ITU ACMA International Training Program 2014

ITU Global Cyber Security Agenda

Sameer Sharma

Regional Director a.i.

ITU Regional Office for Asia-Pacific

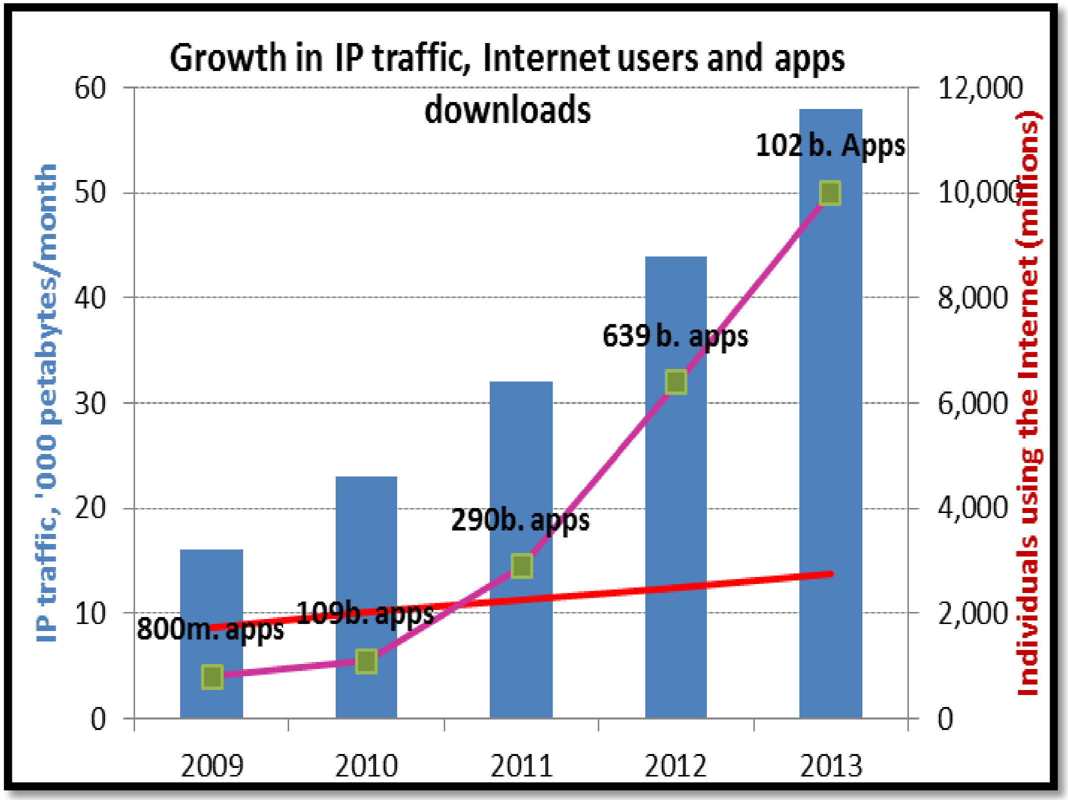
International Telecommunication Union

Committed to connecting the world

Content

- Why Cybersecurity?
- ITU Mandate on Cybersecurity
  - Global Cybersecurity Agenda
  - High Level Experts Group
- ITU Initiatives
  - National CIRT Programme with IMPACT
  - Child Online Protection
  - Global Cybersecurity Index
  - Enhancing Cybersecurity in LDCs
  - National Strategies and Legislations
- UN-wide framework on Cybersecurity & Cybercrime
- Global Partnerships

Growth in ICT



Source: ITU, based on data from ITU, Gartner, Cisco VNI, Telegeography and IDC.

