Ensuring Trust and Confidence in use of ICT

14 September 2017
Colombo, Sri Lanka

Sameer Sharma , Senior Advisor ITU
Shahryar Khan, ITU Expert

Agreed Global Telecommunication/ICT Targets - 2020

Goal 1 Growth : Enable and foster access to and increased use of telecommunications/ICTs

55%
of households should have access to the Internet

60%
of individuals should be using the Internet

40%
Telecommunications/ICTs should be **40%** more affordable

GROWTH

Goal 2 Inclusiveness – Bridge the digital divide and provide broadband for all

50%
of households should have access to the Internet in the developing world; **15%** in the least developed countries

50%
of individuals should be using the Internet in the developing world; **20%** in the least developed countries

40%
affordability gap between developed and developing countries should be reduced by **40%**

5%
Broadband services should cost no more than **5%** of average monthly income in the developing countries

INCLUSION

90%
of the rural population should be covered by broadband services

Gender equality among Internet users should be reached

Enabling environments ensuring accessible ICTs for persons with disabilities should be established in all countries

Goal 3 Sustainability – Manage challenges resulting from the telecommunication/ICT development

40%
improvement in cybersecurity readiness

50%
reduction in volume of redundant e-waste

30%
decrease in Green House Gas emissions per device generated by the telecommunication/ICT sector

SUSTAINABILITY

Goal 4 Innovation and partnership – Lead, improve and adapt to the changing telecommunication/ICT environment

