

## EVOLUTION OF SECURITY INCIDENT RESPONSE TEAMS

*COLLABORATION OF COMPUTER EMERGENCY RESPONSE TEAM AMONG THE  
OIC MEMBER COUNTRIES*

**ORGANISATION OF THE ISLAMIC CONFERENCE - COMPUTER EMERGENCY RESPONSE TEAMS  
OIC-CERT**

**ABDUL-HAKEEM B. D. AJIJOLA**

Executive Partner

Consultancy Support Services (CS2) Limited

[info@consultancyss.com](mailto:info@consultancyss.com)

Sunday, 30 May 2010

LIKE IT OR NOT ...

# The ICT has changed our lifestyle



**E-Commerce**



**Online games**



**E-Government**



**Email / P2P**



**Mobile banking**



**Chatting / Blogging  
/ Cyber Media**



**Online banking /  
investment**

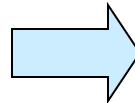


**Social networking sites**

# Cyber Threats Are Changing



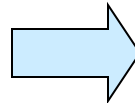
**Large scale, wide spreading incident (e.g. virus, worm outbreak)**



**Specific targeted attack, powerful tool (e.g. Botnet)**



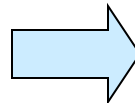
**Script kiddies, crackers**



**Professionals, Criminals**

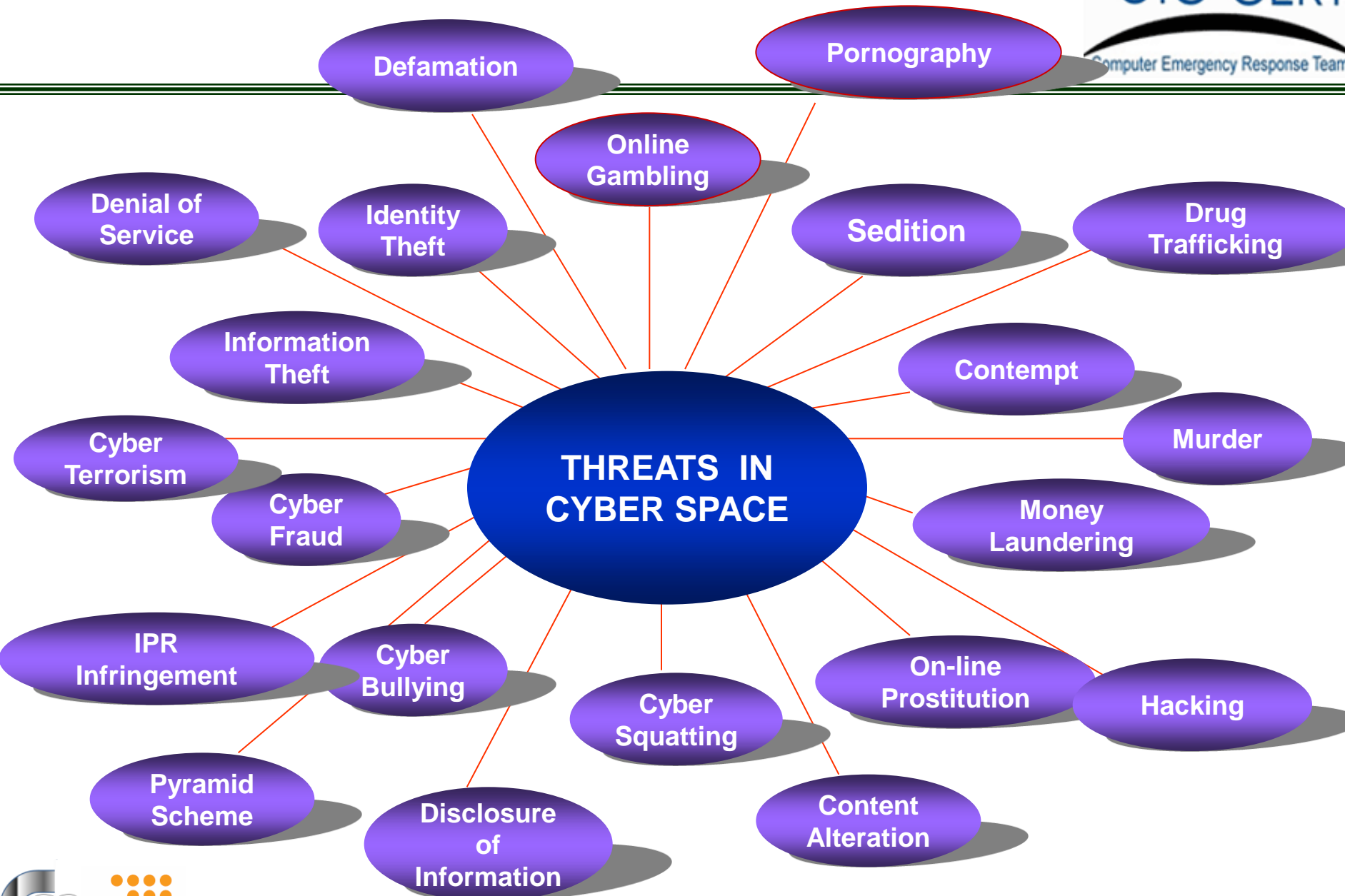


**Motivation: for fun, peer recognition, prestige**



**Specific Motivation: for economic gain, industrial espionage, cyber terrorism**



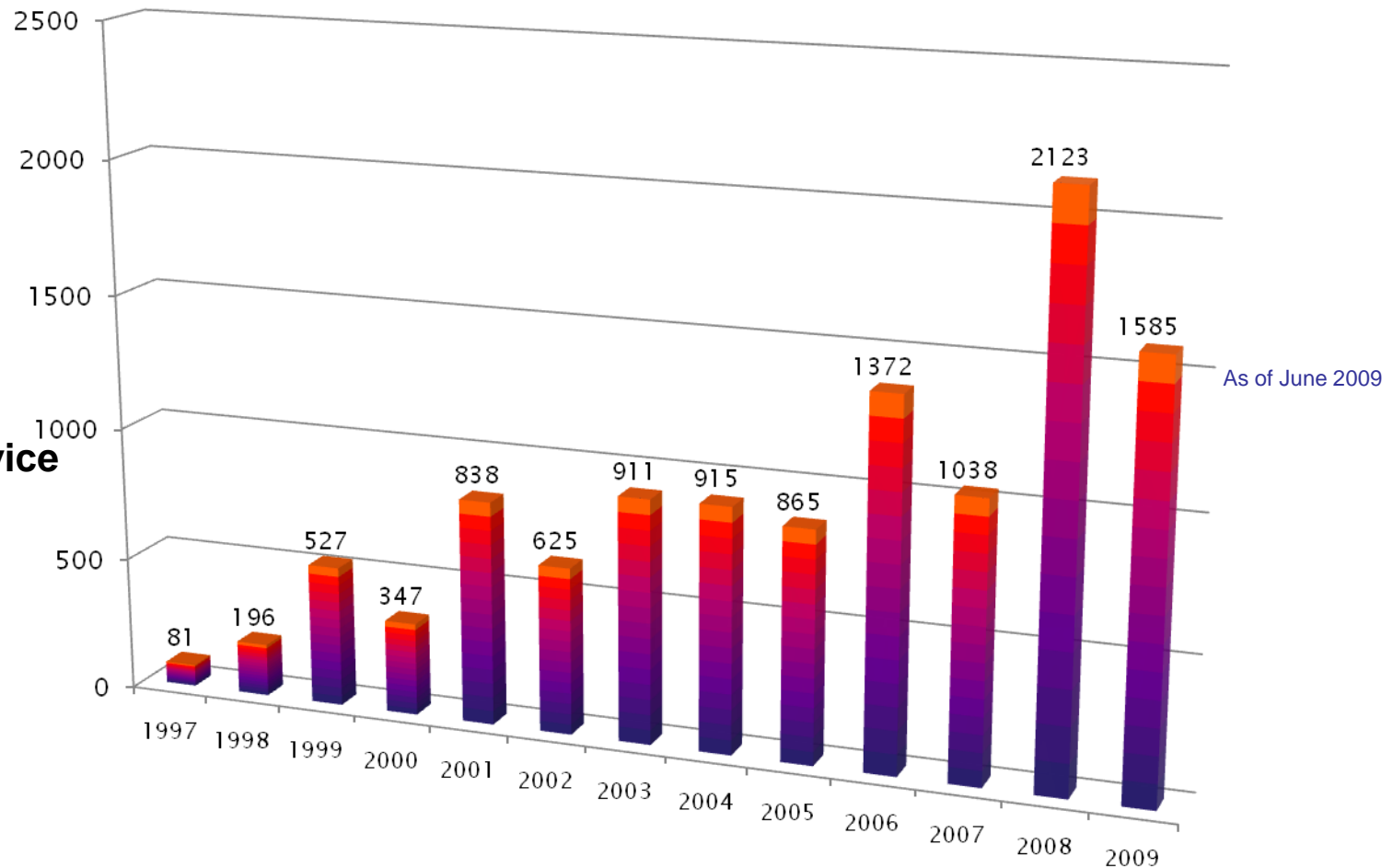


# CYBER SECURITY INCIDENTS (1997-2009) - Malaysia

- A total of 11,423 security incidents were referred since 1997 (excluding spam)

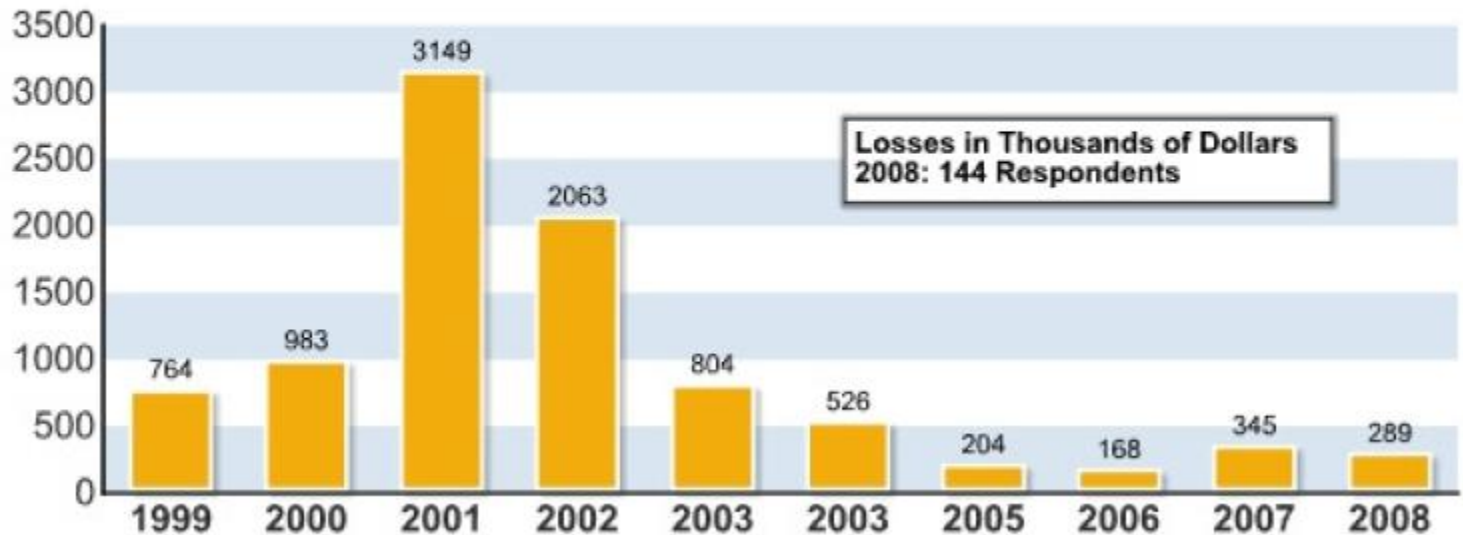
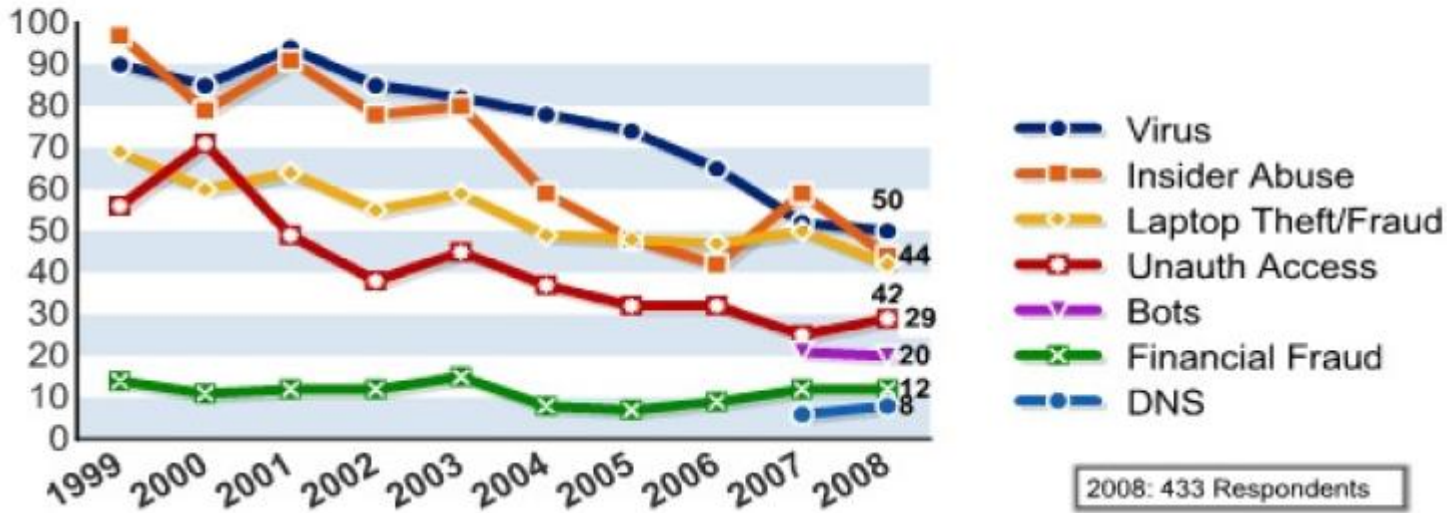
## Type of incidents:

- Intrusion
- Destruction
- Denial-of-Service
- Virus
- Hack Threat
- Forgery
- Harassment

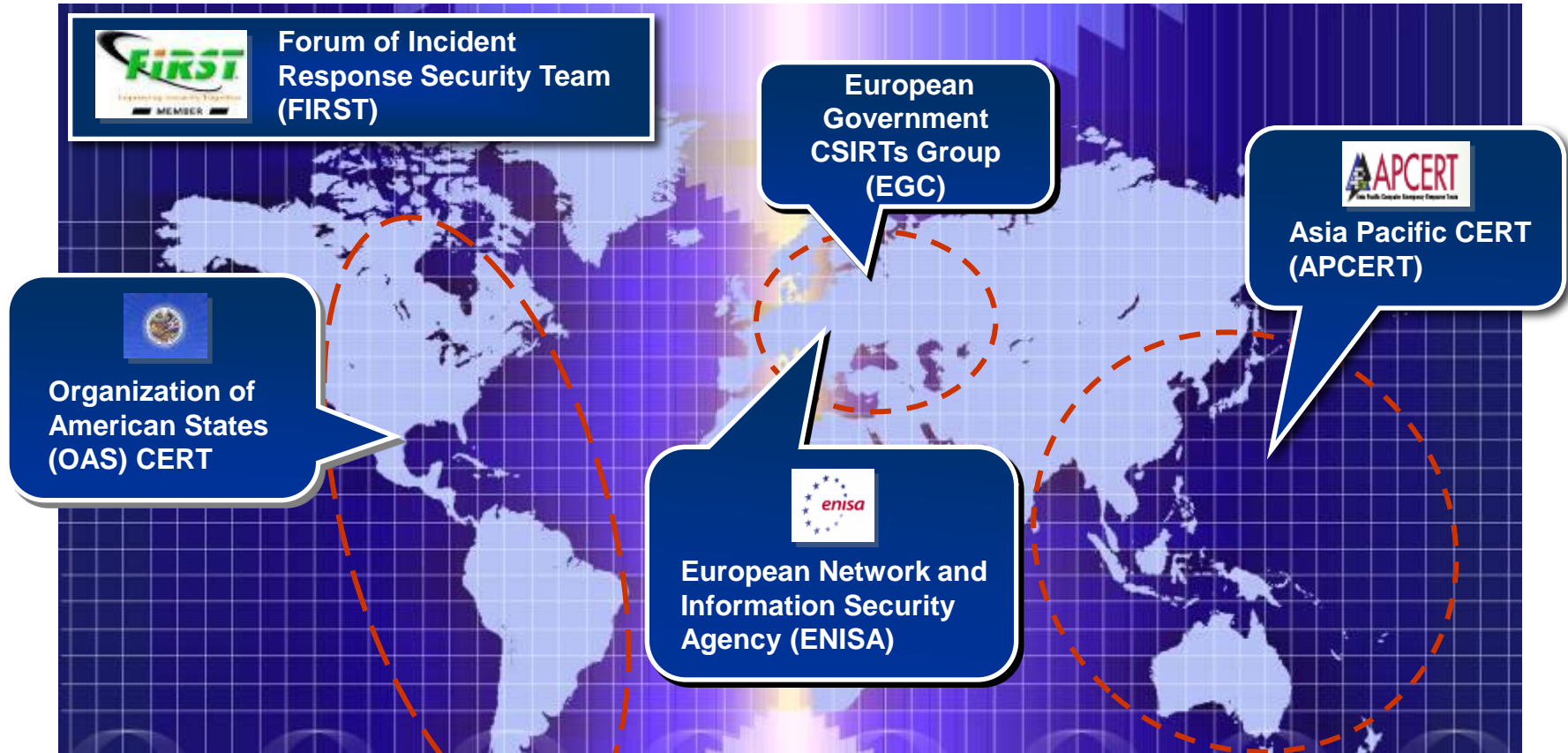


# 2008 CSI COMPUTER CRIME AND SECURITY SURVEY

Figure 13: Percentages of Key Types of Incident



# INTERNATIONAL COLLABORATION TO MINIMISE BORDERLESS THREATS



This growing cyber threat in the world requires a collaborative approach with various CERT organisations with full support from their respective governments

# ASPIRATION OF OIC-CERT (Organization of Islamic Conference – Computer Emergency Response Team)



**Conceptualization : 21 - 23 June 2005**

**Islamic Development Bank Board of Governors' Annual Meeting in Putrajaya, Malaysia**

- Agreed to initiate the establishment of OIC-CERT Task Force

**Task Force Meeting : 27 July 2006**

**OIC-CERT Task Force Meeting in Kuala Lumpur, Malaysia**

- Formation of OIC-CERT Task Force (Malaysia, Tunisia, Pakistan, Saudi Arabia, Nigeria)

**Task Force Meeting : 1 - 2 April 2008**

**OIC-CERT Task Force Meeting and Conference in Tunis, Tunisia**

- Formalization of OIC-CERT to be submitted to the OIC

**18 - 20 June 2008**

**35th Session of the OIC Council of Foreign Ministers in Kampala, Uganda**

- **Acceptance of Resolution on the establishment of OIC-CERT**