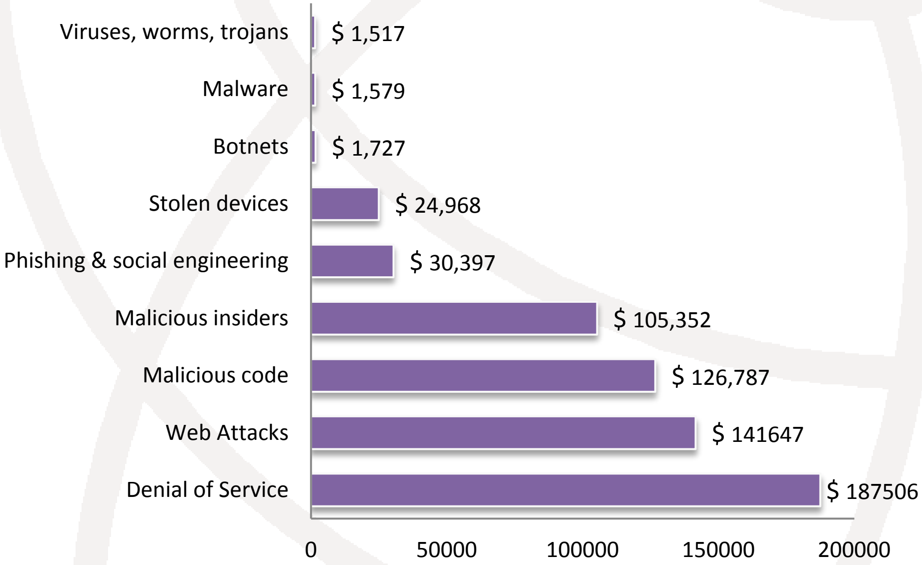
- Mobile cellular subscriptions nearly equals the world's population
- Smartphones are leading the way in drawing consumers online
- IP traffic continues to show healthy growth
- Mobile video traffic accounts for more than 50 per cent of mobile data traffic
- Apps market adds millions of users per month

Online Devices/ Networks :
Prone to cyber attack

March 2011	• Hackers penetrate French government computer network • South Korea Defense Network penetrated • RSA Secure ID compromised • Attacks at EU's Commission and External Action Service
June 2011	• Attacks at Sony. Millions of logins leaked • Attacks and NATO internal network • Attacks at International Monetary Fund (IMF) • Hackers disrupt 51 Malaysian government websites • UK Treasury under sustained cyberattack
October 2011	• Cyber-attacks on UK at disturbing levels • Japan under Heavy Cyber Attack
November 2011	• Hackers destroyed a pump used by a US water utility • Duqu computer virus Detected by Iran civil defense organization • More than 100 Pakistani Government Sites Under Malware attack • Thousands of United Nation (UNDP) logins leaked • Cyber attacks hit Fujitsu local government system in Japan • Largest DDOS attack hit Chinese company
January 2012	• Hackers attack Brazil's largest private bank, shut down online banking • European Parliament says its website taken offline by attackers • Investigations Involving the Internet and Computer Networks • DDoS against Polish government websites • Hackers manipulated railway computers • 103 Government of Kenya websites hacked overnight