Telecommunication/ICT environment conducive to innovation

Effective partnerships of stakeholders in telecommunication/ICT environment

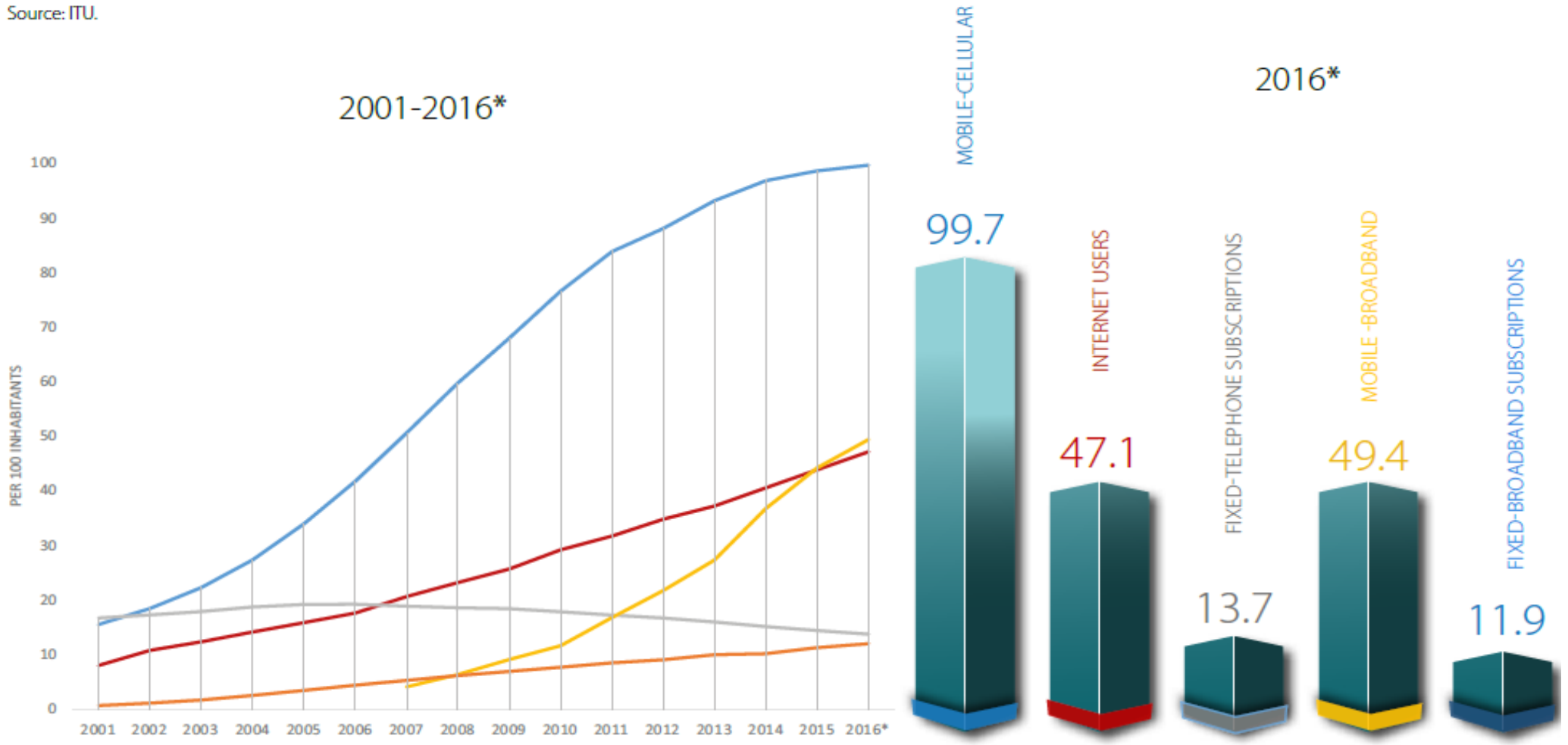
INNOVATION

CELEBRATING 25 YEARS OF ACHIEVEMENTS

Global ICT Developments Worldwide

Note: *Estimates.

Source: ITU.



CELEBRATING 25 YEARS OF ACHIEVEMENTS

Internet of Things

The ITU-T's definition of the IoT calls it "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"

What Is It?

"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication" (ITU-T)

Who Makes It?

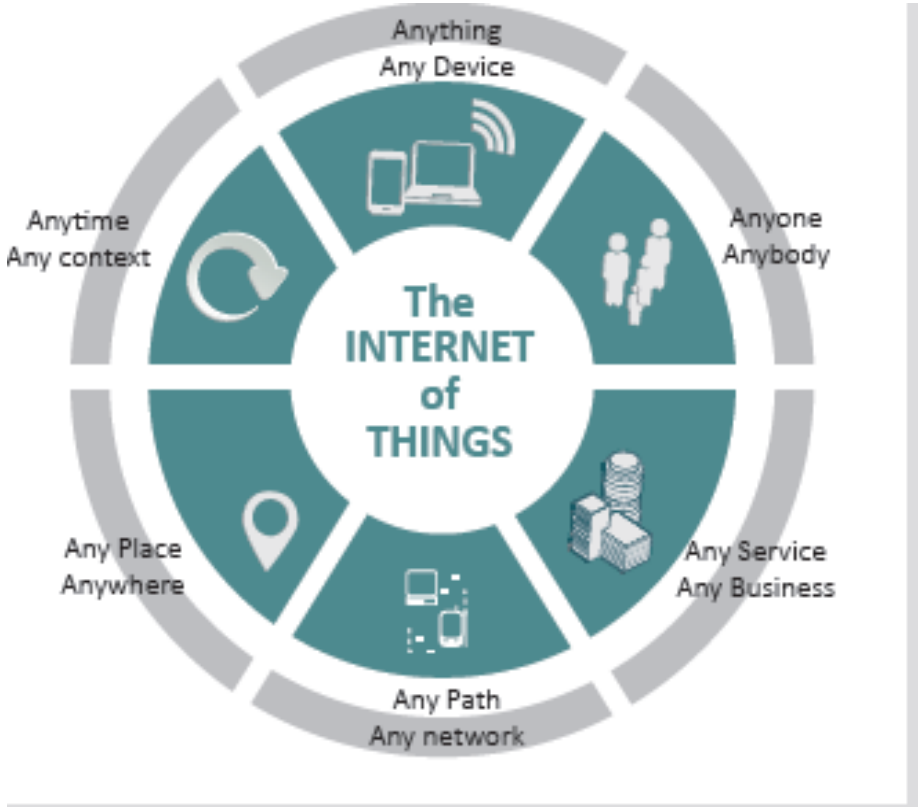
Device manufacturers, network operators, application platforms, software developers and (cloud-based) data analytics services providers

How Is It Accessed?

