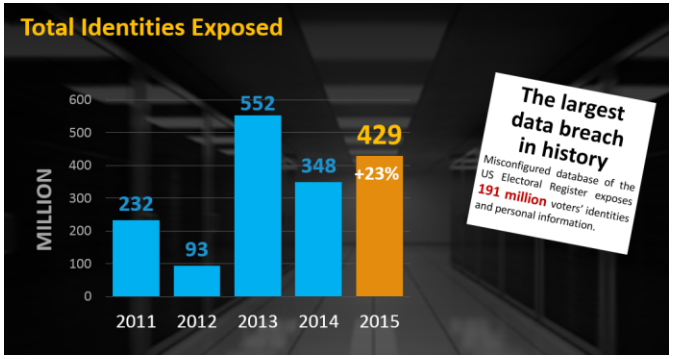
BDT Cybersecurity Program

Cybersecurity Week From the Center of the World and 4th Regional Cyber Drill for the Americas Region
Quito, Ecuador, 27 June 2016

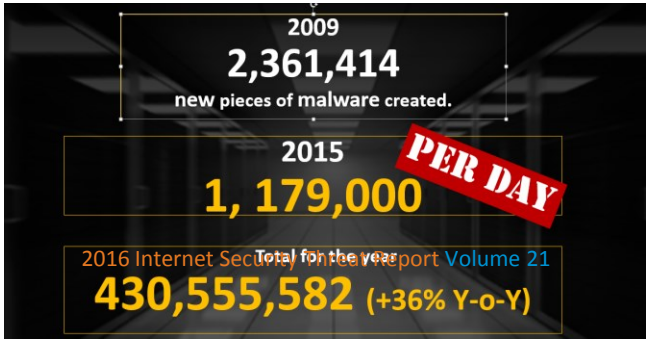
Luc Dandurand
Head of ICT Applications and Cybersecurity Division
Telecommunications Development Bureau, ITU

The Importance of Cybersecurity

- From industrial age to information societies
  - Increasing dependence on the availability of ICTs
  - Number of Internet users growing constantly
    - Now 40% of world's population
  - Internet of Things and Smart Society initiatives will dramatically accelerate these trends



- Statistics and reports show that cyber-threats are on the rise



- Developing countries most at risk as they adopt broader use of ICTs

- Need for building cybersecurity capacity
  - Protection is crucial for the socio-economic wellbeing of a country in the adoption of new technologies

2015 Cyber-Threat Landscape

- **430 Million** new pieces of unique **malware** discovered
- A **record 9 mega breaches** (>10m identities) occurred in 2015
- **~191 Million** identities exposed in the **largest** data breach in history
- **55% increase** in the number of **spear-phishing** campaigns attacks in 2015
- **35% increase** in **crypto-ransomware** as it spread beyond end-users to holding businesses hostage
- **3 out of every 4** legitimate websites found to have **unpatched vulnerabilities**
- **125% increase** in the number of **zero-day** vulnerabilities discovered
- **Half** of all targeted attacks were against **small/medium businesses**

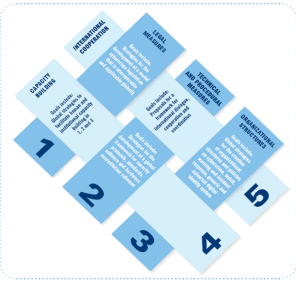
ITU Mandate on Cybersecurity

Committed to Connecting the World

International Telecommunication Union

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



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.

GCA GLOBAL CYBERSECURITY AGENDA

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.

BDT Cybersecurity Service Catalogue

Engagement and awareness

- Global Cybersecurity Index
- Global, Regional and National events
- Information dissemination

Computer Incident Response Team (CIRT) Program

- CIRT design
- CIRT implementation
- CIRT enhancement

Cyber Drills

- Regional drills
- National drills

National Cybersecurity Strategy (NCS)