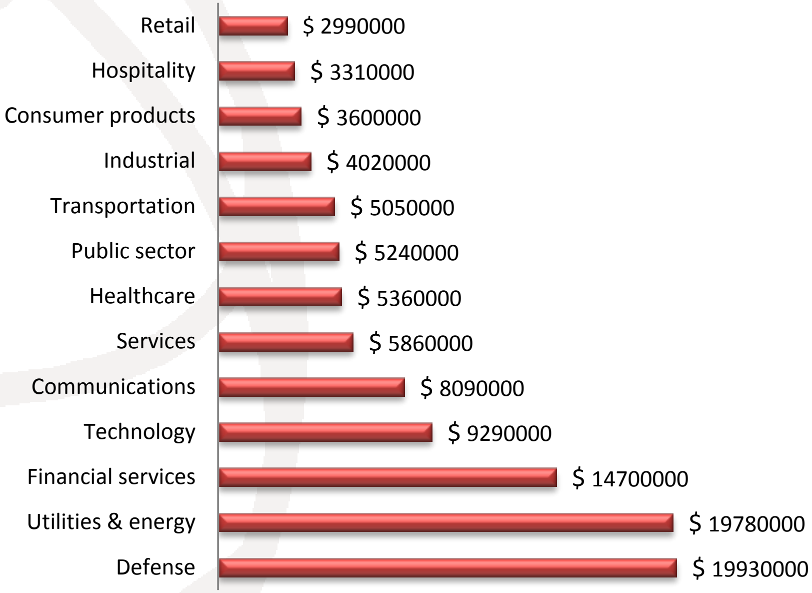
Financial Impact

- It is estimated that overall cost of cybercrime is as much as $1 trillion on a global basis.
- The estimated average cost to an individual US organization was $3.8 million per year in 2010.
- In 2011 the estimated average cost to an individual US organization is $5.9 million per year, with a range from $1.5 million to $36.5 million per organization.
- The most costly cyber crimes are those caused by malicious code, denial of service, stolen or hijacked devices and malicious insiders.
- Cyber Crime costs British Economy ₤27 Billion a year.



Average annualized cyber crime cost weighted by the frequency of attack incidents

Source: http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf



Average annualized cost by sector for sample of 50 US organizations for 2011

Source: http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

Key Cybersecurity Challenges

- Lack of adequate and interoperable national or regional legal frameworks
- Lack of secure software and ICT-based applications
- Lack of appropriate national and global organizational structures to deal with cyber incidents
- Lack of information security professionals and skills within governments; lack of basic awareness among users
- Lack of international cooperation between industry experts, law enforcements, regulators, academia & international organizations, etc. to address a global challenge

Cybersecurity not seen yet as a cross-sector, multi-dimensional concern. Still seen as a technical/technology problem.

ITU mandate on cybersecurity

2003 – 2005
WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 - “**Building Confidence and Security in the use of ICTs**”

world summit
on the **information society**
Geneva 2003 - Tunis 2005

INTERNATIONAL COOPERATION
LEGAL MEASURES
CAPACITY BUILDING
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

2007
Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General
GCA is a **framework for international cooperation in cybersecurity**

2008 to date
ITU Membership endorsed the GCA as the ITU-wide strategy on international cooperation.

G C A GLOBAL CYBERSECURITY AGENDA

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

Child Online Protection

Building confidence and security in the use of ICTs is widely present in **PP and Conferences**’ resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues, from legal to policy, to technical and organization measures.

ITU-T Activities

ITU-T Study Group 17

- Lead Study Group for Telecommunication Security
- Mandate for Question 4/17 (Q.4/17): Cybersecurity
- Provides ICT Security Standards Roadmap
- ITU-T Cybersecurity Information Exchange Framework (CYBEX)
- ITU-T Security Manual "Security in telecommunications and information technology
- Focus Group on Identity Management (IdM)
- Approved over 100 Recommendations on security for communication
- JCA on COP

WTSA Resolutions

- ITU WTSA Resolution 50: Cybersecurity
- ITU WTSA Resolution 52: Countering and combating spam
- ITU WTSA Resolution 58: Encourage the creation of national computer incident response teams, particularly for developing countries

ITU-R Activities

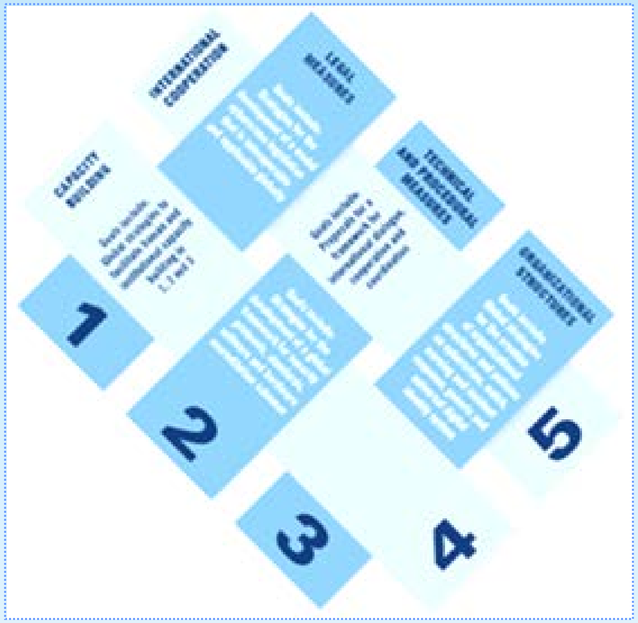
- Establish fundamental security principles for IMT-2000 (3G) networks
- Issue ITU-R Recommendation on security issues in network management architecture for digital satellite system and performance enhancements of transmission control protocol over satellite networks