**14 - 15 January 2009**

**OIC-CERT 1st Annual General Meeting in Kuala Lumpur, Malaysia**

- **Formal establishment of OIC-CERT**
- **16 OIC member states are members of OIC-CERT**

**23 - 25 May 2009**

**36th Session of the OIC Council of Foreign Ministers in Damascus, Syria**

- **Acceptance of OIC-CERT as an Affiliated Institution of the OIC**

# MEMBERS OF OIC-CERT (1)

## CHAIR



**MALAYSIA** : CyberSecurity Malaysia, Ministry of Science, Technology & Innovation

## SECRETARIAT



**TUNISIA** : National Agency for Computer Security (CERT-TCC)

## FULL MEMBERS

*14 MEMBERS*



**SAUDI ARABIA** : Communications & Information Technology Commission (CITC)



**PAKISTAN** : National Response Center for Cyber Crimes, Federal Investigation Agency (FIA) HQs



**NIGERIA** : Consultancy Support Services (CS2)



**IRAN** : IrCERT (APA), Iran Telecommunication Research Center (ITRC)



**EGYPT** : Ministry of Communication and Information Technology



**SYRIA** : Ministry of Communication and Technology

# MEMBERS OF OIC-CERT (2)

## FULL MEMBERS



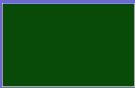
**MOROCCO** : Ministry of Industry and New Technologies



**INDONESIA** : Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII)



**BRUNEI** : Brunei Computer Emergency Response Team (BRUCERT)



**LIBYA** : Centre for Economic Information and Documentation, Ministry of Economy, Trade and Investment



**OMAN** : Information Technology Authority



**JORDAN** : National Center for Security and Crisis Management, Royal Court

## GENERAL MEMBERS

*2 MEMBERS*

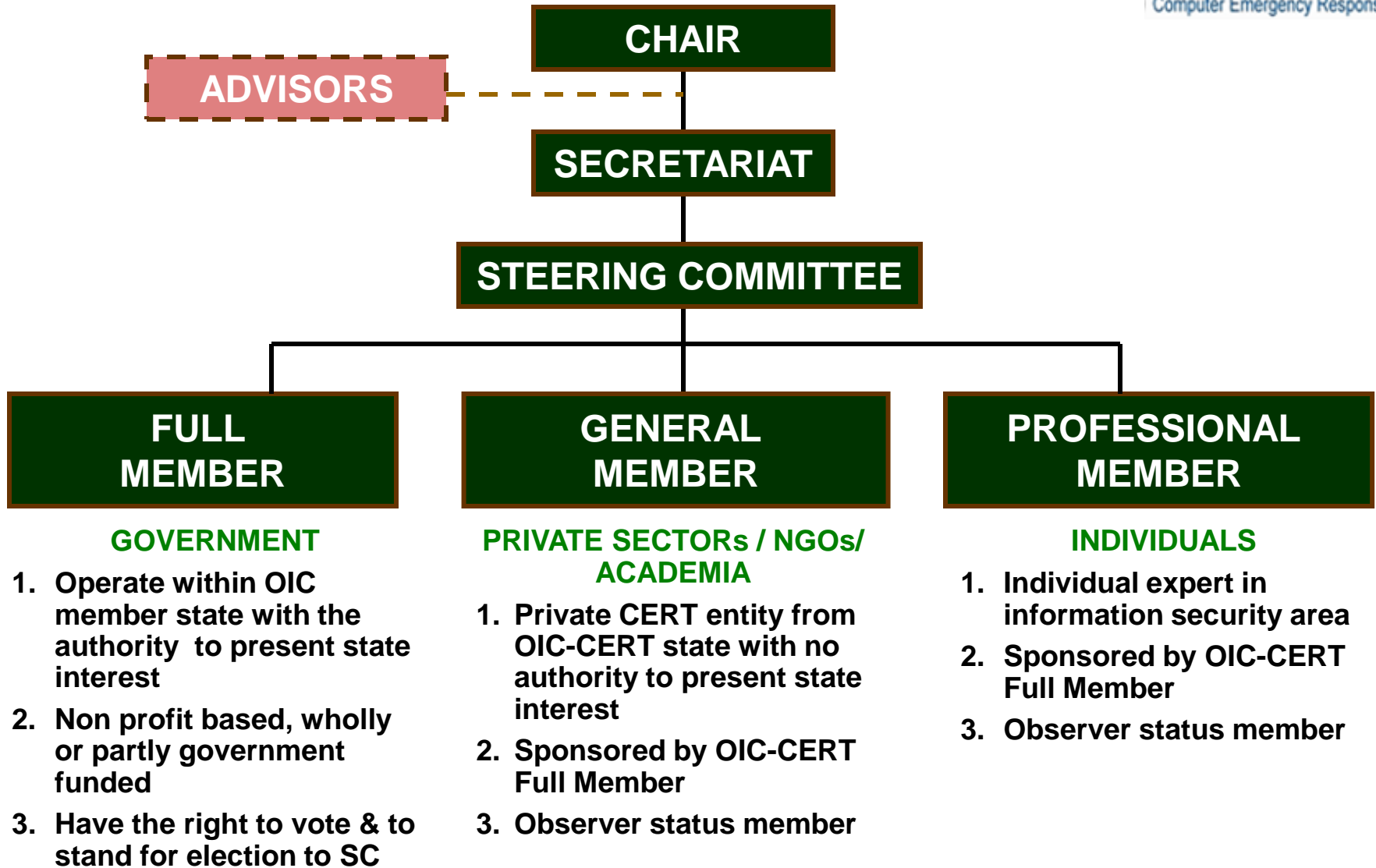


**BANGLADESH** : Bangladesh Computer Emergency Response Team (BDCERT)

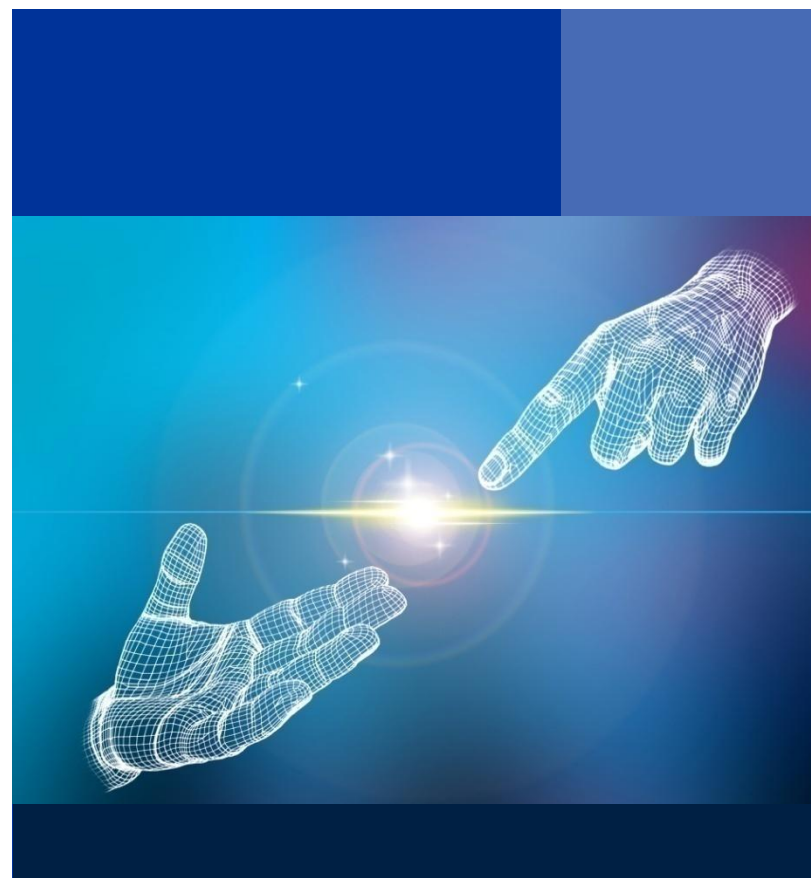


**TURKEY** : Turkey Computer Emergency Response Team (TR-CERT)

# GOVERNANCE STRUCTURE



- ❑ Strengthen the relationships amongst CERTs in the OIC member countries
- ❑ Enhance information sharing in cyber security field
- ❑ Prevent and reduce cyber-crimes
- ❑ Cultivate and foster education and outreach ICT security programs
- ❑ Promote collaborative technology research and development
- ❑ Provide cyber emergency channels among member countries



- ❑ Project OIC as pro-active in acting against cyber threats
- ❑ Establish a trusted network among OIC communities in preventing crime in cyberspace
- ❑ Promote collaborative activities i.e. research, education, technology development and outreach programmes among OIC countries
