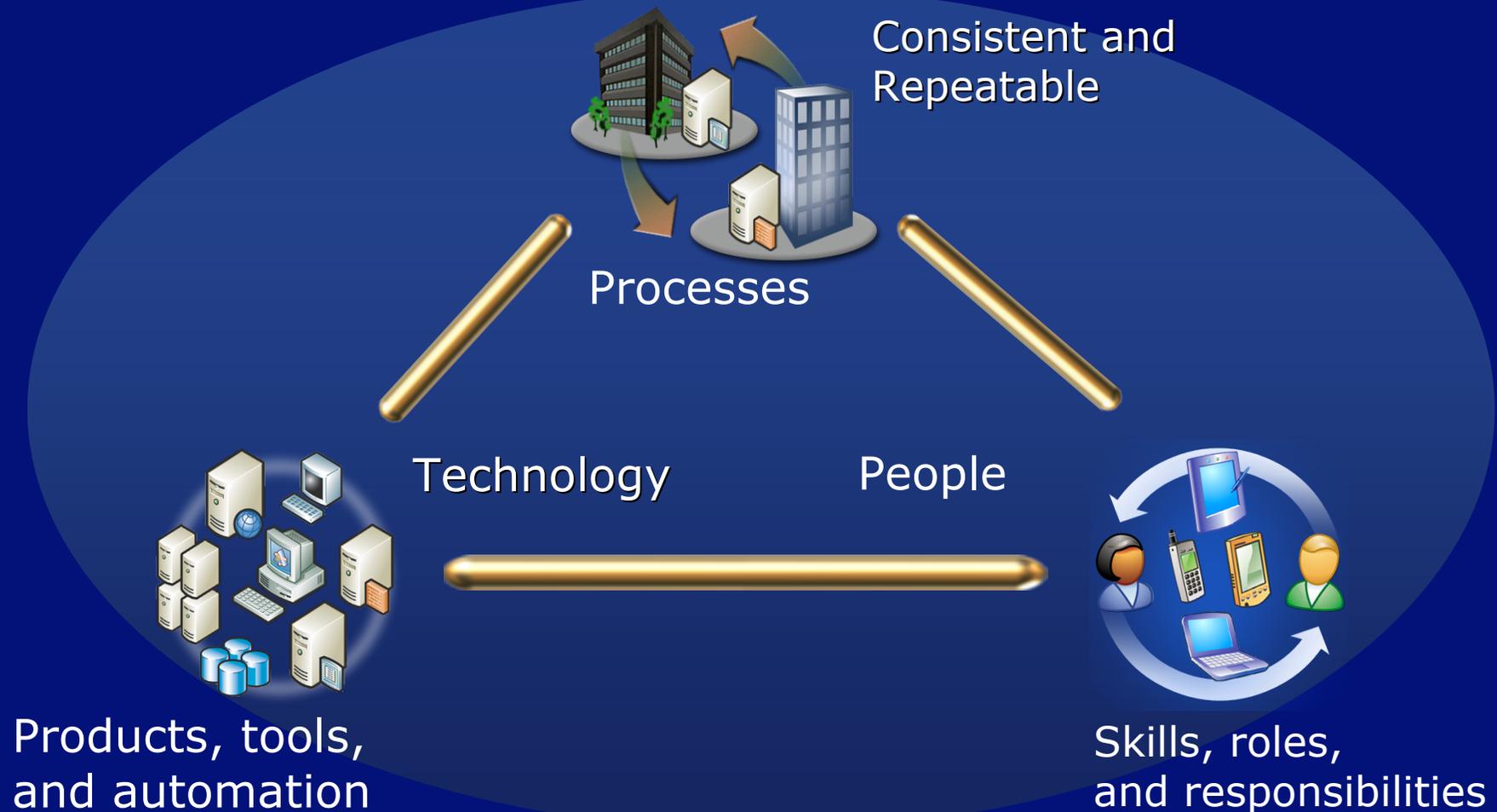


5. Awareness and Education

- Challenges continue to increase. Eradication of security incidents is not foreseen in the near future.
- End-users and consumers increasing.
- Awareness and education in Information and Network Security issues are critical to success.



5. Awareness and Education





5. Awareness and Education

- MCMC for the past 2 years have organized nationwide awareness programs on E-Security.
- The campaign is jointly held with the Consumer Forum of Malaysia (CfM) and other bodies such as the ICT Security Division of MAMPU, NISER and MSC Trustgate, a certification authority licensee.
- Brochures and pamphlets were distributed.
- Awareness program stressed the need for end-users to commit themselves towards best practices, positive use of the Internet and educating them of the avenues for them to lodge complaints, reports on any security incidents.



5. Awareness and Education

- A current project that the MCMC is presently working on, in collaboration with relevant information and network security experts is the “Information Network Security Compendium”.
- The compendium will consist of articles on matters relating to best practices and security know-how written by experts who will share their experiences.
- Once completed, the compendium will be made available to the general public hopefully by Q1, 2005



5. Awareness and Education

- The Information and Network Security Policy for the Communications and Multimedia industry will also call for the implementation of a “culture of security” within CMA licensees.
- Policies should be in place.
- Compliance towards policies must be asserted.
- Security policies as enabler and not as impediment to businesses.



6. Capacity Building

- Promotion of Information and Network Security Standards.
- Workshops and Training - organized by MCMC
- Talks and presentations to target groups
- Information and Network Security Certifications - CISSP, GIAC, GSEC etc - to be covered in the Information and Network Security Policy for the Communications and Multimedia industry.
- Need for knowledge users.



7. International Collaborative Work

- Lead ATRC's action-plan against SPAM;
- Working Group member in APEC TEL's E-Security Task Group on "Spy ware"
- Working Group member in APEC TEL's E-Security Task Group on "Wireless Security"
- Malaysia's lead representative at APEC TEL's E-Security Task Group meetings
- Malaysia's lead representative to the APEC TEL Cyber Crime meeting in Hanoi, August 2004



8. Other Plans

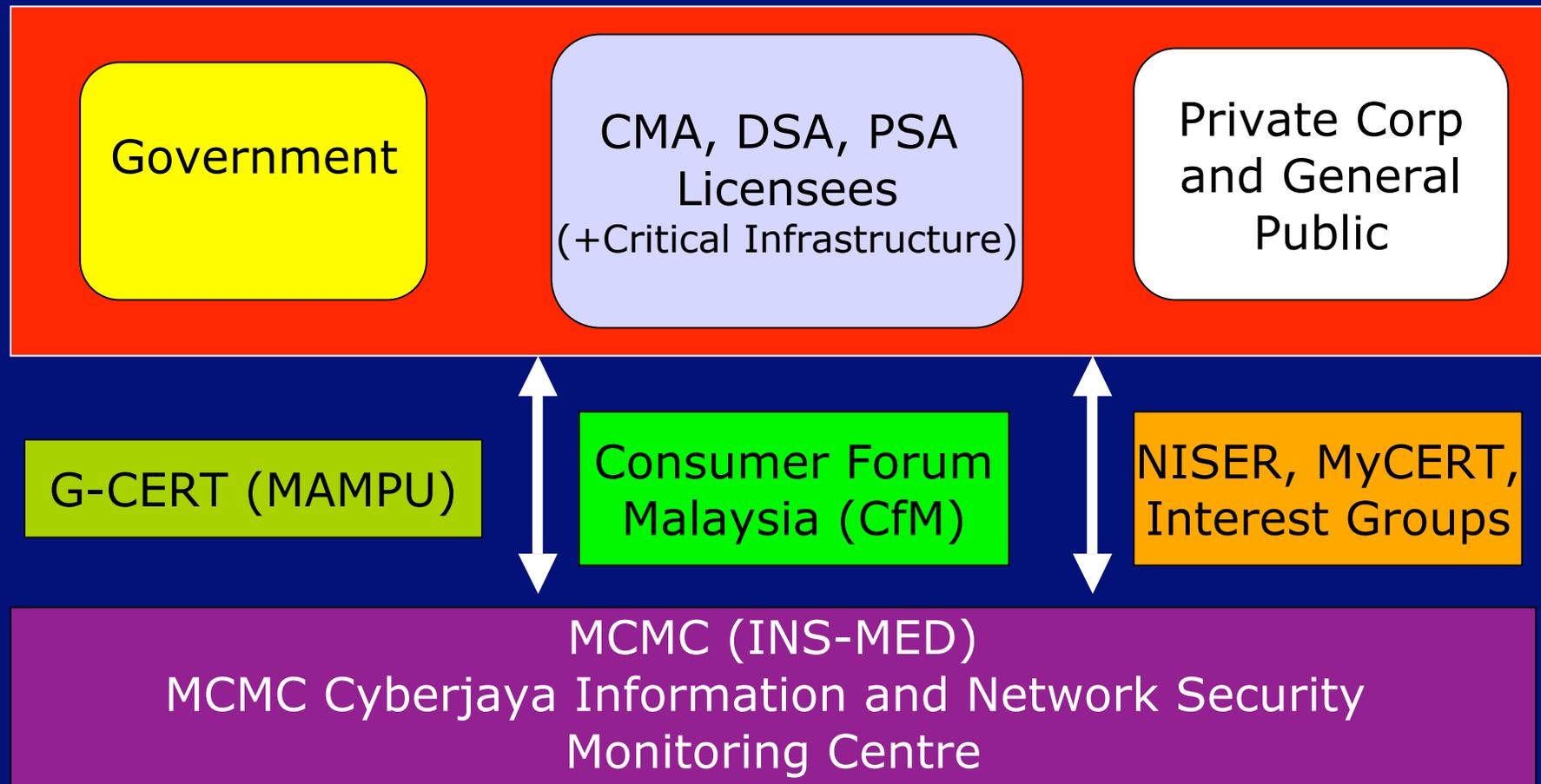
- Network Monitoring Centre (NMC)
 - This follows the example of countries such as Korea and Japan. It will not monitor activities of end-users but would function as an alerting and management tool to coordinate efforts with the relevant stakeholders such as ISPs in addressing security incidents over the network.
- Info Network Security Portal
 - The proposed portal will act as a one-stop information portal on Information and Network Security, initiatives by MCMC, how the general public, companies and stakeholders can play a role, advices, alerts, complaints etc.



D. Stakeholders in meeting the challenges



Information and Network Security Management in the Communications and Multimedia Industry





Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

Thank You

Malaysian Communications and
Multimedia Commission
63000 Cyberjaya, Selangor Darul Ehsan
MALAYSIA
www.mcmc.gov.my