An Agency Under

MOSTI

Promoting a Culture of Cybersecurity among *Critical National Information Infrastructure*

ITU Workshop, Doha,Qatar
February 18-21, 2008
By R.Azrina R.Othman
CyberSecurity Malaysia

Securing Our Cyberspace

Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Sharing Platform
- Cyber Security Exercise
- Way Forward

Cyber Threats are Real, Cyber Attacks Are Happening!

CyberSecurity MALAYSIA

Cyberspace must be part of everyone's life, says PM

By Tan Choe Choe and Wan Hamidi Hamid

MALACCA: Information and communications technology (ICT) is for everyone — from the office worker to the estate worker.

Prime Minister Datuk Seri Abdullah Ahmad Badawi said no category of Malaysians should be denied participation in the process of using ICT to turn the country into a developed nation.

"Whether you are an estate worker, a factory worker or a clerk, you have to participate in and help develop ICT for Malaysia to reach the status of a developed nation."

He said that all levels of society had to participate in ICT for Malaysia to compete with other countries in an era of globalisation.

Bebas tapi bertanggungjawab

Mukadimah

DATUK SERI DR. JAMALUDIN MOHD JARJIS

MINGGUAN: Sebagai Menteri yang diberikan tanggungjawab dan amanah

Sudah ada garis panduan seperti *Bill of*

Invest in cyber security, says expert

UTM hit by virus attacks

More than 6,000 computers infected

By MEERA VIJAYAN

Prof Zaruri Mohamad said the virus attacks were widespread which, in turn, makes our network slower."

Federal Prosecutor: Cybercrime Is Funding Organized Crime

CYBER WARS

Chinese hackers cyber-attacking British government networks

by Staff Writers
London (AFP) Sept 6, 2007

Chinese computer hackers are infiltrating British government networks, giving them access to secret information, according to media reports on Thursday.

The reports in The Times and The Independent newspapers come a day after US President George W. Bush said he may bring up the issue of suspected Chinese cyber-attacks on the US defence department in a meeting with China's President Hu Jintao.

cal control of actually re- d by hackers. e were about 150 million dwide, includ- es, offices and encies, which l by bot net- the mischief ntrollers could d launching -of-service at- computer re- able to users. so be used to vate informa- ne banking in-

formation, steal it and forward it to others.

"They can also use bot networks to shut things down. Imagine a country the size of Malaysia having its computer systems hijacked and used for criminal activity," he said.

Schmidt told the *New Straits Times* Malaysia did not suffer from a bad reputation thanks to good work by the government through agencies such as CyberSecurity Malaysia.

From an organisational perspective, he said Malaysia, was far ahead of many other countries in terms of cyber security.

TAIPEI TIMES

Published on Taipei Times
http://www.taipeitimes.com/News/taiwan/archives/2007/07/23/2003370881

DPP branches attacked by Chinese computer virus

By Rich Chang
STAFF REPORTER
Monday, Jul 23, 2007, Page 3

Securing Our Cyberspace

Recent Incident Of Cyber War Against A Nation

Cyber Attack on Estonia

- **Occurred in May 2007**
- **Estonia was under cyber attacks for 3 weeks**
- **Attack targeted government, banking, media and police websites**
- **Paralyzed internet communication.**
- **Attacks from 128 sources outside Estonia**
- **US and European countries aided Estonia in overcoming the cyber attacks**

Impact:

Huge economic losses incurred as online based transactions were disrupted

Cyber Attacks on Malaysia?

WHAT IF OUR CRITICAL INFRASTRUCTURE ARE UNDER ATTACK ?

ARE WE READY ?

HOW DO WE DEAL WITH IT ?