<u>ITU-R Recommendations</u>

- Recommendation ITU-R M.1078: Security principles for International Mobile Telecommunications-2000 (IMT-2000)
- Recommendation ITU-R M.1223: Evaluation of security mechanisms for IMT-2000
- Recommendation ITU-R M.1457: Detailed specifications of the radio interfaces of International Mobile Telecommunications-2000 (IMT-2000)
- Recommendation ITU-R M.1645: Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000
- Recommendation ITU-R S.1250: Network management architecture for digital satellite systems forming part of SDH transport networks in the fixed-satellite service
- Recommendation ITU-R S.1711: Performance enhancements of transmission control protocol over satellite networks

Global Cybersecurtiy Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.
- GCA builds upon five pillars:
    1. Legal Measures
    2. Technical and Procedural Measures
    3. Organizational Structure
    4. Capacity Building
    5. International Cooperation
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.
- H.E. Blaise Compaoré, President of Burkina Faso, and H.E. Dr Óscar Arias Sánchez, Former President of the Republic of Costa Rica and Nobel Peace Laureate, are both Patrons of the GCA.


INTERNATIONAL COOPERATION
LEGAL MEASURES
CAPACITY BUILDING
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

High-Level Expert Group (HLEG)

- The High-Level Expert Group (HLEG) on Cybersecurity was established in 2007. It is comprised of over 100 renowned experts from a broad range of backgrounds, sectors and geographical regions.
- These experts worked tirelessly to formulate proposals to the ITU Secretary-General on strategies to curb cyberthreats, combat cybercrime and promote cybersecurity.
- Its outputs include the Report of the Chairman of the HLEG, a set of strategic proposals, and the HLEG Global Strategic Report, which summarizes the HLEG's work in seeking to promote cybersecurity around the world.

International Telecommunication Union

ITU Global Cybersecurity Agenda (GCA)

High-level Experts Group (HLEG)

Global Strategic Report

ITU: Committed to connecting the world

e-mail: gca@itu.int — www.itu.int/cybersecurity/gca

GCA: From Strategy to Action

Global Cybersecurity Agenda (GCA)

1. Legal Measures

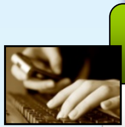
Publication : Understanding Cybercrime A Guide for Developing Countries
MoU with UNODC for assistance
ITU-EC project model law for ACP

2. Technical and Procedural Measures

ITU Standardization Work: ITU-T , ITU-D SG1 Q22
ITU-R recommendations on security
ICT Security Standards Roadmap
ITU-T JCA on COP

3. Organizational Structures

National CIRT deployment
ITU work on National CIRTs cooperation
ITU Cybersecurity Information Exchange Network (CYBEX)
ITU-D SG 1 Q22



4. Capacity Building

ITU National Cybersecurity Strategy Guide
Report on ITU-D SG1 Q22
Technical assistance and projects:LDCs
Regional Cybersecurity Seminars
National Cyber drills

5. International Cooperation

ITU High-Level Expert Group (HLEG)
ITU-IMPACT Collaboration
ITU’s Child Online Protection(COP)
Collaboration with UN, and other IGOs, as well as with Symantec, Trend Micro, ABI research, etc