- ❑ Open up businesses opportunities among OIC communities to provide cyber security solutions

- ❑ Encourage participation from OIC member countries to be a member of OIC-CERT
- ❑ Welcome collaboration with other Regional CERT establishments
- ❑ The OIC-CERT regional workshops are planned to be held at three regions namely Middle East, Africa and Asia.
  - For the Middle East region, hosted by the Ministry of Communication and Technologies, Egypt on 8-9 June 2010
  - For the Africa region, hosted by the Ministry of Industry, Trade and New Technology of Morocco on 24-25 June 2010
  - For the Asia region, hosted by CyberSecurity Malaysia on 28-29 October 2010
- ❑ OIC-CERT Seminar & 2nd AGM in Islamabad, Pakistan in October 2010

# THANK YOU

## Websites

  
[www.cybersecurity.my](http://www.cybersecurity.my)

**CNII Portal**  
Critical National Information Infrastructure  
[cnii.cybersecurity.my](http://cnii.cybersecurity.my)

  
[www.mycert.org.my](http://www.mycert.org.my)

  
**eSecurity**  
TOWARDS BUILDING A SECURITY CULTURE  
[www.esecurity.org.my](http://www.esecurity.org.my)

## Emails

  **for general inquiries**  
[info@cybersecurity.my](mailto:info@cybersecurity.my)

  **for incidence reporting**  
[cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)