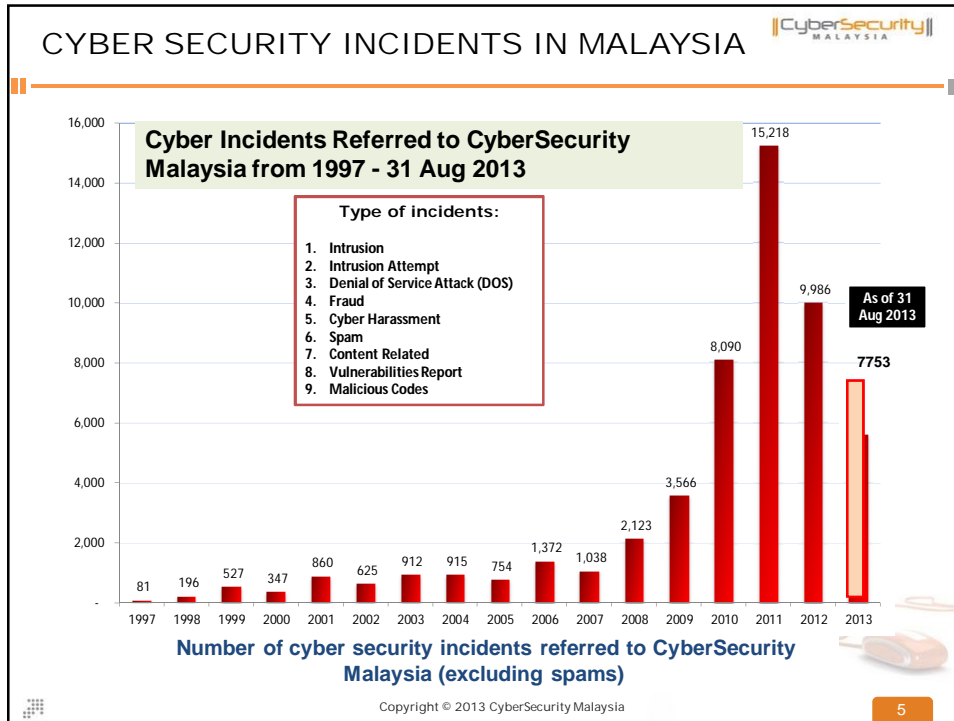


CYBER THREATS TARGETING AT VARIOUS LEVELS				
STRATEGIC LEVEL Act of aggression / hostile actions by state, organization and state-sponsored actors. - Well planned, sophisticated and complex	War of Perception -Cyber Propaganda	Cyber Terrorism	Cyber War	Hacktivism
		Political Cyber Espionage	Economic Cyber Espionage	Military Cyber Espionage
MIDDLE LEVEL - sophisticated and may serve initial steps for strategic attacks	Botnet	Distributed Denial of Service (DDoS)	Advance Persistence Threats (APTs)	Malware
OPERATIONAL LEVEL Targeting individuals and groups - Low level skills	Cyber Bullying	Online Gambling	Phishing -ID Theft	Denial of Service
	Defamation	Malware/Virus Infection	Pornography	Identity Theft
	IPR Infringement	Money Laundering	Sedition	Cyber Fraud
	Internet Mule	Cyber Stalking	Love Scam	Cyber Stalking



CATEGORIES OF CYBER THREATS - Malaysia's perspectives CyberSecurity MALAYSIA

Technology Related Threats

Hacking

Fraud

Malicious Software

Denial of Service Attack

Espionage

Issues

Cross-Border Investigation & Evidential Matters

International Collaboration

International Laws

Sedition

Defamation

Chat, Forum & Electronic

Pornography

Online Gambling

CyberSecurity MALAYSIA 6

Copyright © 2013 CyberSecurity Malaysia

CyberSecurity MALAYSIA

HUMAN IS THE WEAKEST LINK

WOMAN FALLS VICTIM TO IDENTITY THEFT

Monday January 17, 2011

Beware the Facebook felons
By P. ARUNA
aruna@theastar.com.my

Beware of phishing websites
KUALA LUMPUR: Members of the public are reminded to beware of fake websites used to conduct phishing. Because the fake website copies the website's appearance.

Credit Card

Copyright © 2013 CyberSecurityMalaysia

7

CyberSecurity MALAYSIA

CAPACITY BUILDING TO STRENGTHEN CYBER SECURITY

Copyright © 2013 CyberSecurityMalaysia

8

CyberSecurity MALAYSIA

THE COUNCIL FOR SECURITY COOPERATION IN ASIA PACIFIC (CSCAP) MEMORANDUM NO.20

CSCAP Memorandum No.20 tabled at ARF in May 2012 recommends that at the level of regional cooperation, the ASEAN Regional Forum should:

Implement **capacity building and technical assistance measures**. Priority should be given on developing a program of advice, training and technical assistance that strengthens the cyber security capacity, including capability of crisis management of all states.