ITU-IMPACT Initiative

- Since 2008 – a global initiative – for technical capacity building
- 149 Member States joined this global initiative
- Conducted over 50 country assessment to determine cybersecurity readiness for establishing National CIRTs
- Facilitated the deployment of 7 National CIRTs and 7 more in progress
- Trained over 2700 cybersecurity professional and practitioners globally
- Granted over 360 scholarships to 52 countries
- Conducted world's first cyber drills benefitting more than 60 countries

  - Next drill for Americas region in Peru on 8-10 September 2014

IMPACT

International Telecommunication Union

Committed to connecting the world

ITU’s Child Online Protection

- Under the GCA umbrella, ITU initiated the Child Online Protection initiative (COP) in November 2008.
- COP has been established as an international collaborative network for promoting the online protection of children and young people worldwide by providing guidance on safe online behavior.

Objectives

- Identify risks and vulnerabilities to children in cyberspace
- Create awareness
- Develop practical tools to help minimize risk
- Share knowledge and experience

July 2013: H.E. Dame Patience Goodluck Jonathan, First Lady of Nigeria was appointed ITU COP Champion

The Global Cybersecurity Index (GCI)

Objective

The Global Cybersecurity Index (GCI) aims to measure and rank each nation state's level of cybersecurity development in five main areas:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- National and International Cooperation

Goal

Promote government strategies at a national level

Drive implementation efforts across industries and sectors

Integrate security into the core of technological progress

Foster a global culture of cybersecurity

ABIresearch®

ITU

Global Cybersecurity Index

Global Cybersecurity Index

Timeframe & Project Activities

The project represents an undertaking of 12 to 18 months. Expected delivery of the full index is Q4 2014.

The timeframe is split into six regional stages:

- Arab States
- Europe
- Asia Pacific
- Americas
- Commonwealth of Independent States
- Africa

Phases for each regional stage:

- **Primary Research**: Contact relevant national stakeholders to collect data
- **Secondary Research**: Internal databases, publicly-available resources
- **Data Extraction**: Organize and sort through collected data
- **Data Input**: Assess the performance of each nation state

Global Cybersecurity Index

Current Survey Response - 79

Afghanistan
Algeria (People's Democratic Republic of)
Armenia (Republic of)
Azerbaijan
Bangladesh (People's Republic of)
Barbados
Bhutan (Kingdom of)
Bosnia and Herzegovina
Botswana
Brunei Darussalam
Bulgaria (Republic of)
Burkina Faso
Burundi
Cameroon (Republic of)
Cape Verde
Colombia
Comoros (Union of the)
Congo
Cote d'Ivoire
Democratic republic of Congo
Djibouti (Republic of)
Dominican Republic
Egypt (Arab Republic of)
Fiji
Finland
Federated States of Micronesia
Gabon
Gambia
Georgia
Grenada
Guatemala (Republic of)
Guinea (Republic of)
Italy
Jordan
Hong Kong
Kenya
Kiribati
Lebanon
Lesotho
Liberia
Libya
Malawi
Maldives (Republic of)
Mali (Republic of)
Marshall Islands
Mauritania (Islamic Republic of)
Mauritius
Montenegro
Morocco (Kingdom of)
Myanmar
Namibia
Oman (Sultanate of)
Panama (Republic of)
Papua New Guinea
Qatar (State of)
Romania
Russian Federation
Saint Kitts and Nevis (Federation of)
Sao Tome & Principe
Sierra Leone
Slovakia
Somali Democratic Republic
South Africa
Sri Lanka
Sudan (Republic of the)
Swaziland (Kingdom of)
Syrian Arab Republic
Tanzania
Togolese Republic
Tonga
Trinidad and Tobago
Turkey
Tuvalu
United Kingdom of Great Britain and Northern Ireland
Uruguay
Vanuatu (Republic of)
Zambia (Republic of)
Zimbabwe

Enhancing Cybersecurity in Least Developed Countries project

Aims at supporting the 49 Least Developed Countries in strengthening their cybersecurity capabilities.