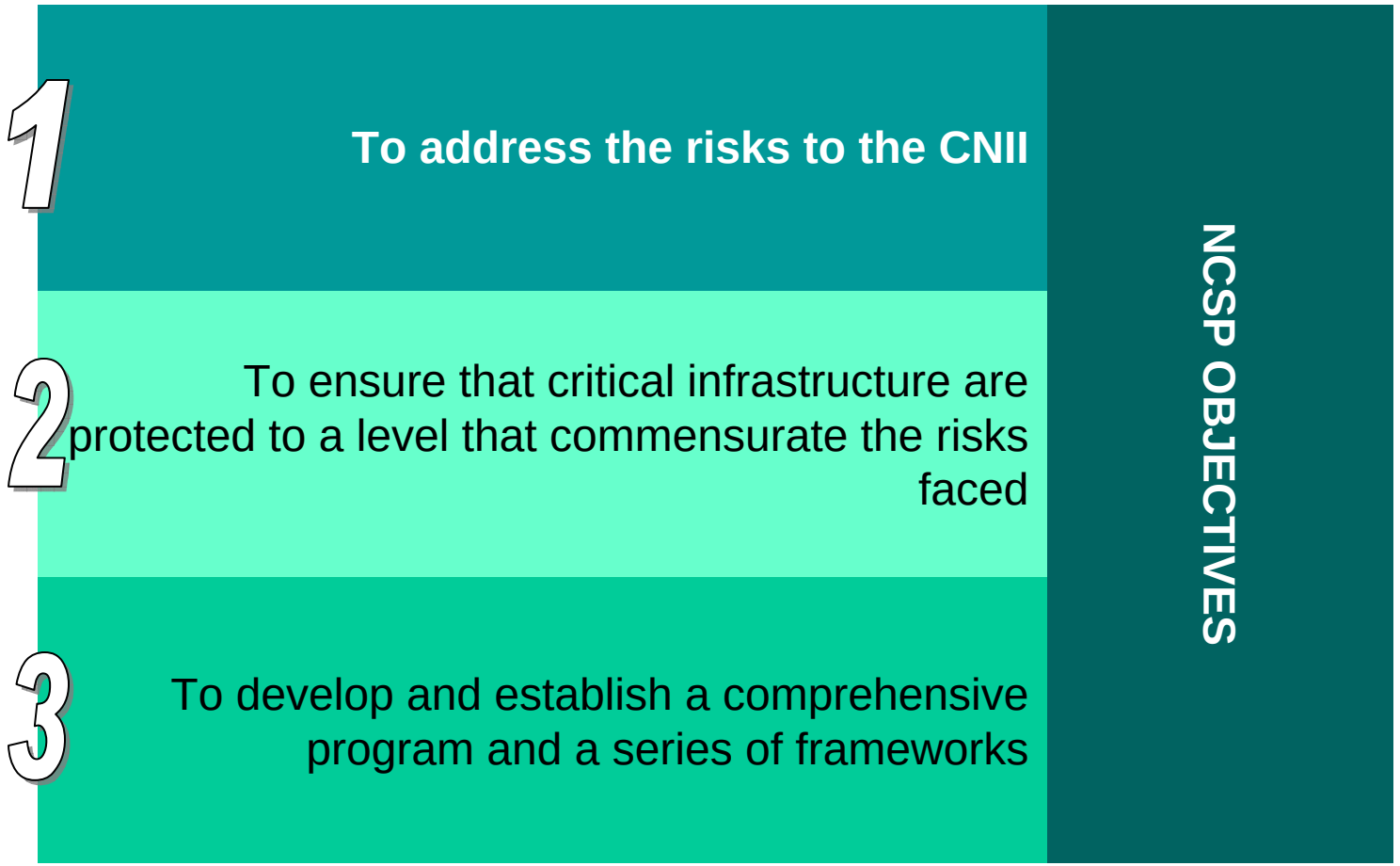
Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Platform
- Cyber Exercise
- Way Forward

Introduction to The National Cyber Security Policy

In 2006, **National Cyber Security Policy (NCSP)** was initiated by the Ministry of Science Technology and Innovation, to harness national effort to enhance the security of Malaysia's **Critical National Information Infrastructure (CNII)**

Objective of the National Cyber Security Policy



National Cyber Security Framework

Malaysia'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'

Establishment of a national info security coordination centre	Reduction of & increased in success in, the prosecution in cyber crime.	Expansion of national certification scheme for infosecmgmt & assurance	Reduced no. of InfoSec incidents through improved awareness & skill level	Acceptance & utilization of local developed info security products	Strengthen or include infosec enforcement role in all CNII regulatorsl	CNII resilience against cyber crime, terrorism, info warfare	International branding on CNII protection with improved awareness & skill level

NATIONAL CYBER SECURITY POLICY THRUST

PT 1 EFFECTIVE GOVERNANCE	PT 2 LEGISLATIVE & REGULATORY FRAMEWORK	PT 3 CYBER SECURITY TECHNOLOGY FRAMEWORK	PT 4 CULTURE OF SECURITY & CAPACITY BUILDING	PT 5 RESEARCH & DEVELOPMENT TOWARDS SELF RELIANCE	PT 6 COMPLIANCE & ENFORCEMENT	PT 7 CYBER SECURITY EMERGENCY READINESS	PT 8 INTERNATIONAL COOPERATION
Framework for high level decision making body	Framework adopted as baseline for addressing legal issues	Framework as baseline for formulating Infosec requirement	Addressing the Human element	Need coordinator to develop roadmap for research	Identify baseline standards & risk assessment framework	Have proper emergency response mechanism in place	Identify & coordinate international platform

NCSP's Policy Thrust 4: Culture of Security & Capacity Building

- Develop, foster and maintain a national culture of security
- Standardise and coordinate cyber security awareness and education programmes across all elements of the CNII
- Establish an effective mechanism for cyber security knowledge dissemination at the national level
- Identify minimum requirements and qualifications for information security professionals