Copyright © 2013 CyberSecurity Malaysia 9

CyberSecurity MALAYSIA

CAPACITY BUILDING - Malaysia's Initiatives

National Cyber Security Policy – Policy Thrusts

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 infosec mgmt & 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 regulators	CNII resilience against cyber crime, terrorism, info warfare	International branding on CNII protection with improved awareness & skill level
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
Ministry of Science, Technology & Innovation	Attorney General's Office	Ministry of Science, Technology & Innovation	Ministry of Science, Technology & Innovation	Ministry of Science, Technology & Innovation	Ministry of Information, Communication & Culture	National Security Council	Ministry of Information, Communication & Culture

PT – Policy Thrust 10


Copyright © 2013 CyberSecurity Malaysia

CyberSecurity
MALAYSIA


CAPACITY BUILDING - Malaysia's Initiatives




InfoSecurity Professional Development & Outreach

InfoSecurity Professional Development



Outreach



		
<p>Provides competency and professional Training programs</p>	<p>Develops curriculum in cyber security for colleges, polytechnics and universities to build expertise in cyber security with MOE</p>	<p>Collaboration between CyberSecurity Malaysia and Institute of Higher Learning (IHL) in various comprehensive cyber security modules</p>

Malaysia emphasizes on the importance of capacity building


- as of Dec 2012 – **3045 professionals**.
- targeted ratio of **1:2000 in 2020** with- required number of **17,026 professionals**
(based on estimated population population increment rate **1.8% per year**)
- to nurture about **1748** information security professionals yearly

Copyright © 2013 CyberSecurity Malaysia

11

CyberSecurity
MALAYSIA

NATIONAL STRATEGY FOR CYBER SECURITY ACCULTURATION & CAPACITY BUILDING PROGRAM

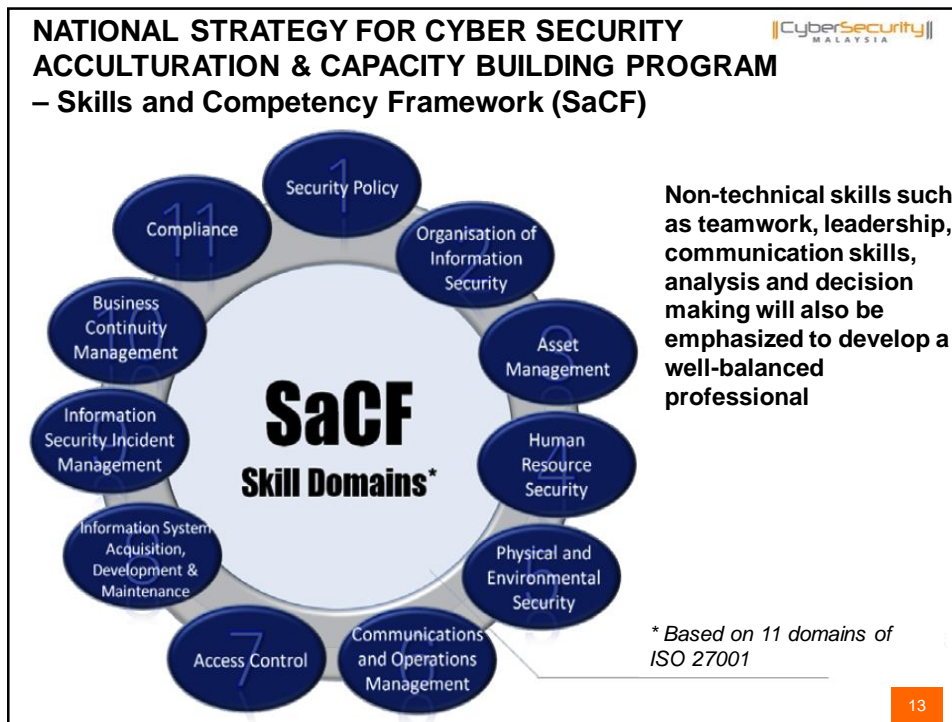


The study was completed in November 2010

- The capacity building programs are targeted towards **Critical National Information Infrastructure (CNII)** and the **Malaysian society** at all levels
- Focusing on efforts to **increase the knowledge and skill sets** on the information security workforce
- Aimed at creating a **quality and well-equipped information security workforce** and **promoting recognition** of the Information Security profession.

Copyright © 2013 CyberSecurity Malaysia

12



THE GUIDELINE TO DETERMINE INFORMATION SECURITY PROFESSIONALS REQUIREMENTS FOR THE CNII AGENCIES / ORGANIZATIONS

- Developed in May 2013
- To provide a guideline when:
 - CNII agency / organization wishes to set up a team of Information Security Professionals
 - CNII agency / organization wishes to assess the adequacy of its current Information Security Professionals
- Three areas of the Information Security Professional requirements that a CNII agency/organization should address:
 - Roles & Responsibilities of Information Security Professionals
 - Competency of Information Security Professionals
 - Minimum number of Information Security Professionals