How

- **Assessment** for selected key government ministries & subsequent **solutions provision**
- **Capacity building** through training of trainers, workshops,..
- **Customised guidelines** on legislation, regulation and technologies

End Result

- protection of their national infrastructure, including the critical information infrastructure, **thereby making the Internet safer** and protecting Internet users
- serve national priorities and **maximize socio-economic benefits** in line with the objectives of the World Summit on the Information Society (WSIS) and the Millennium Development Goals (MDGs).

We are only as secure as our weakest link …

National Strategies and Legislations

- Establishment of Harmonized Policies for the ICT Market in the ACP States completed in 2013 in 3 subprojects
  - by ITU and European Commission.
  - Enhancing competitiveness in the Caribbean through the harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR Project).
  - Support for harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA Project).
  - Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC Project).
- ITU assists Member States to develop National Cybersecurity Strategies and to adapt their legislations to effectively address cybercrimes
- Understanding Cybercrime: Phenomena, challenges and legal response - an ITU publication

UN-wide framework on Cybersecurity & Cybercrime

- ITU and UNODC, along with some 33 UN Agencies, developed UN-wide framework on Cybersecurity & Cybercrime.
- Document focuses **on the external efforts of UN entities** concerning Member States
- The purpose of this framework is:
  - ✓ To enable **enhanced coordination among UN entities** in their response to concerns of Member States regarding **cybercrime** and **cybersecurity**
- Framework document presented to and endorsed by the UN CEB in November 2013
- Strategy document under preparation for 2014

Building a global partnership

The recent establishment of global collaborations **emphasize the role of ITU as global catalyst on international cooperation in cybersecurity** and BDT as the implementing arm

Capacity building initiatives, joint consultations and more. February 2014 regional Cybercrime Investigation Seminar

Best practices in cybercrime legislations, joint technical assistance to member states, information sharing

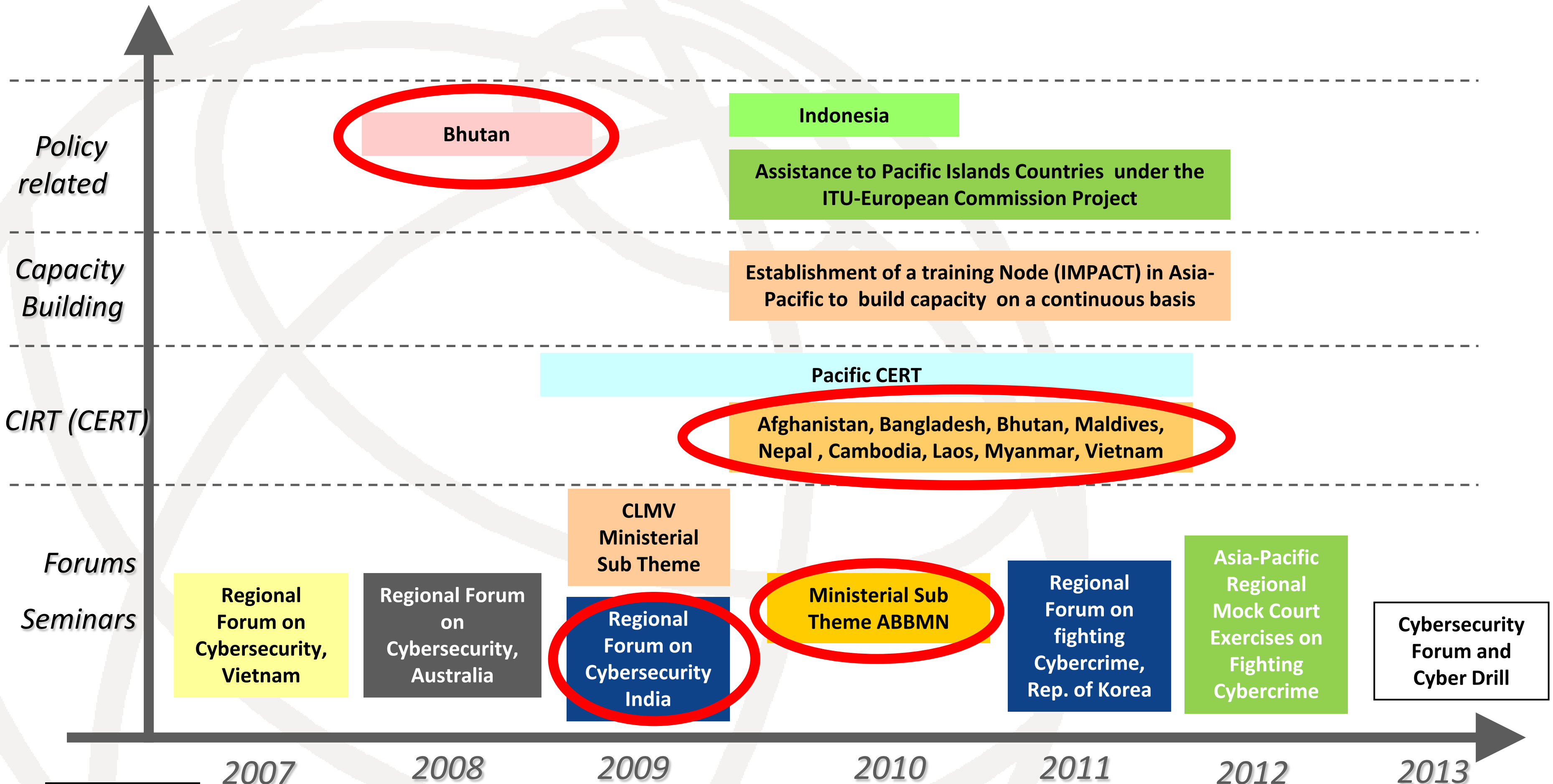
Tap on expertise of globally recognized industry players and accelerate info sharing with ITU member states

