Regional Seminar on Cyber Preparedness
Organised by World Bank Group, Financial Sector Advisory Center (FINSec)

ITU’s work in Cybersecurity and Global Cybersecurity Index (GCI)

Vijay Mauree
Programme Coordinator,
International Telecommunication Union (ITU)
Outline

• About ITU
• ITU Mandate on Cybersecurity
• Global Cybersecurity Index
• ITU-T Study Group 17
• Focus Group Digital Financial Services
• WSIS Forum 2015
ITU is the specialized agency of the UN for telecommunications and ICTs …

… and turns 150 years in 2015

Theme for all year celebrations:
“Telecommunications and ICTs: drivers of innovation”
ITU allocates (1) frequency spectrum to different services, (2) satellite orbit assignments, (3) numbers and identifiers
ITU develops standards
ITU assists developing countries in building up their ICT infrastructure
ITU’s Membership: Public-private partnership

- 193 Member States and Regulatory Bodies
- 750 Sector Members (Companies, Business Associations, NGOs)
- 90+ Academia (Universities & Research Establishments)

(as of May 2015)
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”

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.

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.
Global Cybersecurity 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.
GCA: From Strategy to Action

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’s Child Online Protection (COP)
- Collaboration with UN, and other IGOs, as well as with Symantec, Trend Micro, ABI research, ISOC, Interpol, FIRST, CCI, CTO, & UNODC
Global Cybersecurity Index

Objective
The Global Cybersecurity Index (GCI) aims to measure the level of commitment of each nation in cybersecurity in five main areas:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- National and International Cooperation
104 countries have responded

Final Global and Regional Results 2014 are on ITU Website

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

Next iteration in progress
Many countries share the same ranking which indicates that they have the same level of readiness. The index has a low level of granularity since it aims at capturing the cybersecurity commitment/preparedness of a country and NOT its detailed capabilities or possible vulnerabilities.
## Top three of each region

<table>
<thead>
<tr>
<th>Country – Africa</th>
<th>Index</th>
<th>Regional Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mauritius</td>
<td>0.5882</td>
<td>1</td>
</tr>
<tr>
<td>Uganda</td>
<td>0.5588</td>
<td>2</td>
</tr>
<tr>
<td>Rwanda</td>
<td>0.5294</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country – Americas</th>
<th>Index</th>
<th>Regional Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States of Americas</td>
<td>0.8235</td>
<td>1</td>
</tr>
<tr>
<td>Canada</td>
<td>0.7941</td>
<td>2</td>
</tr>
<tr>
<td>Brazil</td>
<td>0.7059</td>
<td>3</td>
</tr>
</tbody>
</table>
## Top three of each region

<table>
<thead>
<tr>
<th>Country – Arab States</th>
<th>Index</th>
<th>Regional Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oman</td>
<td>0.7647</td>
<td>1</td>
</tr>
<tr>
<td>Qatar</td>
<td>0.6176</td>
<td>2</td>
</tr>
<tr>
<td>Egypt</td>
<td>0.5882</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country – Asia Pacific</th>
<th>Index</th>
<th>Regional Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>0.7647</td>
<td>1</td>
</tr>
<tr>
<td>Malaysia</td>
<td>0.7647</td>
<td>1</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0.7353</td>
<td>2</td>
</tr>
<tr>
<td>India</td>
<td>0.7059</td>
<td>3</td>
</tr>
<tr>
<td>Japan</td>
<td>0.7059</td>
<td>3</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>0.7059</td>
<td>3</td>
</tr>
</tbody>
</table>
## Top three of each region

<table>
<thead>
<tr>
<th>Commonwealth of Independent States</th>
<th>Index</th>
<th>Regional Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azerbaijan</td>
<td>0.5294</td>
<td>1</td>
</tr>
<tr>
<td>Georgia</td>
<td>0.5000</td>
<td>2</td>
</tr>
<tr>
<td>Russia</td>
<td>0.5000</td>
<td>2</td>
</tr>
<tr>
<td>Moldova</td>
<td>0.3824</td>
<td>3</td>
</tr>
</tbody>
</table>
## Top three of each region