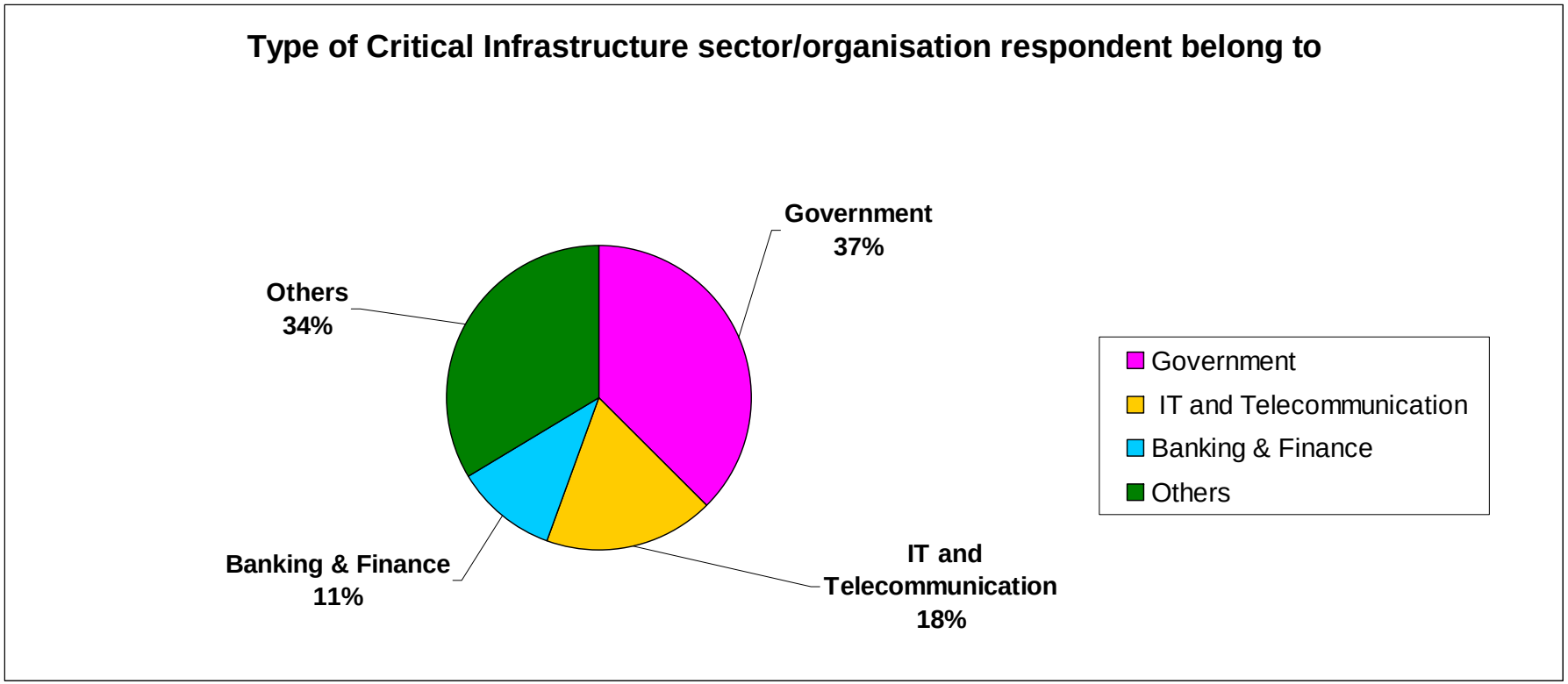
Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Platform
- Cyber Exercise
- Way Forward

Survey 2007 among CNII Organisations - By Sector

The Conference was targeted at participants from GLCs and CNII organisation, the largest number of turnout is from government linked companies. *Aug 29, 2007*

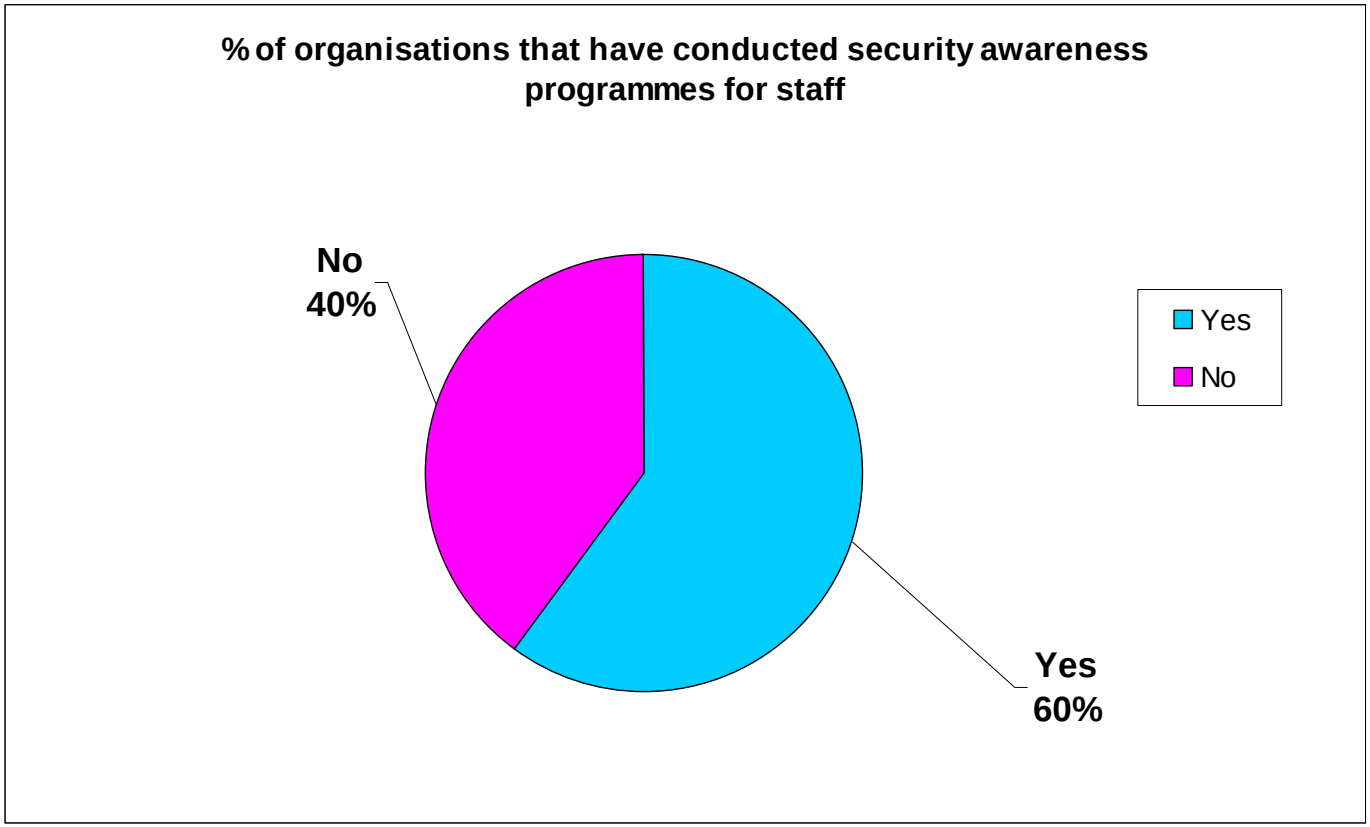
Total of about 100 respondents



Note: CNII - Critical National Information Infrastructure

Does your organisation conduct cyber security awareness programme for all staff?

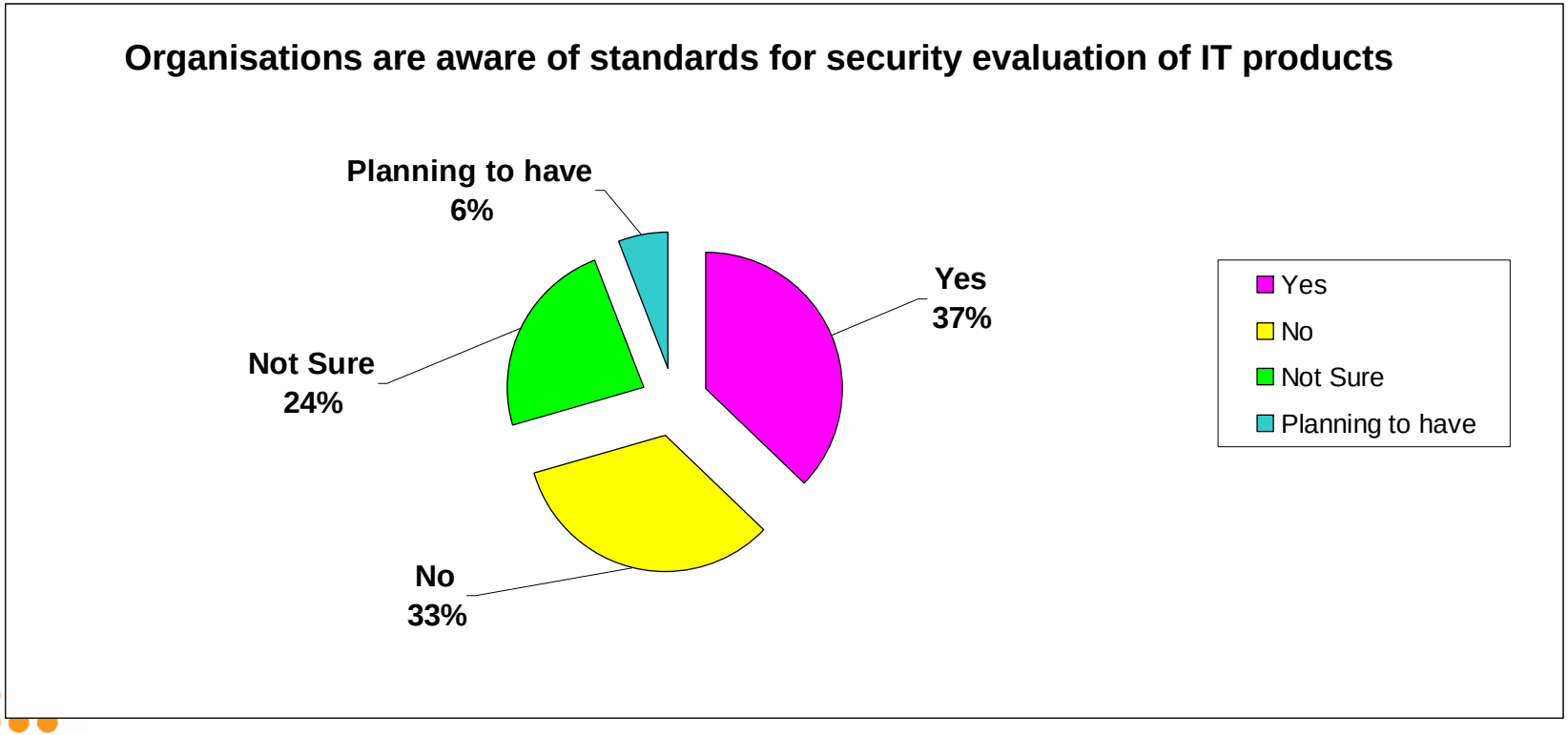
60% of respondents has conducted some form of cyber security awareness programme for staffs.



Survey 2007 among CNII Organisations - Guidelines for Evaluation of IT Products

Do you know that there is a standard guideline (ISO/IEC 15408 Common Criteria for IT Security Evaluation) that can be used to request, develop and evaluate secure IT products?

One third of the respondents are aware that there is such standard guideline to evaluate IT products.



Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Sharing Platform
- Cyber Exercise
- Way Forward

Let's Make The Internet A Safer Place
www.esecurity.org.my

Outreach Program

CyberSecurity MALAYSIA

CYBER SECURITY AND INTERNET SAFETY AWARENESS CAMPAIGN

Content Partners

- MIMOS
- Microsoft
- ChildNet
- enisa
- MDEC

International CERT Communities

Other industry partners

Content Localization & Packaging

CyberSecurity MALAYSIA

MOSTI

Content Channels

- KTAK
- MOHE
- MOE
- KPWKM
- MOI
- MDEC

Target Audience

Children / students

Parents/ home users

Organizations

Competency Development Programs

- Promote various platforms for engagement sessions
  - Seminars, forums & roundtable (e.g. ***Infosec.my*** conducted quarterly)
  - Demos and talks to specific critical sectors
  - Focus group mailing lists discussions
- Encourage hands-on participation
  - Hands-on Workshops
  - Cyber Exercises
  - Expert Lab
- Promote Information Security Professional Certifications

Portal for Critical National Information Infrastructure (CNII)

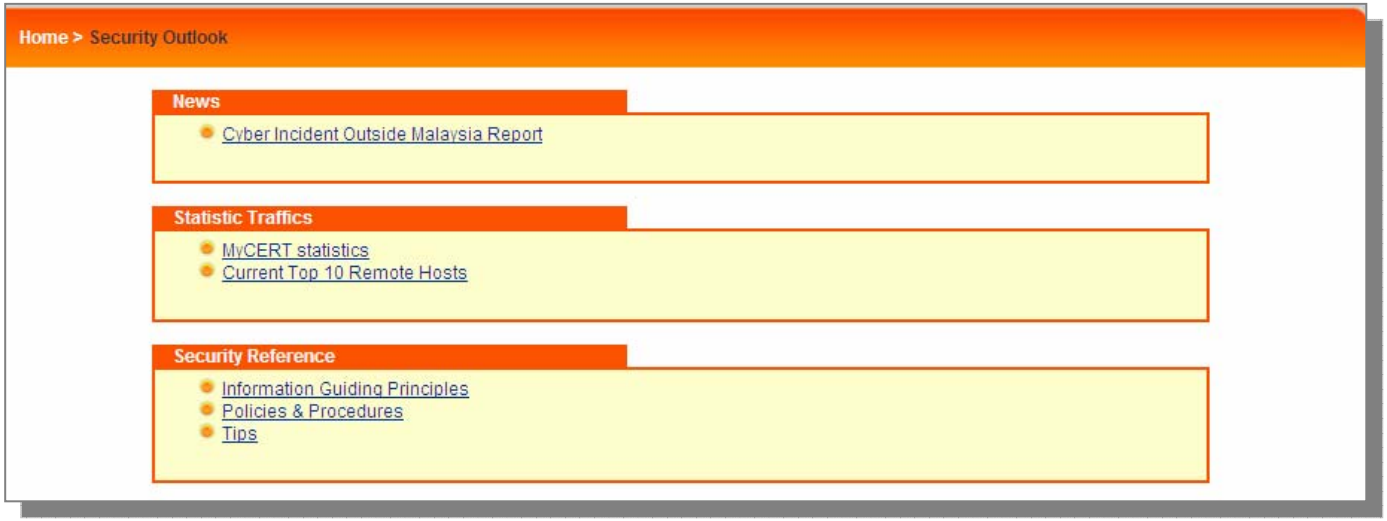
- **The CNII Portal is a security resource portal designed specifically to meet the needs of security practitioners (management & technical) within Critical National Information Infrastructure organisation.**