Collaboration with ABI Research – **The Global Cybersecurity Index (GCI)**

Collaboration with FIRST – To share best practices on computer incident response, engage in joint events, facilitate affiliation of national CIRTS of member states

Collaboration with Member States – Regional Cybersecurity Centres

ITU Cybersecurity Initiatives in Asia-Pacific



Policy related

Bhutan

Indonesia

Assistance to Pacific Islands Countries under the ITU-European Commission Project

Capacity Building

Establishment of a training Node (IMPACT) in Asia-Pacific to build capacity on a continuous basis

CIRT (CERT)

Pacific CERT

Afghanistan, Bangladesh, Bhutan, Maldives, Nepal , Cambodia, Laos, Myanmar, Vietnam

Forums

Seminars

Regional Forum on Cybersecurity, Vietnam

Regional Forum on Cybersecurity, Australia

CLMV Ministerial Sub Theme

Regional Forum on Cybersecurity India

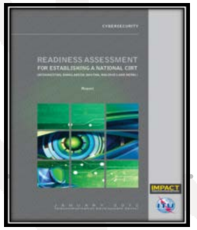
Ministerial Sub Theme ABBMN

Regional Forum on fighting Cybercrime, Rep. of Korea

Asia-Pacific Regional Mock Court Exercises on Fighting Cybercrime

Cybersecurity Forum and Cyber Drill

2007 *2008* *2009* *2010* *2011* *2012* *2013*



CIRT Assessment in ABBMN Countries

Conclusions

- While it will never be possible to completely remove all risks, drawing together an effective package of policies and practices, infrastructure and technology, awareness and communication can do a great deal to help.
- The international cooperation, based on a multi-stakeholder approach and the belief that every organization – whether online or mobile, educator or legislator, technical expert or industry body – has something to contribute.
- By working together with ITU, all interested stakeholders and countries, can achieve this critical international collaboration, confronting child online threats with a dynamic and unified coalition.

Let’s work together

- ✓ Respond to the questionnaire for the Global Cyber Security Index
- ✓ Partner with us to ‘**Enhance Cybersecurity in Least Developed Countries’**
- ✓ International cooperation to address Child Online Protection
- ✓ Join our study groups
- ✓ National CIRT assessment, implementation or join our cyberdrills

More information on the above at

http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx