GLOBAL CYBERSECURITY INDEX

An initiative under ITU’s Global Cybersecurity Agenda

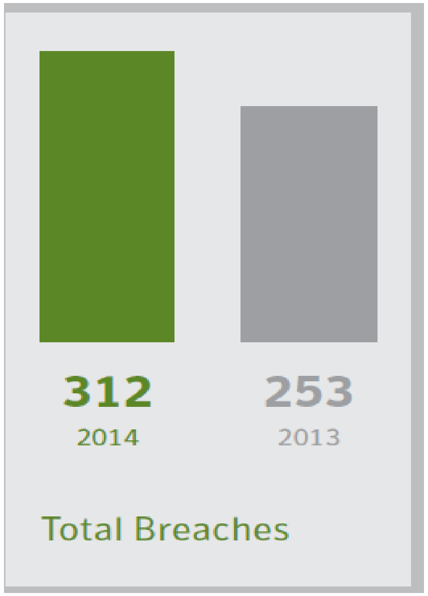
II Cybersecurity Forum
Bogota, 3-5 Aug 2015

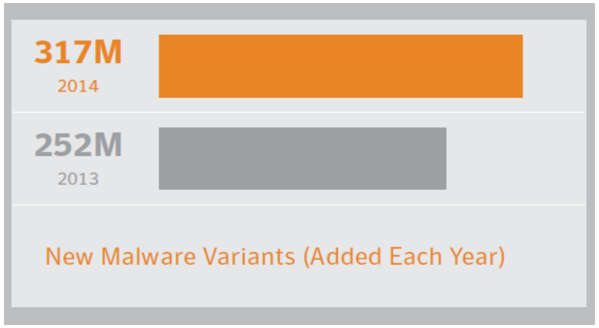
Content

- The importance of Cybersecurity
- GCI 2014
- GCI version 2

The importance of Cybersecurity

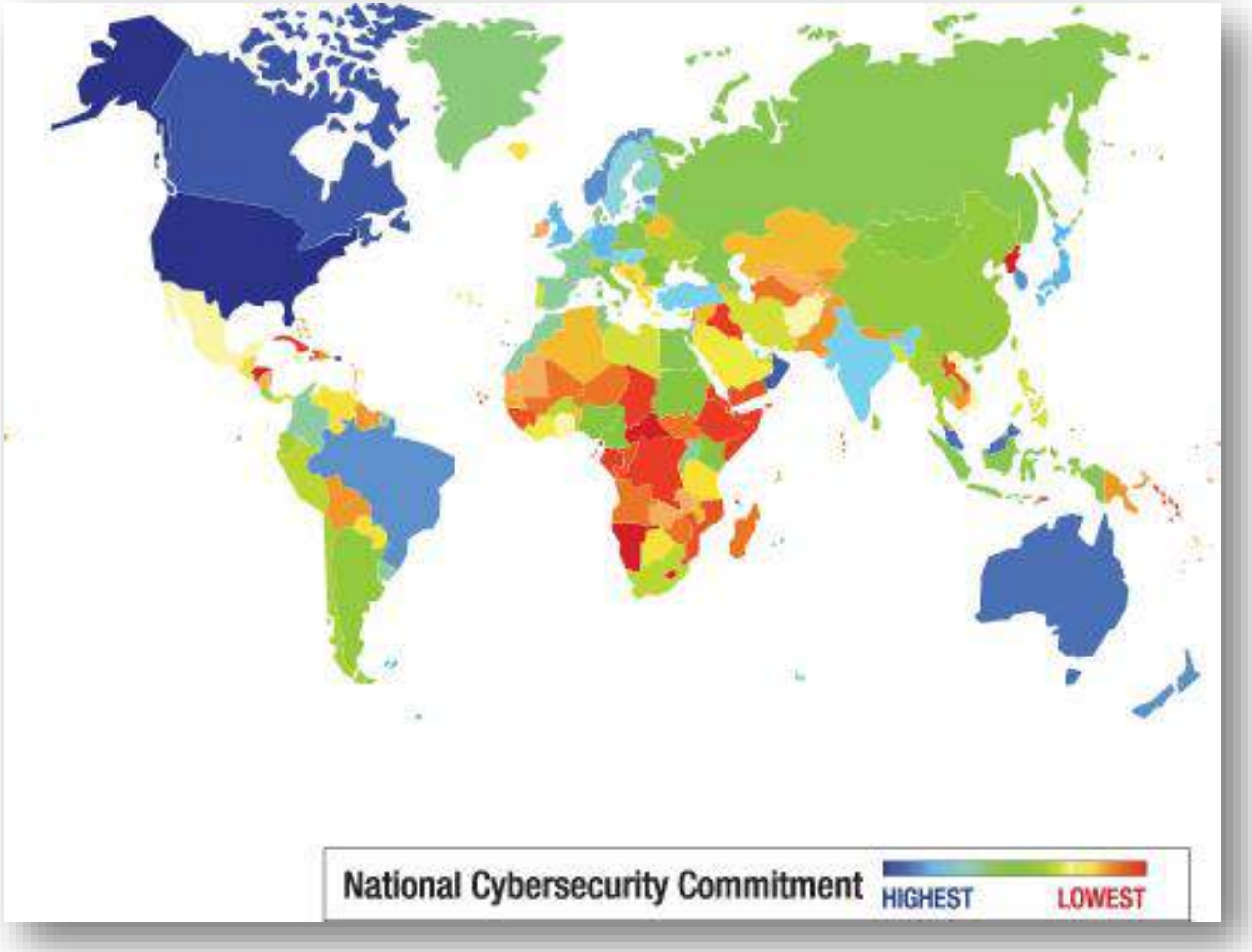
- From industrial age to information societies
  - Increasing dependence on the availability of ICTs
  - Number of Internet users growing constantly (now 40% of world's population)
- Statistics and reports show that cyber-threats are on the rise
  - The likely annual cost to the global economy from Cybercrime is estimated at more than $455 billion *(Source: McAfee Report on Economic Impact of Cybercrime, 2013).*
- Developing countries most at risk as they adopt broader use of ICTs
  - E.g. Africa leading in Mobile-broadband penetration: almost 20% in 2014 - up from less than 2% in 2010 *(Source: ITU ICT Statistics)*
- Need for building cybersecurity capacity
  - Protection is crucial for the socio-economic wellbeing of a country in the adoption of new technologies





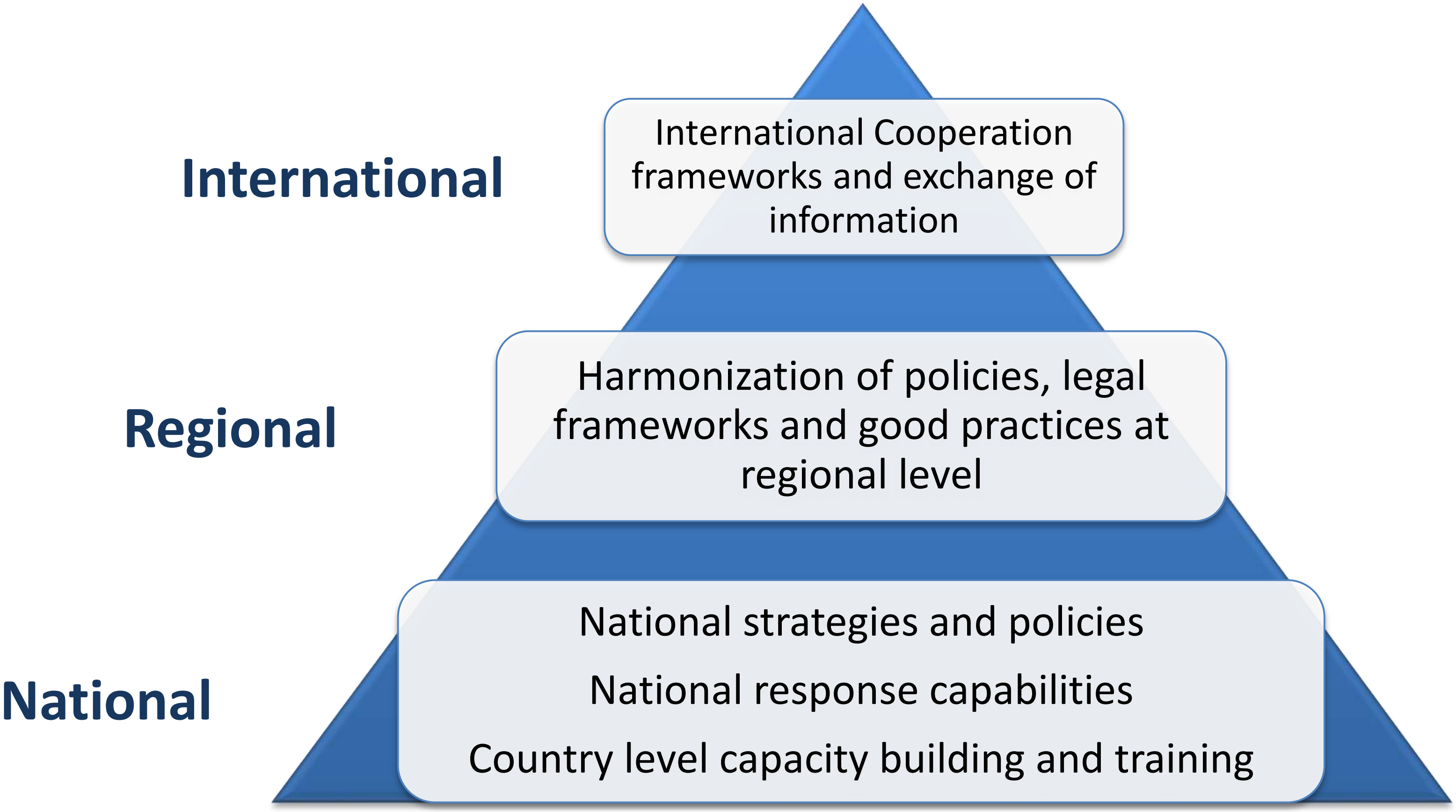
Source: Symantec 2015 Internet Security Threat Report

Level of Commitment of Countries…



Coordinated Response

Need for a multi-level response to the cybersecurity challenges



International

International Cooperation frameworks and exchange of information

Regional

Harmonization of policies, legal frameworks and good practices at regional level

National

National strategies and policies

National response capabilities

Country level capacity building and training

Holistic Approach- Five areas of action

Legal Measures

- Legal Measures Strategy
- Government Legal Authority
- Adequate and harmonized legal frameworks

Technical/Procedural Measures

- National Cybersecurity Goals and Framework
- Secure Government Infrastructure
- Global Technical Collaboration

Organizational Structures

- Government Coordination
- National Focal Point
- National CIRT
- Public-Private Partnerships

Capacity Building

- Cybersecurity Skills and Training
- Culture of Cybersecurity
- Cybersecurity Innovation

International Cooperation

- Enhanced collaboration (multistakeholder, Bi/Multi lateral)
- Inter-Agency Collaboration

GCI 2014

Objective

The Global Cybersecurity Index (GCI) measures and ranks each nation state's level of cybersecurity development in five main areas:

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

Goals

- Promote cyberesecurity 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

Final Global and Regional Results 2014 are on ITU Website

Join us for the Next iteration – we are looking for partners

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

Conceptual Framework

Following the Global Cybersecurity Agenda Framework, the GCI identifies 5 indicators

1. **Legal**

- Criminal Legislation
- Regulation and Compliance

2. **Technical**

- CERT/CIRT/CSIRT
- Standards
- Certification

3. **Organizational**

- Policy
- Roadmap for Governance
- Responsible Agency
- National Benchmarking

4. **Capacity Building**

- Standardization Development
- Manpower Development
- Professional Certification
- Agency Certification

5. **Cooperation**

- Intra-state Cooperation
- Intra-agency Cooperation
- Public-private Partnerships
- International Cooperation

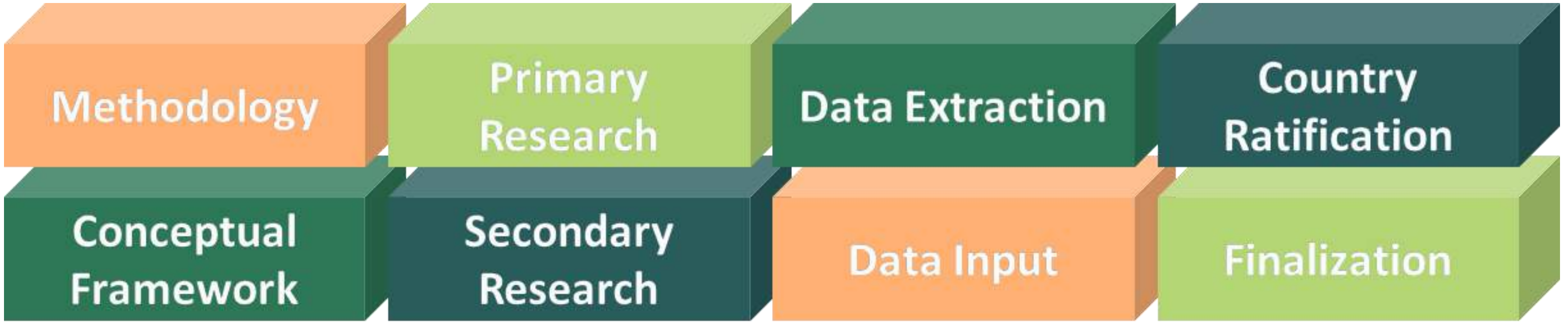
Timeframe and Project Activities

The project represents a combined effort of **18 months**, from inception to publication.

As well as a global rank, the GCI averages ranks in **6 regions**:

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

GCI Research Phases



Methodology

Conceptual Framework

Primary Research

Secondary Research

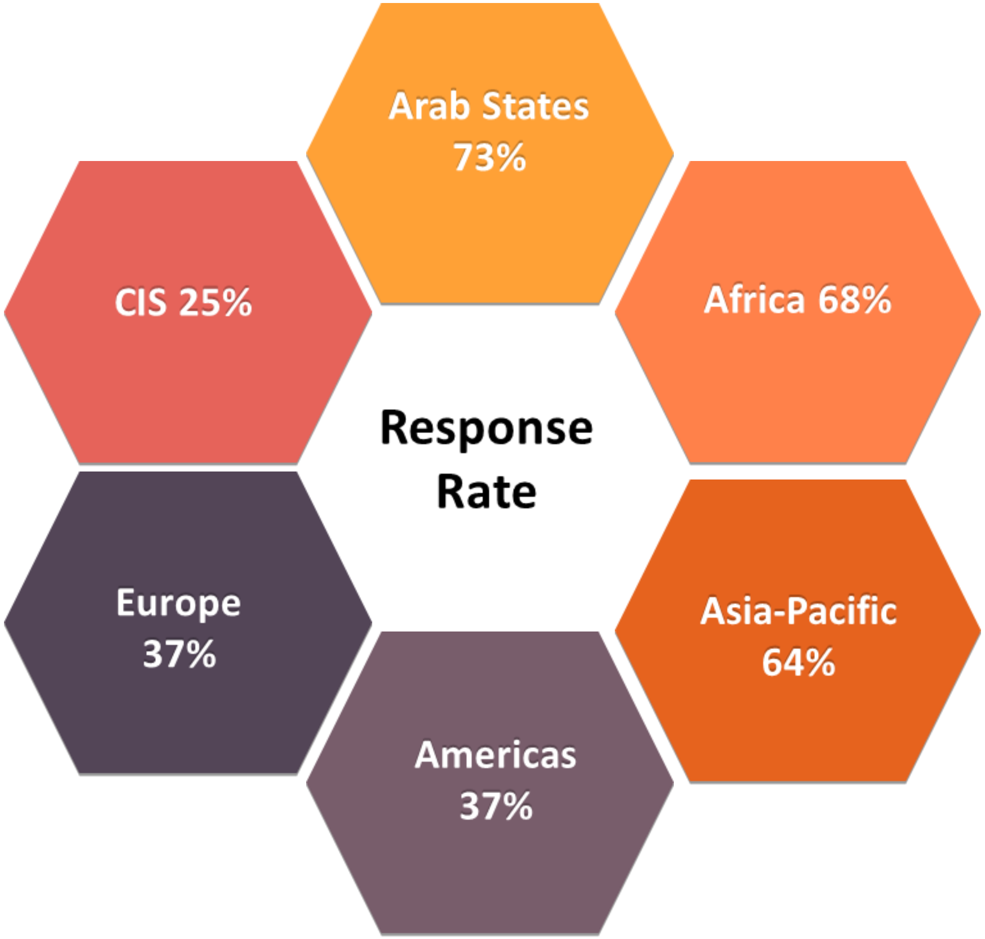
Data Extraction

Data Input

Country Ratification

Finalization

Primary Research



- **Surveys** sent out to all ITU Member States
- Available in **English**, **French** and **Spanish** languages
- **105** total responses received

GCI Results: Top 5

Country	Index	Global Rank
United States of America	**0.824**	**1**
Canada	**0.794**	**2**
Australia	**0.765**	**3**
Malaysia	**0.765**	**3**
Oman	**0.765**	**3**
New Zealand	**0.735**	**4**
Norway	**0.735**	**4**
Brazil	**0.706**	**5**
Estonia	**0.706**	**5**
Germany	**0.706**	**5**
India	**0.706**	**5**
Japan	**0.706**	**5**
Republic of Korea	**0.706**	**5**
United Kingdom	**0.706**	**5**

URUGUAY

LEGAL MEASURES

- **Regulatory Framework on Cybersecurity**
- **Policy on Information Security** in Public Sector
- **Information Security Direction**
- National Computer Incident Response Centre **CERTuy Decree**
- Personal **data protection and habeas data action** Act
- EU Commission decision on the adequate **protection of personal data** by Uruguay (2912)
- Uruguay became the **first non-European state to join COE's personal data protection convention** (2013)

OMAN

TECHNICAL

- **Oman National Computer Emergency Readiness Team** (OCERT)
- Oman's **Information Security Management Framework** is part of the overall ITA standards framework and is based on a structured collection of independent guidelines, processes and practices, primarily from ISO 27011
- **Information Technology Authority** (ITA) as a parent organization of OCERT is **ISO 27001 certified** and encouraging all organizations to adopt and implement the ISO 27001 framework
- Through the **cybersecurity professional development service**, OCERT is providing professional **cybersecurity training** in different security domains by providing information security competency and capability courses and certifications
- The training is **categorized to three levels** (Level 3, Level 2 and Level 1, with Level 1 being the most senior level)

TURKEY

ORGANIZATIONAL

- The **National Cybersecurity Strategy and Action Plan** 2013 -2014
- The action plan consists of **29 main actions** and **95 sub-actions** and assigns responsibilities about legislation, capacity building, development of technical infrastructure, etc.
- The **Cybersecurity Board** was established in order to determine the measures regarding cybersecurity; to approve the prepared plans, programs, reports, procedures, principles, and standards; and ensure their application and coordination
- In the last 3 years, **three cybersecurity exercises** were organized at **the national level** with participants from both the public and private sector. The exercise played a big role in **raising awareness** of cybersecurity and also were a great tool for **measuring the development** of cybersecurity.

AZERBAIJAN

CAPACITY BUILDING

- Azerbaijan Ministry of Communications and High Technologies has officially recognized national or sector-specific **research and development programs/projects for cybersecurity** standards, best practices, and guidelines to be applied in the private and the public sector
- The Technical Committee is to implement the **preparation of national standards** on the basis of international (regional) and interstate standards
- Azerbaijan conducts **short training courses on E-government and information security**
- AZ-CERT organizes **capture-the-flag competitions** to enhance professional competence in information security
- The IT and Communications Department of the State Oil Company of Azerbaijan Republic (SOCAR) **is certified under ISO 27001:2005**
- SOCART IT and Communications Department is certified under ISO 27001:2005

REPUBLIC OF KOREA

COOPERATION

- KISA has in place a number of **memorandums of understanding on cybersecurity cooperation** with the following: OCSIA (United Kingdom), INCB (Israel), Australia, CNCERT (China), STS (Kazakhstan), CERT Romania, Korea-China-Japan CERT and private sector cooperation with Microsoft, Checkpoint and McAfee
- **Information Communications Infrastructure Protection Committee** to decide and deliberate on protection of critical ICT infrastructure to guarantee national security and stabilize the life of people
- **National Cybersecurity Conference**: Private/public/military response team (Art. 8) organized and operated for decision-making on cyber threats, situation monitoring, analyzing of threats and joint investigation
- **Cooperation and participation** in meetings with **APCERT** (Asia-Pacific Computer Emergency Response Team), **FIRST** (Forum on Incident Response and Security Teams)

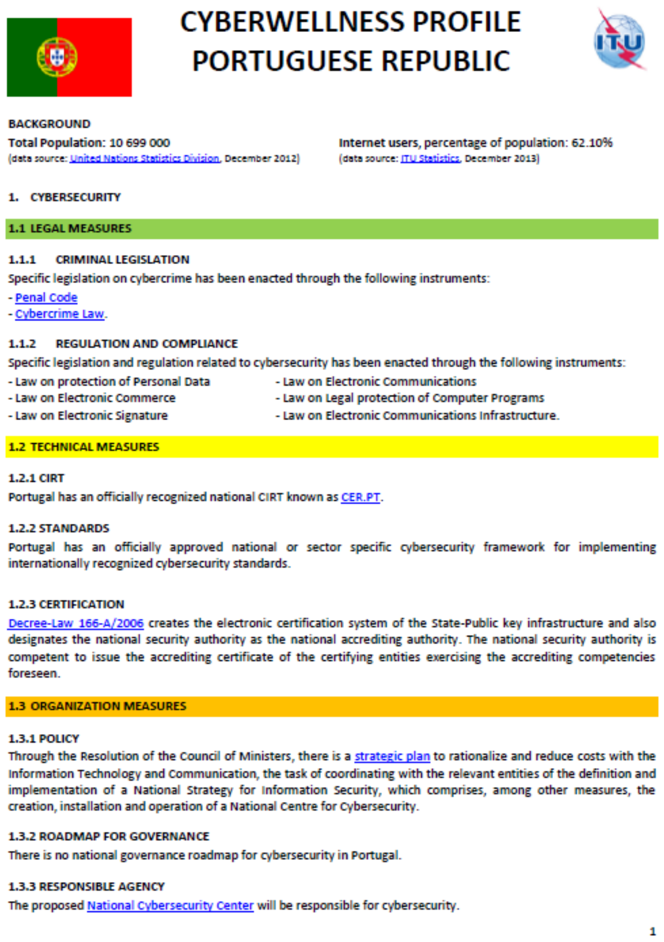
Cyberwellness Country Profiles

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

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

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

EXAMPLE ⟶



CYBERWELLNESS PROFILE
PORTUGUESE REPUBLIC

BACKGROUND

Total Population: 10 699 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 62.10%
(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:
- Penal Code
- Cybercrime Law.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:
- Law on protection of Personal Data
- Law on Electronic Commerce
- Law on Electronic Signature
- Law on Electronic Communications
- Law on Legal protection of Computer Programs
- Law on Electronic Communications Infrastructure.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Portugal has an officially recognized national CIRT known as CER.PT.

1.2.2 STANDARDS

Portugal has an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

Decree-Law 166-A/2006 creates the electronic certification system of the State-Public key infrastructure and also designates the national security authority as the national accrediting authority. The national security authority is competent to issue the accrediting certificate of the certifying entities exercising the accrediting competencies foreseen.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Through the Resolution of the Council of Ministers, there is a strategic plan to rationalize and reduce costs with the Information Technology and Communication, the task of coordinating with the relevant entities of the definition and implementation of a National Strategy for Information Security, which comprises, among other measures, the creation, installation and operation of a National Centre for Cybersecurity.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national governance roadmap for cybersecurity in Portugal.

1.3.3 RESPONSIBLE AGENCY

The proposed National Cybersecurity Center will be responsible for cybersecurity.

1

GCI Version 2

GCI Version 2

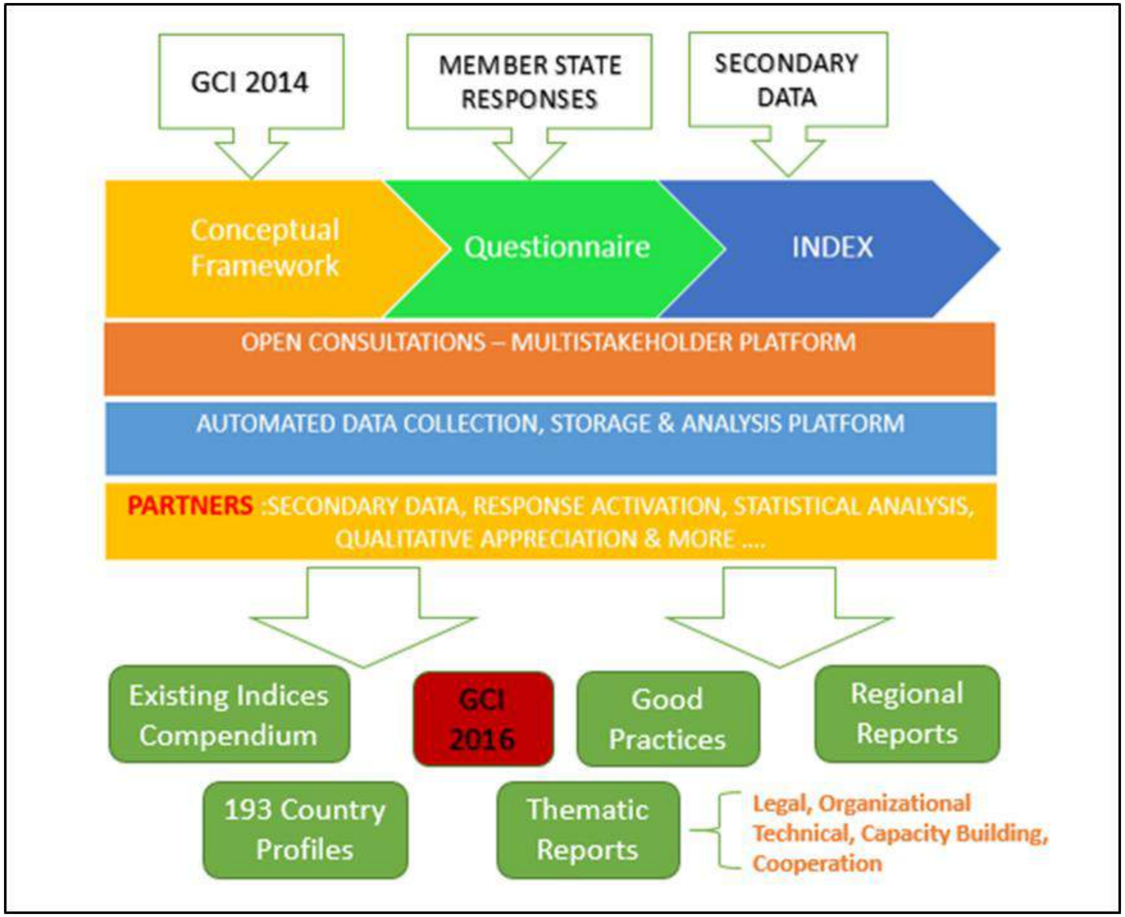
- Resolution 130 (Rev. Busan, 2014)

“invites Member States to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI) …”

What is new?

- Have a unique value addition to the sphere of existing Cybersecurity indices
- Capture more details on Cybersecurity
- Enhance consultation with Member States
- Expand the partnerships into a multi-stakeholder collaborative platform

Overall Approach


GCI 2014
MEMBER STATE RESPONSES
SECONDARY DATA
Conceptual Framework
Questionnaire
INDEX
OPEN CONSULTATIONS – MULTISTAKEHOLDER PLATFORM
AUTOMATED DATA COLLECTION, STORAGE & ANALYSIS PLATFORM
PARTNERS :SECONDARY DATA, RESPONSE ACTIVATION, STATISTICAL ANALYSIS, QUALITATIVE APPRECIATION & MORE ....
Existing Indices Compendium
GCI 2016
Good Practices
Regional Reports
193 Country Profiles
Thematic Reports
Legal, Organizational Technical, Capacity Building, Cooperation

Unique Value Addition

What makes the GCI unique is the balanced combination of:

- The broad geographic range covering all Member States of ITU
- The study of cybersecurity in five broad areas (pillars of Global Cybersecurity Agenda)
- The scoring and ranking mechanisms
- The cyberwellness country profiles

Index of Indices has been submitted as a contribution to the work of ITU D SG2 Q 3/2.

More details captured

- Go beyond 5 pillars of Global Cybersecurity Agenda (GCA)
- Go in more details on each pillar
- Address elements needed by SG2Question3
- Address elements for Connect 2020

➢ Goal 3 Sustainability: Manage Challenges resulting for telecommunications / ICT development

➢ Target 3.1. Improve cybersecurity readiness by 40%

Improved consultation with Member States

- Study group 2 Question 3
  - Contribution submitted for rapporteurs’ meeting of 29 April
  - SG 3/2 agreed to review and endorse the GCIv2, and to make it the main instrument for data collection to meet their own needs.
  - Open consultation for 1 month in July
  - The SG 3/2 will endorse the harmonized questionnaire at main meeting of September 2015

- WSIS Forum
  - 2015: release of GCI 2014 report and inform on new version preparation
  - 2016: announcement of Global Results based on GCI version 2
  - Every WSIS event thereafter: annual results announced

Expansion of Tiered Partnerships

- “Primary” Partners : ABI Research
  - Commitment, Continuity, Positive Experience, Expertise
- New “Contributing” Partners
  - Domain Experts, Academia, Industry, Other organizations doing similar work
- Partnership
  - Expertise (Index Development, Statistical analysis, Software tools provision, Qualitative review of results
  - Data sharing
  - Funding

High level Work Plan

Index of indices	June 2015
New partnerships	July 2015
Draft questionnaire & conceptual framework	mid-July 2015
Open consultations	mid-July 2015
Final questionnaire & conceptual framework	Sep 2015
Circular letter to MS with online questionnaire	Oct 2015
Data collection	Oct 2015 – mid-March 2016
Analysis of responses	mid-April 2016
GCIv2 results & all other deliverables	May 2016

What is GCI for you …

- “Help us to build a tool that you can use to gauge your cybersecurity readiness and to take informed decision thereon” K. Huseinovic, ITU

- “The GCI is a collaborative index not a competitive one” A. Boyd, ABI Research

- “GCI is a capacity building tool, nothing more than that”

M. Obiso, ITU

JOIN US

- As a partner
  - o Add to this body of knowledge under construction
  - o Your expertise on thematic to help enhance the GCI process and deliverables
  - o Connect better with ITU and Member States

- As a respondent to a questionnaire
  - o Reflect your Country's achievements and plans for enhancing cybersecurity
  - o Share best practices
  - o Position your country on the cybersecurity commitment scale

Some Upcoming ITU Cybersecurity Events

- Cyberdrills
  - Americas: Colombia 3 – 6 Aug 2015
  - Europe & CIS: Montenegro 30 Sep – 2 Oct 2015

- Study Group Meetings
  - ITU-T SG17 Meeting, 8 – 17 Sep 2015
  - Cybersecurity Workshop, 8 Sep 2015
  - ITU-D SG2Q3 Meeting, 9 Sep 2015

- International Conference “Keeping Children and Young People Safe Online”, Warsaw, Poland, 22-23 Sep 2015
- Cybersecurity Conference, Sibiu, Romania, 24-25 Sep 2015

www.itu.int/cybersecurity

Thank You

Tym Kurpeta
Project Manager
ABI Research
kurpeta@abiresearch.com

ABIresearch®