- **Platform to share guidelines and best practice among CNII, across sector**

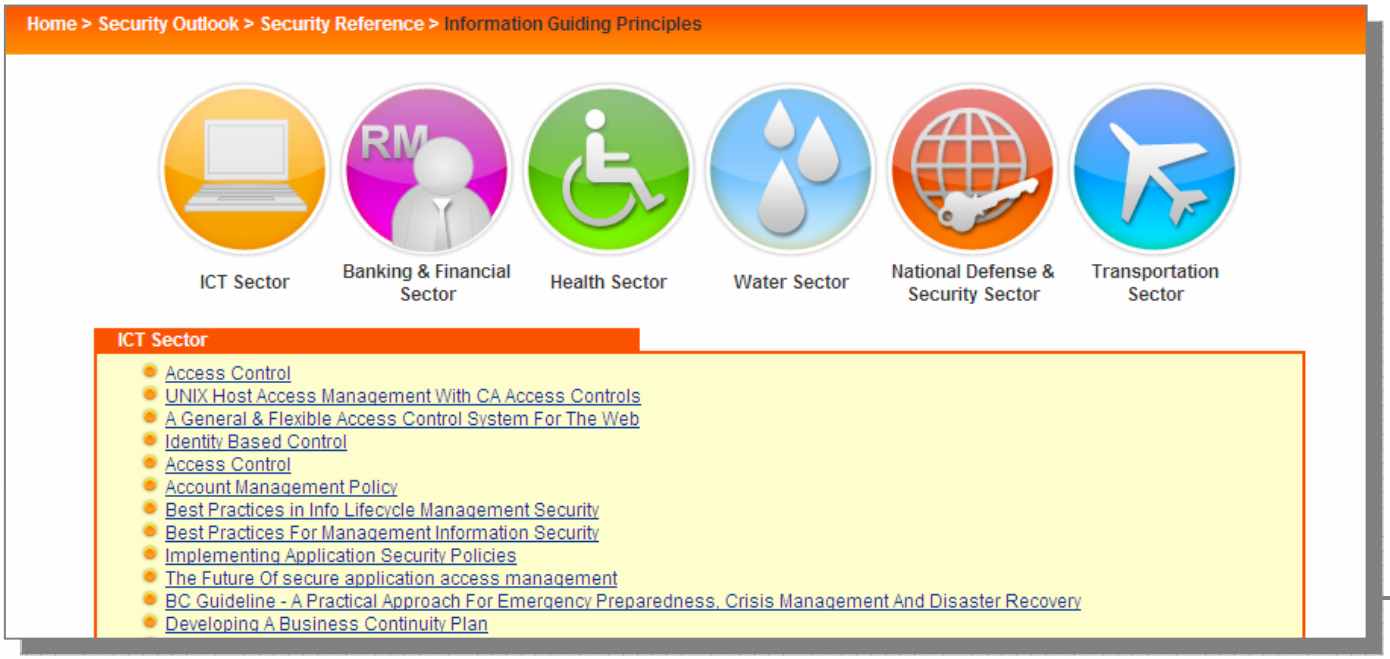
- **Provide latest news on information security and security advisories**

Customized contents for Management & Technical security practitioners

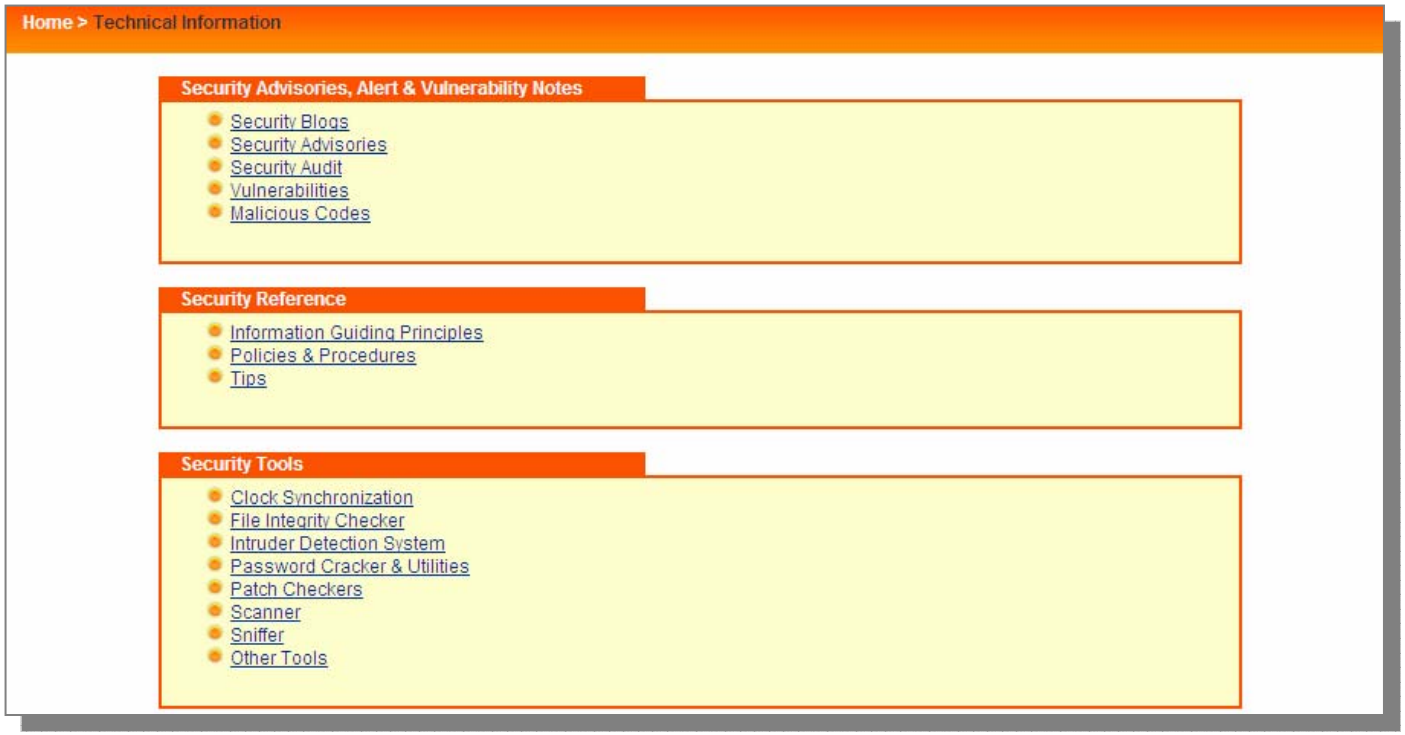
Front page.