Connection of IoT devices via Wi-Fi, Bluetooth, mobile phone networks, specialized radio networks, global Internet

Main current areas of investment

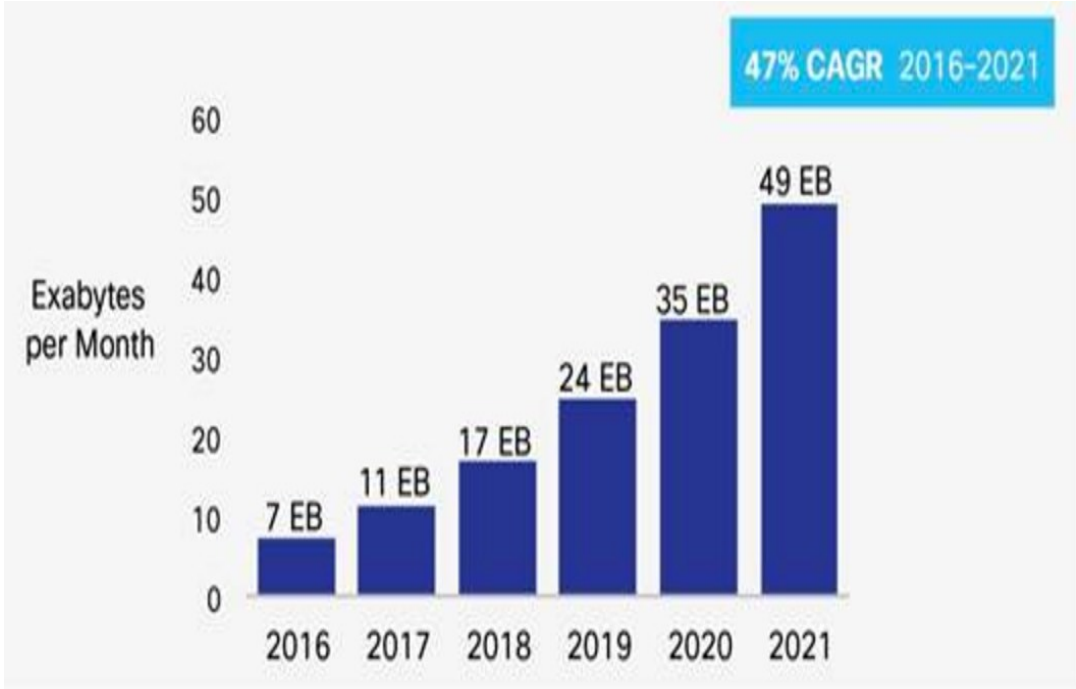
- Smart cities
- Smart metering & grids
- Connected vehicles
- Healthcare



CELEBRATING 25 YEARS OF ACHIEVEMENTS

Digital Content: Disrupting and Empowering

- The disruption that the app economy and digital content has caused has also, in turn, revolutionized the world and empowered consumers.
- By the year 2021, there will be **4.6 billion global internet users** and **27.1 billion network devices and connections.**
- Global mobile data traffic is expected to grow to **49 exabytes per month by 2021**, a sevenfold increase over 2016.
- These trends alongside disruptive innovations have enabled consumers to become empowered along technological, social, economic and legal dimensions.



Source: Cisco VNI Mobile, 2017

Digital Societies: Emerging Policy and Regulatory issues

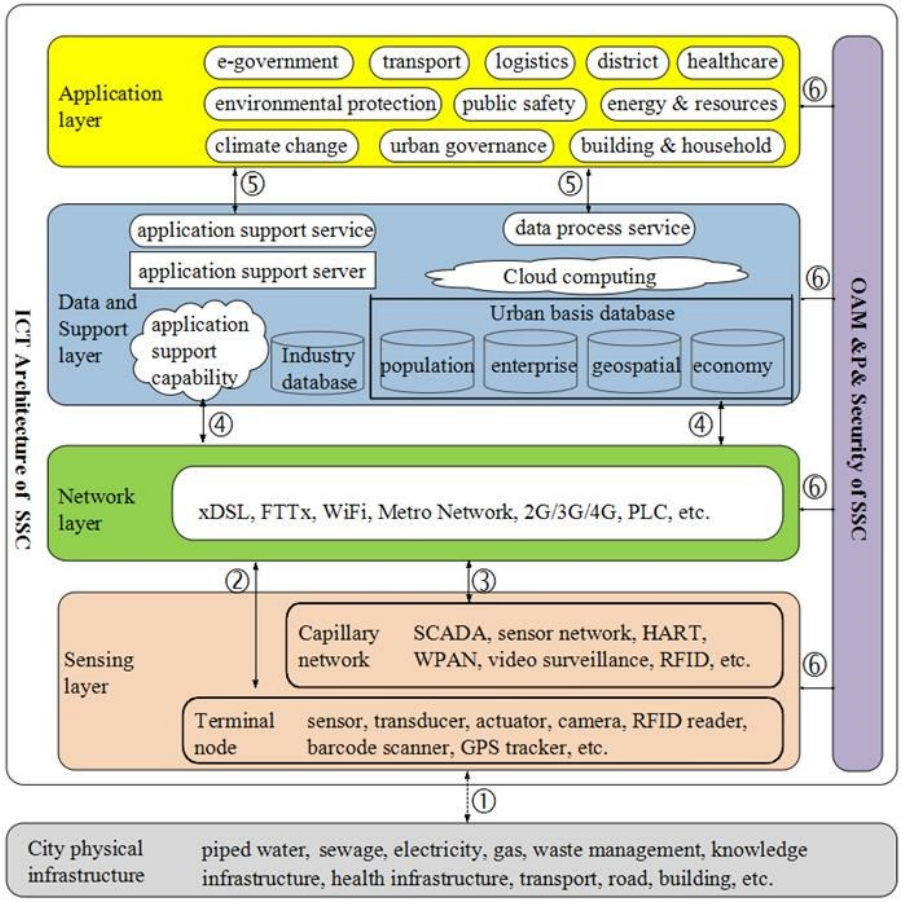
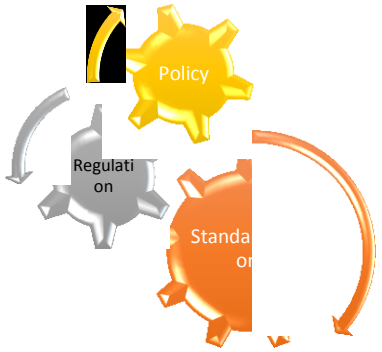


Figure source: ITU-T Focus Group on Smart Sustainable Cities: *Overview of smart sustainable cities infrastructure*

A multi-tier SSC (smart sustainable city) ICT architecture from communication view (physical perspective)

Telecom/ ICT Sector Issues (examples)



- Cross-Sector Collaboration
- Competition
- Investment
- Licensing
- Spectrum
- HetNets
- Broadband
- Cloud
- Roaming
- Interoperability
- QoS/QoE, Consumer
- Numbering & Addressing
- Big Data & Open Data
- Security
- Privacy
- Right of Way
- Green ICTs
- Infrastructure Sharing
- Data Centres
- e-Waste
- Number Portability
- Emergency Telecommunications