Copyright © 2013 CyberSecurity Malaysia

14

CyberSecurity
MALAYSIA

THE GUIDELINE TO DETERMINE INFORMATION SECURITY PROFESSIONALS REQUIREMENTS FOR THE CNII AGENCIES / ORGANIZATIONS

- Information Security Professional Requirements

Copyright © 2013 CyberSecurityMalaysia

15

LIST OF CERTIFICATIONS

Management related certifications

- ISACA[®] Certified Information Security Manager (CISM)
- ISACA[®] Certified Information Systems Auditor (CISA)
- (ISC)²[®] Certified Information Systems Security Professional (CISSP)
- (ISC)²[®] Information Systems Security Management Professional (CISSP-ISSMP)

Technical related certifications

- CERT[®]-Certified Computer Security Incident Handler (CSIH)
- Certified Wireless Network Professional (CWNP[®]) - Certified Wireless Network Administrator (CWNA)
- Certified Wireless Network Professional (CWNP[®]) - Certified Wireless Network Security Professional (CWSP)
- CompTIA[®] Advanced Security Practitioner (CASP)
- CompTIA[®] A+ CE
- CompTIA[®] Network+ CE
- CompTIA[®] Security+ CE
- Critical Infrastructure Institute (CII) - Professional Critical Infrastructure Professional (PCIP)
- DRI International - Associate Business Continuity Professional (ABCP)
- DRI International - Certified Business Continuity Professional (CBCP)
- EC-Council - Computer Hacking Forensic Investigator (CHFI)
- EC-Council - Certified Ethical Hacker (CEH)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Forensic Examiner (GCFE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCI/A)
- GIAC Security Leadership (GSLC)
- GIAC Information Security Fundamentals (GISF)
- ISACA[®] Certified Information Systems Auditor (CISA)
- (ISC)²[®] Certified Authorization Professional (CAP)
- (ISC)²[®] Systems Security Certified Practitioner (SSCP)
- (ISC)²[®] Certified Information Systems Security Professional (CISSP)
- (ISC)²[®] Information Systems Security Engineering Professional (CISSP-ISSMP)
- (ISC)²[®] Information Systems Security Architecture Professional (CISSP-ISSAP)
- (ISC)²[®] Information Systems Security Engineering Professional (CISSP-ISSEP)
- ISO/IEC 27001 Certified Lead Auditor
- ITIL[®] Intermediate Certificate: Operation Support & Analysis (OSA)
- MILE2[®] Certified Penetration Testing Engineer

16

PORTAL FOR INFORMATION SECURITY PROFESSIONALS

CYBERGURU
INFORMATION SECURITY PROFESSIONAL TRAINING

Brought to you by


 An agency under MOSTI
 Ministry of Science, Technology and Innovation

Home About Us Courses Instructor Calendar Download Facilities Gallery

Cyberguru is the **new-gen portal** to surf all the happenings and professional development in **Information Security**

MEMBER OF MALAYSIAN INFORMATION SECURITY PROFESSIONAL (MISP)
[REGISTER NOW](#)


OUR CLIENTS

TALENT INCUBATION

<https://www.cyberguru.my/cybersec/>
 Copyright © 2013 CyberSecurity Malaysia

17

MALAYSIA'S INITIATIVES - OIC CERT



56 OIC Members
 MALAYSIA is the CHAIR
 OIC-CERT

Collaborate with Islamic Development Bank in providing training to OIC-CERT members in cyber security

OIC-CERT WAY FORWARD
 Public Private Partnership through an alliance Platform to raise capability & readiness of nations and achieve common grounds

GCSA
 (Global Cyber Security Alliance)

EDUCATION & OUTREACH

PROFESSIONAL TRAINING

WEALTH CREATION SOLUTIONS

TO BE AT PAR WITH INTERNATIONAL STANDARDS & BEST PRACTICES


Copyright © 2013 CyberSecurity Malaysia

18

MALAYSIA'S INITIATIVES
- Cyber Crisis Handling Exercises

Regional Cyber Drill
- using our experiences in coordinating the annual Asia Pacific Computer Emergency Response Team Cyber Exercise (APCERT)

Domestic Cyber Drill (X-Maya)
- exercising high-level of national preparedness for cyber crisis involving Government & critical sectors under the coordination of National Security Council




Copyright © 2013 CyberSecurityMalaysia

19

CONCLUSION

- Malaysia gives emphasis on human factor
– the key asset to strengthen domestic cyber security
- Malaysia continues to adopt evolutionary and innovative approach in capacity building program
- As part of regional community, Malaysia's efforts in capacity building is also to strengthen regional cyber security
- Regional states to collaborate and combine ideas to stay ahead of rapidly changing cyber threats



Copyright © 2013 CyberSecurityMalaysia

20



Thank you

Corporate Office

CyberSecurity Malaysia,
Level 5, Sapura@Mines
No. 7 Jalan Tasek
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888
F : +603 8945 3205
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

Northern Regional Office

Level 19, Perak Techno-Trade Centre
Bandar Meru Raya, Off Jalan Jelapang
30020 Ipoh, Perak Darul Ridzuan, Malaysia

T: +605 528 2088
F: +605 528 1905

 www.facebook.com/CyberSecurityMalaysia

 twitter.com/cybersecuritymy

 www.youtube.com/cybersecuritymy



Copyright © 2013 CyberSecurity Malaysia

21