- National Cybersecurity assessment
- NCS development support

In-Country Technical Assistance

- Technical Support (e.g. vulnerability assessments)
- Risk Management Support

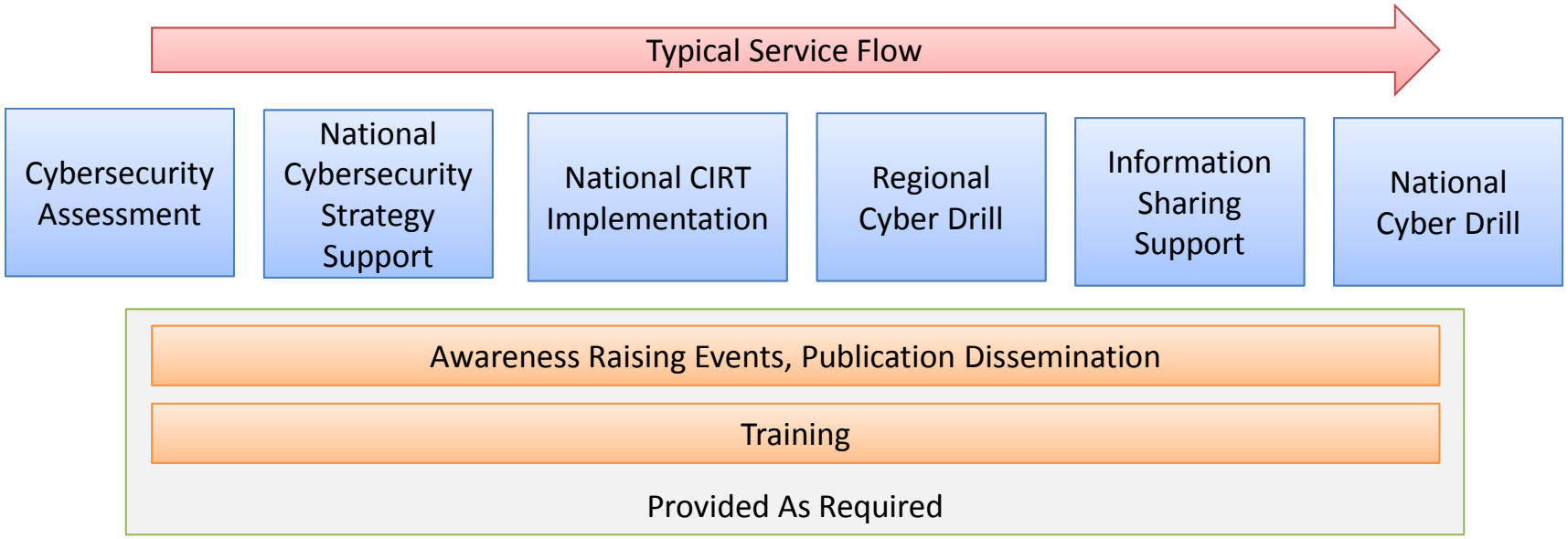
Information sharing

- Best Practices Sharing
- Information Exchange Tools and Techniques

Human Capacity Building

- Curricula and Training Programs
- Bespoke Training

Flow of Cybersecurity Services



Global Cybersecurity index - GCI

The GCI measures the commitment of countries to cybersecurity in the 5 pillars of the Global Cybersecurity Agenda:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- Cooperation

Goals

- help countries identify areas for improvement
- motivate them to take action to improve their GCI ranking
- help harmonize practices
- foster a global culture of cybersecurity

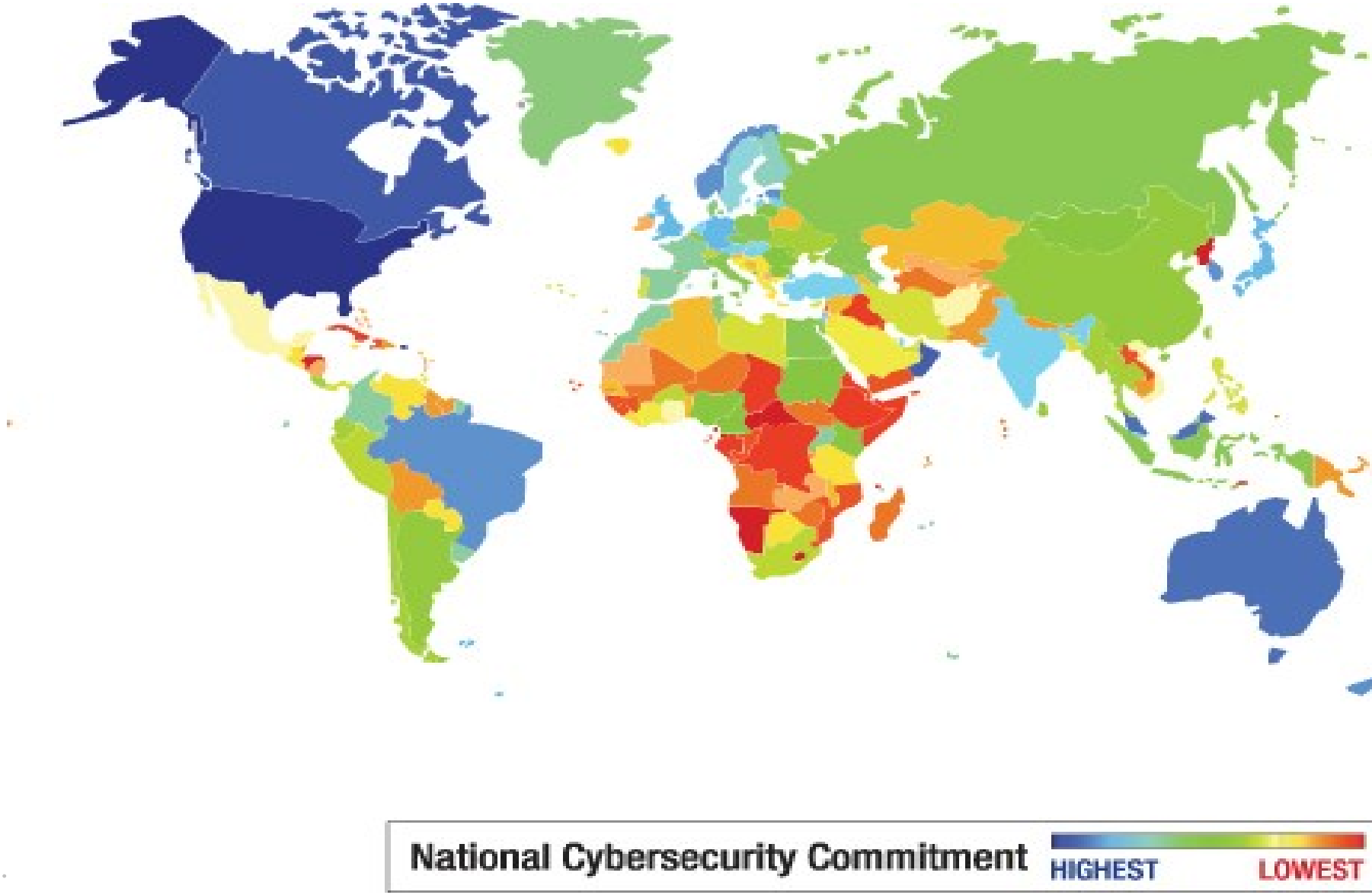
Final Global and Regional Results 2014 are on ITU Website

2016 Version Ongoing!

134 Countries have responded, analysis ongoing

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

GCI 2014 Results



Global Cybersecurity index - Partnership

GCI PARTNERS for data sharing, response collection and expertise in analysis

FIRST
Improving Security Together

unicri
United Nations
Interregional Crime and Justice
Research Institute

KISA
Korea Internet & Security Agency

INDIANA UNIVERSITY

ACTIONABLE
THREAT INTELLIGENCE
REDTEAM
CYBER

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE

POTOMAC INSTITUTE
FOR POLICY STUDIES

RCC
المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

NTRA
EGYPT
National Telecom
Regulatory Authority

WORLD BANK GROUP

Global Cybersecurity index - GCI 2016 status

194 Member States

134 Surveys submitted

21 Online surveys being filled

39 have not responded

35 America Region Member States

23 Surveys submitted

5 Online surveys being filled

7 have not responded

Thank you for participating Antigua and Barbuda, Argentina, Barbados, Belize, Bolivia, Brazil, Chile, Columbia, Costa Rica, Dominican Republic, Ecuador, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago, Uruguay, Venezuela.

GCI Submission needed for Cuba, Guatemala, Saint Kitts and Nevis, Saint Lucia, USA.

Focal Points Needed for Bahamas, Canada, Dominica, El Salvador, Grenada, Guyana, Haiti.

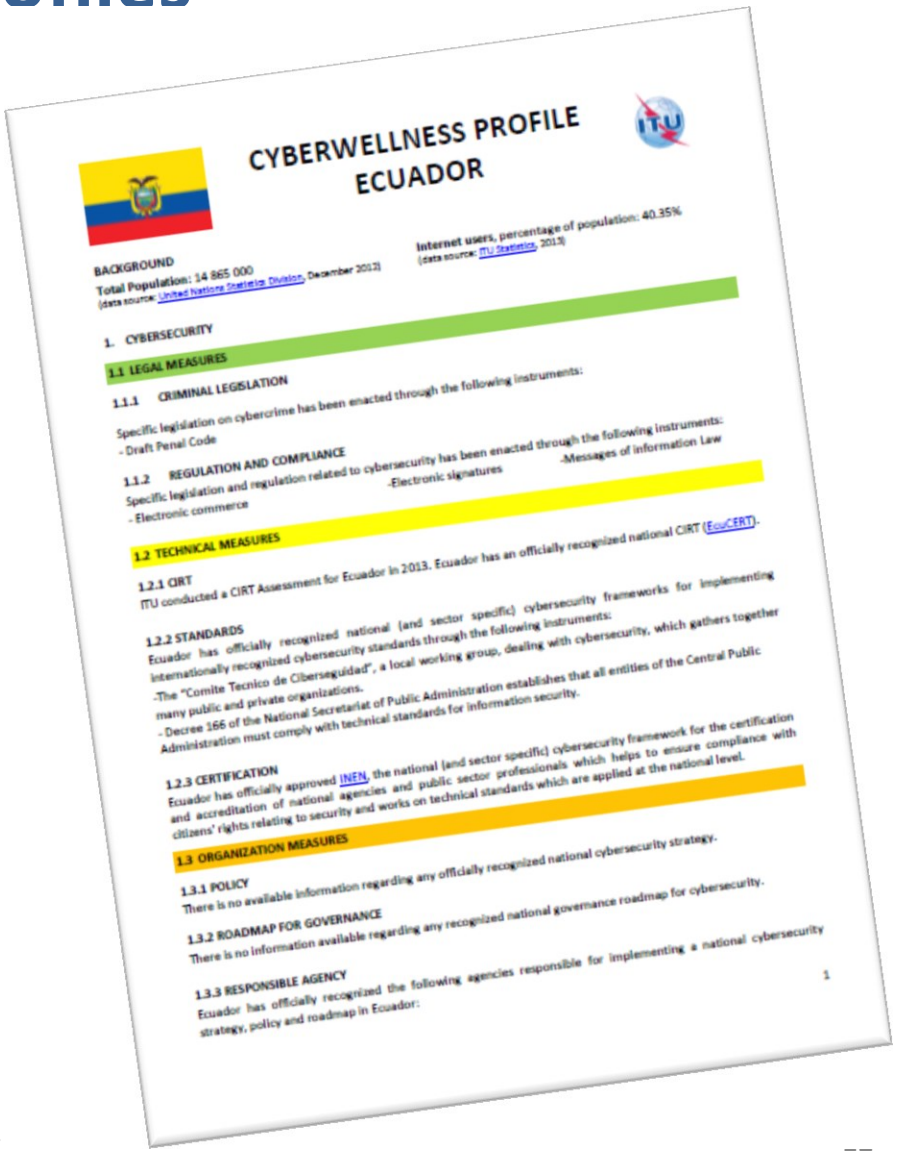
Cyberwellness Country Profiles

Factual information on cybersecurity achievements on each country based on the GCA pillars

- Live documents
- Invite countries to assist us in maintaining updated information

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

Example →



CYBERWELLNESS PROFILE
ECUADOR

BACKGROUND
Total Population: 14 865 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 40.35%
(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:
- Draft Penal Code

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:
- Electronic commerce
-Electronic signatures
-Messages of information Law

1.2 TECHNICAL MEASURES

1.2.1 CIRT

ITU conducted a CIRT Assessment for Ecuador in 2013. Ecuador has an officially recognized national CIRT (EcuCERT).

1.2.2 STANDARDS

Ecuador has officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:
-The "Comite Tecnico de Ciberseguidad", a local working group, dealing with cybersecurity, which gathers together many public and private organizations.
- Decree 166 of the National Secretariat of Public Administration establishes that all entities of the Central Public Administration must comply with technical standards for information security.

1.2.3 CERTIFICATION

Ecuador has officially approved INEN, the national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals which helps to ensure compliance with citizens' rights relating to security and works on technical standards which are applied at the national level.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

There is no available information regarding any officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no information available regarding any recognized national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Ecuador has officially recognized the following agencies responsible for implementing a national cybersecurity strategy, policy and roadmap in Ecuador:

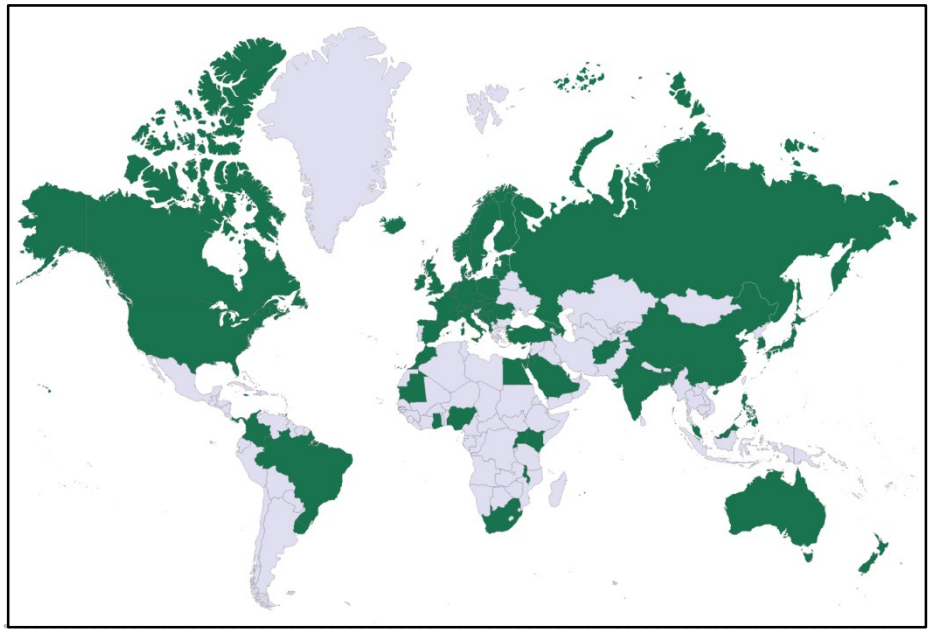
1

National Cybersecurity Strategy Guide

Reference Guide and Support Tool to help Member States produce a National Cybersecurity Strategy

- Only 72 out of the ITU's 193 Member States have a National Cybersecurity Strategy

- New guide being developed under open consultation and multi-stakeholder approach, and will replace ITU's previous National Cybersecurity Strategy Guide



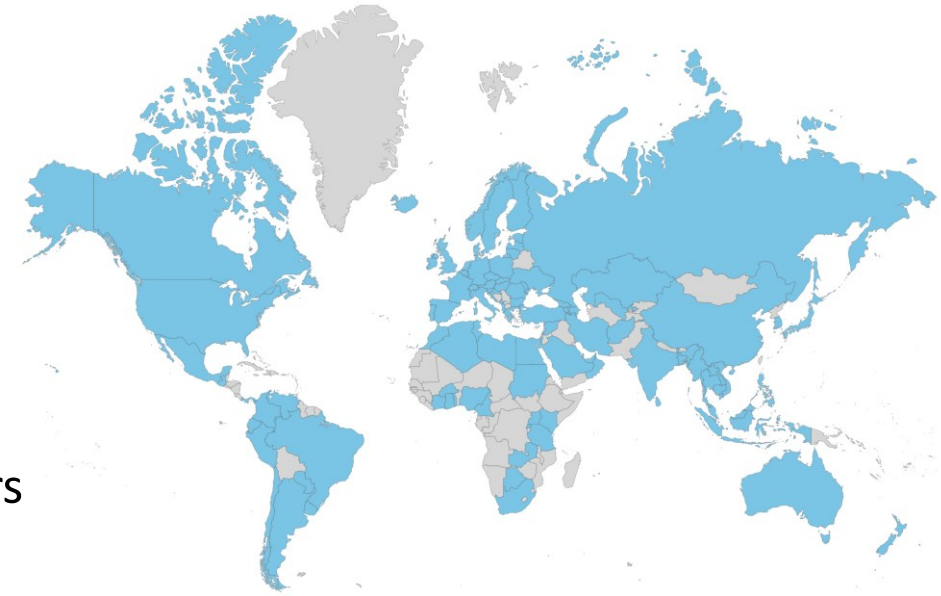
National Cyber Security Toolkit
Joint Effort by 15 Partners

All project partners contribute their knowledge and expertise in the National Cyber Security domain

National CIRTs
The First Line of Cyber-Response

Responsible for:

- Coordinating incident response
- Dissemination of early warnings and alerts
- Facilitating communications and information sharing among stakeholders
- Developing mitigation and response strategies
- Publishing best practices in incident response as well as prevention advice;
- Coordinating international cooperation on cyber incidents;



102 National CIRTs Worldwide

Need to fill the gap!

ITU's National CIRT Programme

- Assessments conducted for **67** countries
- Implementation completed for **11** countries

  Burkina Faso, Côte d'Ivoire, Cyprus, Ghana, Jamaica, Kenya, Montenegro, Tanzania, Trinidad and Tobago, Uganda, Zambia.

- Implementation in progress for **4** countries

  Barbados, Burundi, Gambia, Lebanon

- **15 regional** cyber drills conducted with participation of over **115** countries

Structured Approach to Building a National CIRT

- Use an approach based on community-accepted practices, re-using existing materials and solutions
  - We plan to use FIRST's CSIRT Services Framework and the materials produced by the GFCE CSIRT Maturity Initiative
- Approach Nations with a structured process
- Deliver customized solution that is adapted to each Nation's specific situation
- National CIRT must be part of a Nation's Cybersecurity Strategy
- Connect the National CIRT to relevant international, regional and national entities

Key Factors to Building a National CIRT

- National CIRT is meant to be the Nation's primary coordination authority
  - Other services are secondary
- Acceptance and recognition by other national stakeholders

FIRST's CSIRT Services Framework Overall Principles

- Simplicity
  - Straightforward high-level model to capture the key elements, get consensus and publish
- Comprehensiveness
  - Include "all" services that a CIRT can provide (independently of the type of CIRT) so to be adopted widely
- Pragmatism
  - Not a theoretical model, but rather a framework based on well consolidated best practices
- Consistence and precision in the language
  - Clear definitions
  - Consistency throughout the framework

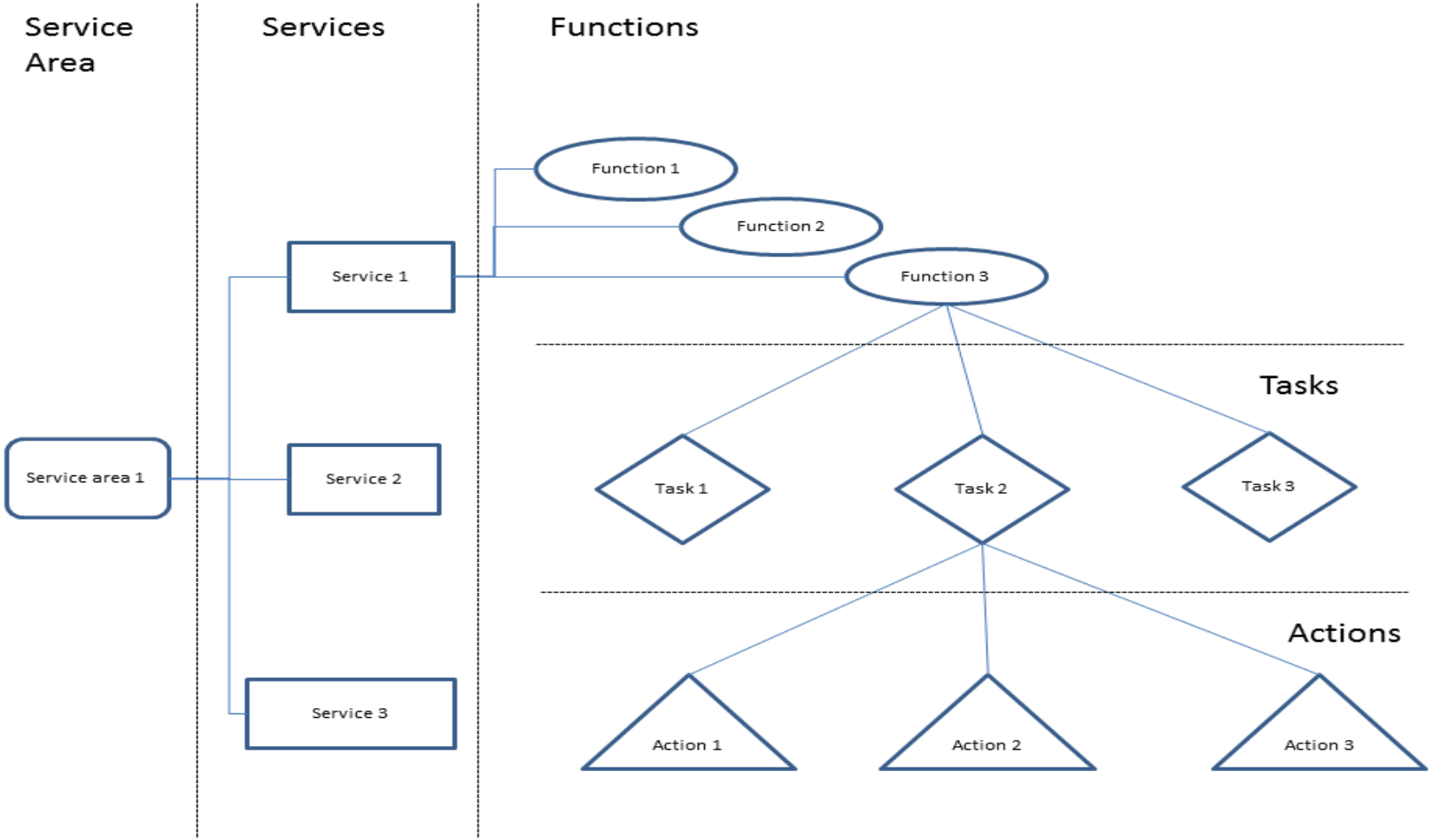
FIRST CSIRT Services Framework
Proposed Structure

- Top-down, hierarchical model
  - Service Area
  - Service
  - Function
  - Task
  - Action
- Service Areas, Services and Functions identify what is being done at different levels of details
- Tasks and Actions identify how it is being done at different levels of details

FIRST's CSIRT Services Framework Services Explained

- SERVICES
  - A mean of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. A service is a coherent, ready-to-use deliverable that is of value to the customer.
  - In the context of CIRT/CERTs/CSIRTs, customers is the CIRT/CERT/CSIRT constituency; therefore services are delivered on behalf or for the identified constituency
- FUNCTION
  - A function is an activity or of activities aimed at fulfilling the purpose of the service.
- TASKS
  - A task is a clearly defined piece of work, composed by one or more actions, sometimes of short or limited duration, to accomplish a specific objective, namely the function.
- ACTION
  - An action is a specific step, undertaken to accomplish a particular task. More actions might be undertaken to accomplish a specific task.

CSIRT Services Framework
Proposed Structure



Service Area	Services
Incident management	Coordination; Analysis; Mitigation; Recovery
Analysis	Artifact; Media; Vulnerability / Exploitation
Information assurance	Risk / Compliance Assessment; Cybersecurity policy advisory; Operating Policies Management; Risk Analysis/Business Continuity Disaster Recovery Advisement; Security Advisement
Situational Awareness	Sensor Operations; Fusion/ Correlation; Development and Curation of Security Intelligence
Outreach/ Communications	Cybersecurity strategic Policy Advisement; Security Awareness Raising; Information Sharing and Publications
Capability Building	Training and Education; Conducting Exercises; Technical advice; Lesson learned analysis; Organization metrics
Research/ Development	Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis Methodologies; Development of processes for Gathering/Fusing/Correlating Security Intelligence; Development of Tools

Demand for CIRT Design & Implementation (Africa)

- Angola
- Benin
- Botswana
- Burundi
- Central African Rep
- Congo (Dem Rep)
- Congo (Republic)
- Equatorial Guinea
- Gabonese Republic
- Gambia
- Madagascar
- Malawi (Design only)
- Namibia
- Senegal
- Sierra Leone
- Zimbabwe

Demand for CIRT Design & Implementation (other regions)

- Americas
  - Anguilla
  - Antigua
  - Dominica
  - Grenada
  - Guatemala
  - Honduras
  - Peru (not National)
  - Suriname (Design only)
- Arab Region
  - Comoros
  - Djibouti (Design only)
  - Maurritania
  - Lebanon
  - Palestine
  - Somalia
  - Djibouti (Design only)
- Europe
  - Albania (Design only)

Demand for CIRT Enhancements

- Kenya
- Uganda

Cybersecurity Initiatives in the Americas Region

Regional Initiative: Building Confidence and Security in the use of telecommunications / ICTs

Regional initiatives are intended to address specific telecommunication/ICT priority areas, through partnerships and resource mobilization to implement small, medium and large scale projects. Under each regional initiative, projects are developed and implemented to meet the real needs of the region.

Cybersecurity Regional Initiative in the Americas Region for 2015-2017 Period

Regional Initiative 5: Capacity building to engage in global ICT policy, with special focus on improving cybersecurity and developing countries' participation in the existing Internet governance institutions

Objective

To enhance the capacity building of Member States, especially developing countries, with a view to promoting an enabling environment, supporting the implementation of ICT initiatives and encouraging developing countries to participate actively in forums on global ICT policy, in close collaboration with existing institutions.

Expected results:

1) Enhanced coordination and sustained national and regional approaches to cybersecurity
2) Support for institutional and organizational mechanisms at the national and regional levels for the effective implementation of cybersecurity strategies
3) Strengthened ability of developing countries to fully engage in existing Internet governance forums in collaboration with the existing Internet institutions.

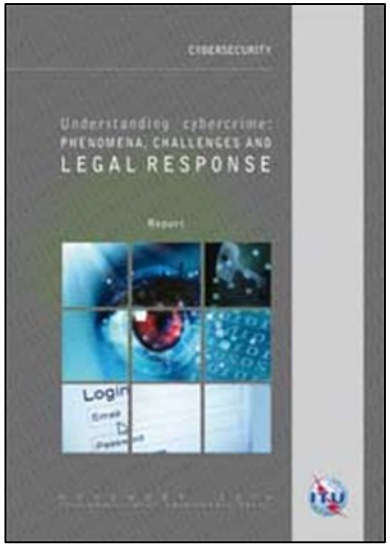
Cybersecurity Activities in the Americas Region

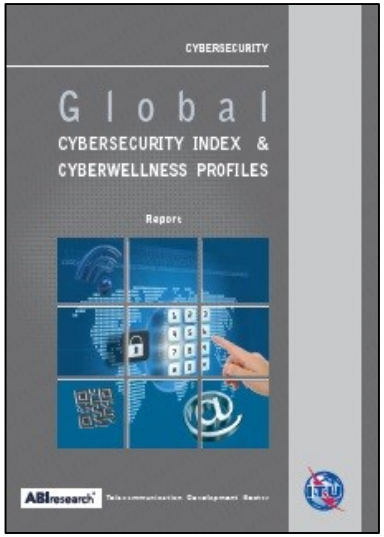
- Ongoing implementation of National CIRT in Barbados
- Discussions to assess National Cybersecurity in Grenada and implement a national CIRT
- Discussions to assess and implement an Academic CIRT in Peru, INICTEL UNI
- Discussions to assess National Cybersecurity in Guatemala and implement a national CIRT. Still pending for the assignment of the budget
- Discussions to assess National Cybersecurity in Honduras and implement a national CIRT. Still pending for the assignment of the budget
- Last year were implemented the National CIRTs in Jamaica and Trinidad and Tobago
- Fourth Regional Cyber Drill for the America in Ecuador, the last one was in last year in Colombia, next year to be determined!

Past Regional Cyber Drills in the America Region

- **2015 – Regional Forum on Cyber security and Third Cyberdrill Applied Learning for Emergency Response Team for the America Region**
  - 3 to 6 August 2015, Bogota, Colombia
  - Hosted by the Ministry of Information, Technology, and Communications of Colombia and The Colombian Chamber for Informatics and Telecommunications (CCTI) and taking place at the University of Los Andes
- **2014 – Applied Learning for Emergency Response Teams**
  - 8 to 10 September 2014, Lima, Peru
  - Co-organized with IMPACT at the invitation of INICTEL UNI
- **2013 – Applied Learning for Emergency Response Teams**
  - 26 to 28 August 2013, Montevideo, Uruguay
  - Co-organized with IMPACT, at the invitation of Latin American and Caribbean Internet Addresses Registry (LACNIC)

Publications





Free download from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx

Thank You

cybersecurity@itu.int