<table>
<thead>
<tr>
<th>Country – Europe</th>
<th>Index</th>
<th>Regional Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norway</td>
<td>0.7353</td>
<td>1</td>
</tr>
<tr>
<td>Estonia</td>
<td>0.7059</td>
<td>2</td>
</tr>
<tr>
<td>Germany</td>
<td>0.7059</td>
<td>2</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>0.7059</td>
<td>2</td>
</tr>
<tr>
<td>Austria</td>
<td>0.6765</td>
<td>3</td>
</tr>
<tr>
<td>Hungary</td>
<td>0.6765</td>
<td>3</td>
</tr>
<tr>
<td>Israel</td>
<td>0.6765</td>
<td>3</td>
</tr>
<tr>
<td>Netherlands</td>
<td>0.6765</td>
<td>3</td>
</tr>
</tbody>
</table>
Cyberwellness Country Profiles

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

Over 196 profiles to date

Live documents – Invite countries to assist us in maintaining updated information cybersecurity@itu.int

EXAMPLE →
Next GCI – results in 2016

GCI is a component in PP-14 Resolution 130 (Busan, 2014)

**Ultimate 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

**Next Steps**
Open GCI to industry and academia partners
Evolution to GCI version 2 – deeper and wider

Contact us at cybersecurity@itu.int
Building a global partnership

Capacity building initiatives, joint consultations and more.

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-T Study Group 17

• ITU-T cybersecurity standards provide critical instruments to deal with rapidly changing and diversifying cybersecurity phenomena, directly contributing to data protection.

• Enumeration standards provides effective means of communication across businesses, government agencies as well as communities.

• Cyber-risks are highly volatile and manifests through unexpected combination of components, that requires careful examination of technical risks through knowledge-base standards.
ITU-T SG 17 Cybersecurity Recommendations

- Cybersecurity:
  - Overview of cybersecurity (Rec. ITU-T X.1205)
  - A vendor-neutral framework for automatic notification of security related information and dissemination of updates (Rec. ITU-T X.1206)
  - Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software (Rec. ITU-T X.1207)
  - A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies (Rec. ITU-T X.1208)
  - Capabilities and their context scenarios for cybersecurity information sharing and exchange (Rec. ITU-T X.1209)
  - Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks (Rec. ITU-T X.1210)
Question 4/17: Cybersecurity

- Cybersecurity by design no longer possible; a new paradigm:
  - know your weaknesses → minimize the vulnerabilities
  - know your attacks → share the heuristics within trust communities
- Current work program (17 Recommendations under development)
  - X.1500 suite: Cybersecurity Information Exchange (CYBEX) – non-prescriptive, extensible, complementary techniques for the new paradigm
    - Weakness, vulnerability and state
    - Event, incident, and heuristics
    - Information exchange policy
    - Identification, discovery, and query
    - Identity assurance
    - Exchange protocols
  - Non-CYBEX deliverables include compendiums and guidelines for
    - Abnormal traffic detection
    - Botnet mitigation
    - Attack source attribution (including traceback)
  - Extensive relationships with many external bodies
CYBEX Recommendations

- CYBERSECURITY INFORMATION EXCHANGE (CYBEX):
  - Overview of cybersecurity information exchange (Rec. ITU-T X.1500)
  - Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange (Rec. ITU-T X.1500.1)
  - Common vulnerabilities and exposures (Rec. ITU-T X.1520)

Rec. ITU-T X.1500 - CYBEX model
CYBEX Recommendations

- CYBEX vulnerability/state exchange:
  - Common vulnerability scoring system (Rec. ITU-T X.1521)
  - Common weakness enumeration (Rec. ITU-T X.1524)
  - Common weakness scoring system (Rec. ITU-T X.1525)
  - Language for the open definition of vulnerabilities and for the assessment of a system state (Rec. ITU-T X.1526)
  - Common platform enumeration (Recs. ITU-T X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4)
Knowledge base of vulnerabilities

• CVE: Common Vulnerability Enumeration
  – A structured means to exchange information on security vulnerabilities and exposures and provides a common identifier for publicly-known problems.
  – http://cve.mitre.org/
  – Standardized as Recommendation ITU-T X.1520

  – National databases:
    • U.S. NIST NVD
    • Japan JVN
Example: vulnerabilities of widely used software for data protection purposes

### CVE entries for MySQL

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2014-5104</td>
<td>Multiple SQL injection vulnerabilities in ol-commerce 2.1.1 allow remote attackers to execute arbitrary SQL commands via the (1) a_country parameter in a process action to affiliate_signup.php, (2) affiliate_banner_id parameter to affiliate_show_banner.php, (3) country parameter in a process action to create_account.php, or (4) entry_country_id parameter in an edit action to admin/create_account.php.</td>
</tr>
<tr>
<td>CVE-2014-4987</td>
<td><code>server_user_groups.php</code> in <code>phpMyAdmin</code> version 5.6.17 and earlier allows remote authenticated users to bypass MySQL user list via a viewUsers request.</td>
</tr>
<tr>
<td>CVE-2014-4260</td>
<td>Unspecified vulnerability in the MySQL Server earlier, and 5.6.17 and earlier, allows remote and availability via vectors related to SRV.</td>
</tr>
</tbody>
</table>

### CVE entries for OpenSSL

<table>
<thead>
<tr>
<th>#</th>
<th>CVE ID</th>
<th>CWE ID</th>
<th># of Exploits</th>
<th>Vulnerability Type(s)</th>
<th>Publish Date</th>
<th>Update Date</th>
<th>Score</th>
<th>Gained Access Level</th>
<th>Access</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CVE-2014-5139</td>
<td>DoS</td>
<td></td>
<td></td>
<td>2014-08-13</td>
<td>2014-08-15</td>
<td>4.3</td>
<td>None</td>
<td>Remote</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>CVE-2014-3512</td>
<td>119</td>
<td>DoS</td>
<td></td>
<td>2014-08-13</td>
<td>2014-08-14</td>
<td>7.5</td>
<td>None</td>
<td>Remote</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>CVE-2014-3511</td>
<td></td>
<td></td>
<td></td>
<td>2014-08-13</td>
<td>2014-08-14</td>
<td>4.3</td>
<td>None</td>
<td>Remote</td>
<td>Medium</td>
</tr>
</tbody>
</table>

The `ssl_set_client_disabled` function in `ssl_ciphers` before 1.0.1 allows remote attackers to execute arbitrary commands via a `ServerHello message that includes SRP ciphersuite with client`. The `ssl_set_client_hello` function in `ssl_ciphers` before 1.0.1 allows man-in-the-middle attacks triggering `ClientHello message fragmentation in communication between a client and server that both supports TLS protocol downgrades`. |
Taxonomy of vulnerabilities

- CWE: Common Weakness Enumeration
  - Group same kind of vulnerabilities into a weakness, and give it a distinct number
  - Provides common names for publicly known problems in the commercial or open source software
  - Intended for security tools and services that can find weaknesses in source code and operational systems
  - Helps better understand and manage software weaknesses related to architecture and design

- http://cwe.mitre.org/
  - Standardized as Recommendation ITU-T X.1524
Improving cybersecurity and data protection throughout IT infrastructure lifecycle

Development
- CWE X.1524
- CAPEC X.1544

Deployment
- CVE X.1520
- CVSS X.1521

Assessment
- OVAL X.1526
- CPE X.1528
ITU Focus Group Digital Financial Services

- Low levels of financial inclusion represent a barrier to socio economic development in developing countries.
- Globally, more than 2 billion adults do not have a formal bank account, most of them in developing economies.
- 59% of adults in the developing countries do not have a formal bank account.
- But 1.6 billion have a mobile phone.
- This presents an opportunity to overcome the financial inclusion problem.
- Digital Financial Services allows the "unbanked" to access basic financial services – not necessarily a formal bank account, but to be able to receive money or make payments via the mobile phone.
ITU Focus Group Digital Financial Services

• Chaired by Sacha Polverini, Bill & Melinda Gates Foundation
• ITU Contact: Vijay Mauree, Programme Coordinator
• Web: http://www.itu.int/en/ITU-T/focusgroups/dfs/
• Next Meetings:
  – End September, Malaysia
  – 15-17 December, ITU, Geneva
Dialogue between ICT and Financial Services Regulators

• Interoperability
• Foster best practices to encourage competition
• Agree on quality of service of mobile networks for digital financial services
• Consumer Protection
• Data Security
Working Groups

- Interoperability
- DFS Ecosystem
- Working Groups
- Consumer Experience & Protection
- Technology, Innovation & Competition
Working Groups

• Mailing Lists
  – Focus Group Digital Financial Services: fgdfs@lists.itu.int
  – Working Group Mailing Lists
    • DFS Ecosystem: dfseco@lists.itu.int
    • Consumer Experience & Protection: dfscep@lists.itu.int
    • Interoperability: dfsinterop@lists.itu.int
    • Technology, Innovation & Competition: dfstic@lists.itu.int
28 May @ 14h
*GCI & Cyberwellness profiles publication*

29 May@ 11h
*Digital Financial Services and Financial Inclusion Workshop*

Thank You

More info @ http://www.itu.int/cybersecurity