Security Outlook page for Managers, CIO, CISO.



Information Guiding Principles page.



Technical Information page for System Administrators, Developer.

Tips page.

Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Sharing Platform
- Cyber Exercise
- Way Forward

Malaysian Incident Handling Drill @MyDrill 2007

- **Conducted on 22nd Nov 2007 by CyberSecurity Malaysia**

- **Participated by a total of 6 teams**
  - **3 ISPs**
  - **1 Antivirus Vendor**
  - **1 Domain Registrar**
  - **CyberSecurity Malaysia**

High level Objectives

- Prepare for potential cyber-security activity related to the Global event such as Beijing 2008 Olympic Games

- Provide different levels of exercise to suit the needs of the various local teams

- Provide an exercise that can be effectively coordinated by the volunteer exercise control group (EXCON)

- Meet the other high-level objectives within the short timeframe available for the drill.

Drill Scenario Background

Inject 1 – Domain Registrar received report that there's a C&C hosted outside Malaysia using a local domain mylovelybot.my. Request to take down domain

Domain Registrar scenario

Inject 2 - Received report of DDoS targeting udp/random port number attacking their DNS.

Malware .exe

Inject 1 – Antivirus Vendor received report from MyCERT involving thousands of PCs from Malaysia infected by a new malware.

Removal & Advisories

Anti-virus vendor scenario

Inject 1 - Report from home user informing of slowness in accessing Beijing Olympic website.

Inject 2 - Website no longer accessible, further investigation shows > than 10,000 IP originating from Malaysia accessing the website, suspected botnet infected.

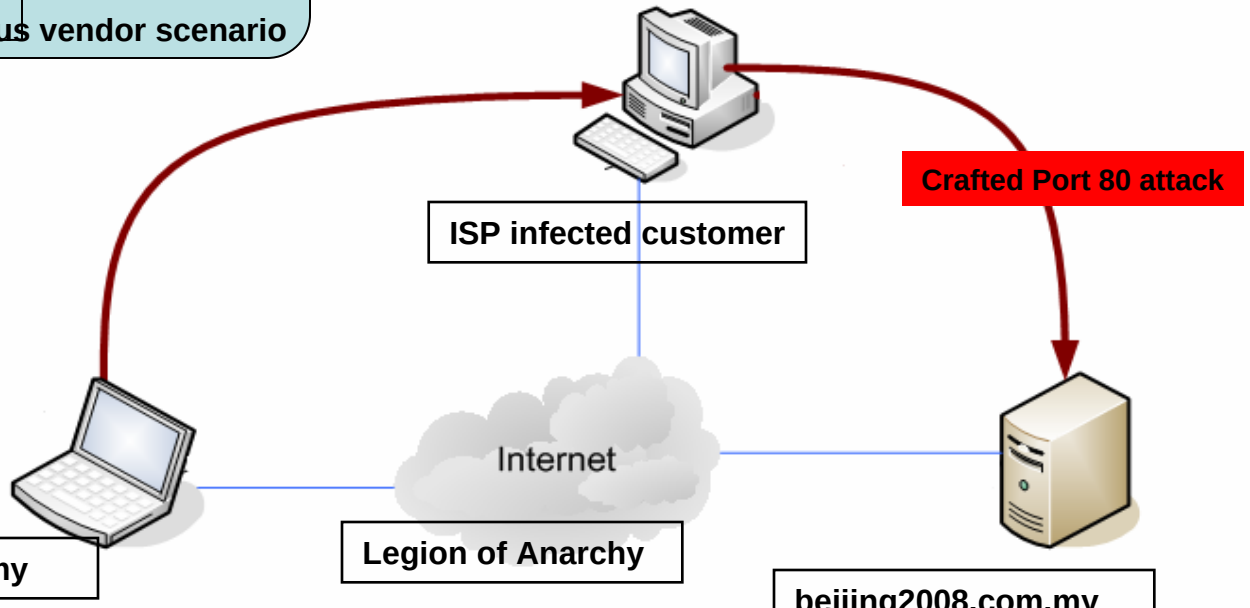
Inject 3 - ISP received malware analysis report from AV vendor (malware infecting their user's PC – bot) containing several critical information i.e.C&C host domain (mylovelybot.my)

ISP scenario

Inject 1 – Input from MyCERT and to produce press release on attack

Press Release

Public Relations scenario



Way Forward

- Innovate and generate materials relevant for the target audience
- Expand partnership with key stakeholders to reach out to target users.
- Device suitable platforms for information sharing among ICT & Information Security practitioners
- Assess effectiveness

An agency under:
Ministry of Science, Technology & Innovation

Postal Address :
CyberSecurity Malaysia (formerly known as NISER),
Level 7, SAPURA @ MINES,
7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan,
Malaysia.

Office Hours : Monday - Friday 08:30 - 17:30 MYT
(Note: Not operational every Saturday and Sunday)

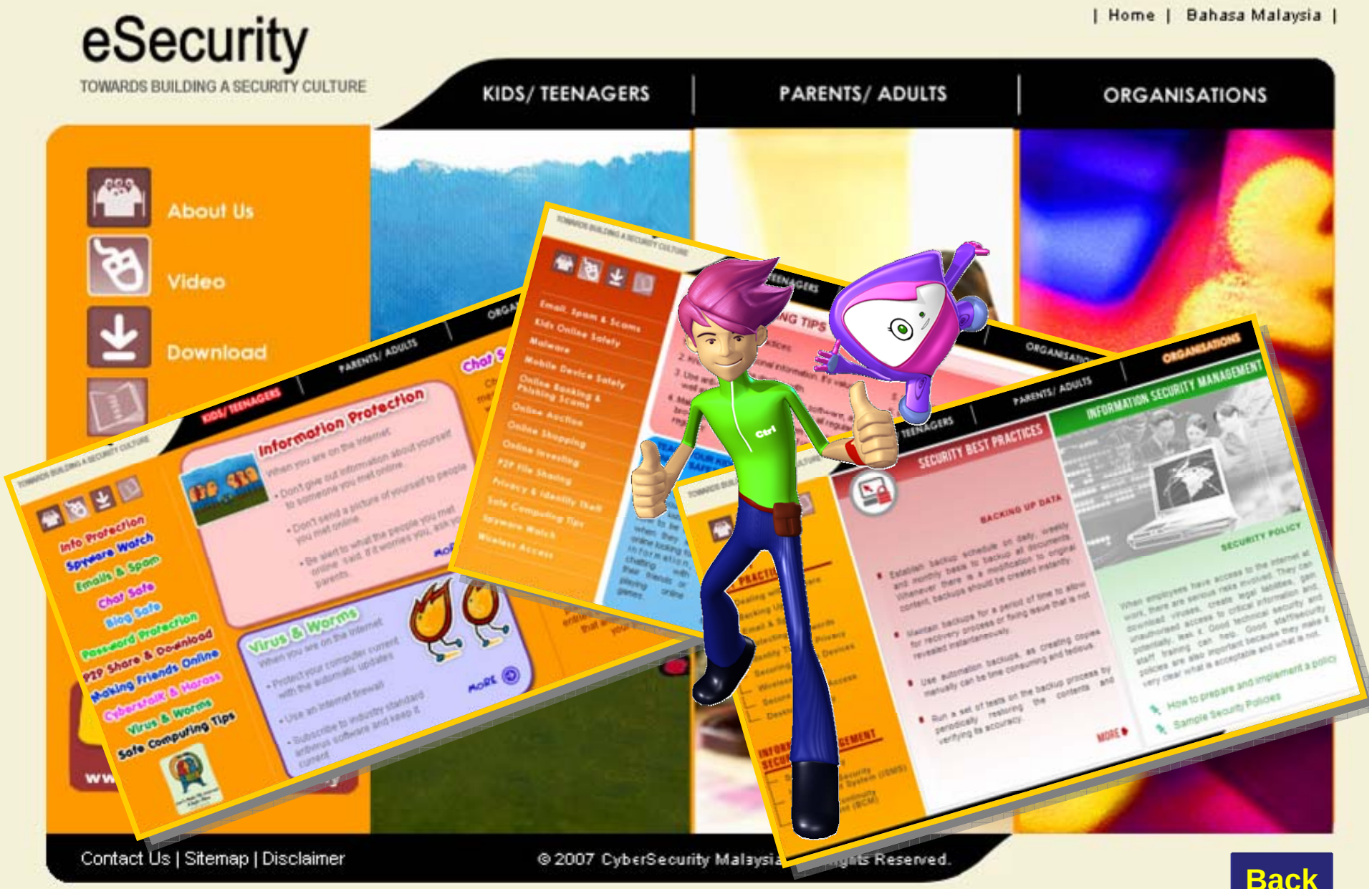
Phone : +603 - 8992 6888

Fax : +603 - 8945 3250

Email : *info [at] cybersecurity.org.my*

Map : Click here to download CyberSecurity Malaysia location map.

Awareness Portal – www.esecurity.org.my

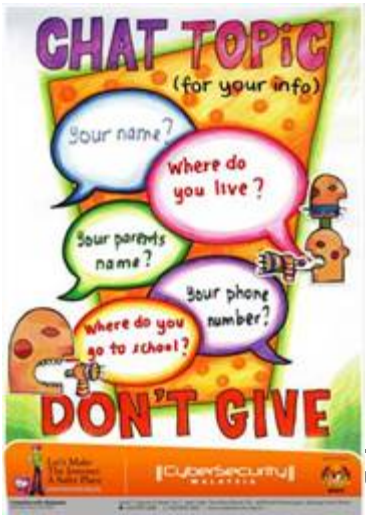


Back

Awareness Posters

(schools, public & organisations)

Back



Awareness Videos

Email & Spam

Safe Chatting

Safe Internet Banking

Cyber Stalking

Back