CELEBRATING 25 YEARS OF ACHIEVEMENTS

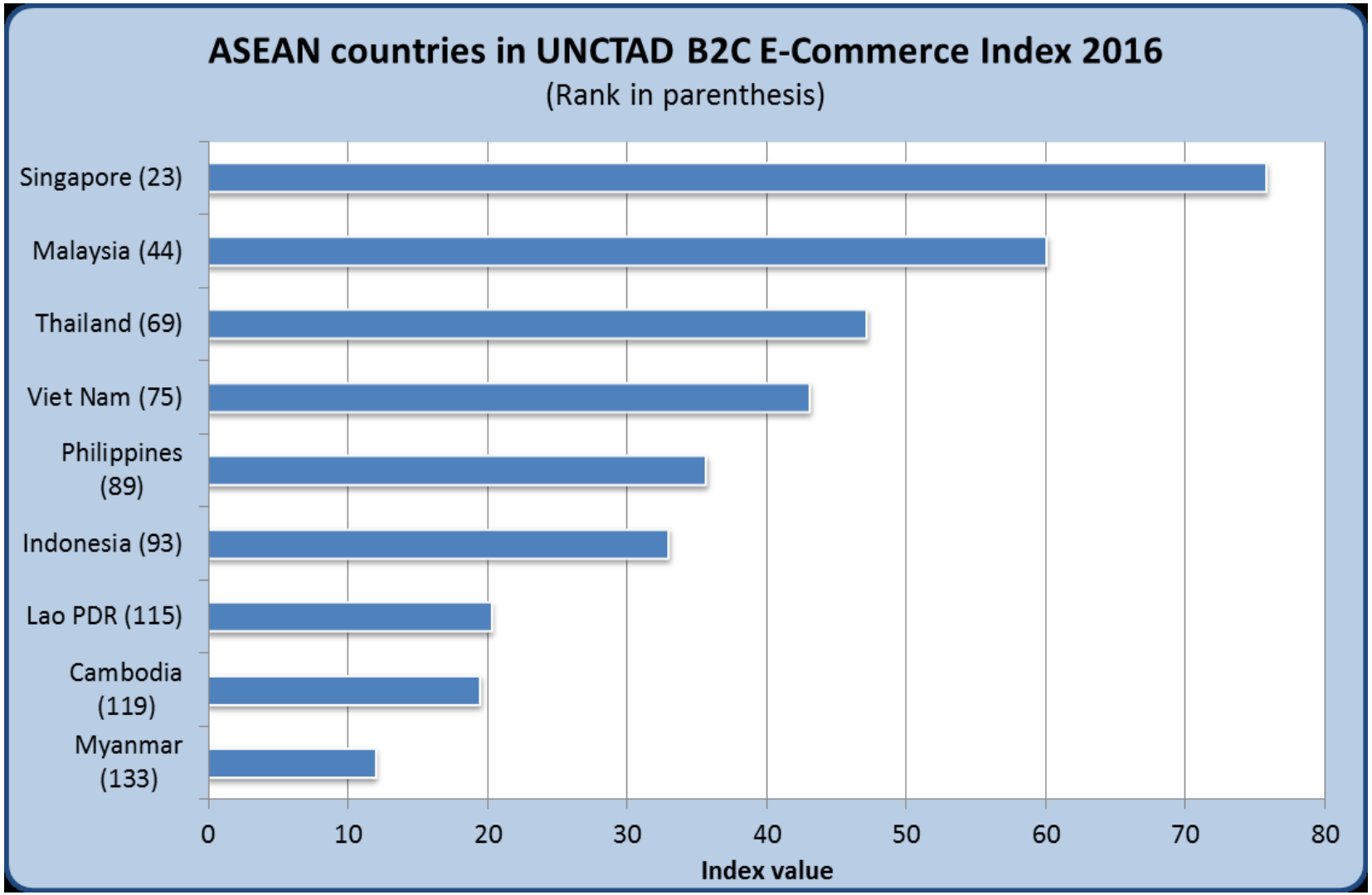
Major E-commerce Markets

		Total		B2B		B2C
	Economy	$ billion	% of GDP	$ billion	% of all e-commerce	$ billion
1	United States	7,055	39%	6,443	91%	612
2	Japan	2,495	60%	2,382	96%	114
3	China	1,991	18%	1,374	69%	617
4	Korea (Rep.)	1,161	84%	1,113	96%	48
5	Germany (2014)	1,037	27%	944	91%	93
6	United Kingdom	845	30%	645	76%	200
7	France (2014)	661	23%	588	89%	73
8	Canada (2014)	470	26%	422	90%	48
9	Spain	242	20%	217	90%	25
10	Australia	216	16%	188	87%	28
	10 above	**16,174**	**34%**	**14,317**	**89%**	**1,857**
	World	***25,293***		***22,389***		***2,904***

Note: Figures in italics are estimates. Missing data were estimated based on average ratios. Converted to $ using annual average exchange rate.
Source: UNCTAD, adapted from US Census Bureau; Japan Ministry of Economy, Trade and Industry; China Bureau of Statistics; KOSTAT (Republic of Korea); EUROSTAT (for Germany); UK Office of National Statistics; INSEE (France); Statistics Canada; Australian Bureau of Statistics and INE (Spain).

Source: UNCTAD 2015

UNCTAD B2C E- Commerce Index 2016



Source: UNCTAD

CELEBRATING 25 YEARS OF ACHIEVEMENTS

Key Cybersecurity Challenges

- Lack of adequate and interoperable national or regional legal frameworks
- Lack of secure software for 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
- Complexity of ICTs imply a need for the ability to respond, not just protect, as cybersecurity incidents will happen even if protective measures are deployed.

Cybersecurity not seen yet as a cross-sector, multi-dimensional concern.

Still seen as a technical/technology problem.

CELEBRATING 25 YEARS OF ACHIEVEMENTS

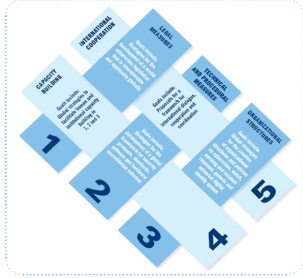
Coordinated Response

Need for a multi-level response to the cybersecurity challenges

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



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.

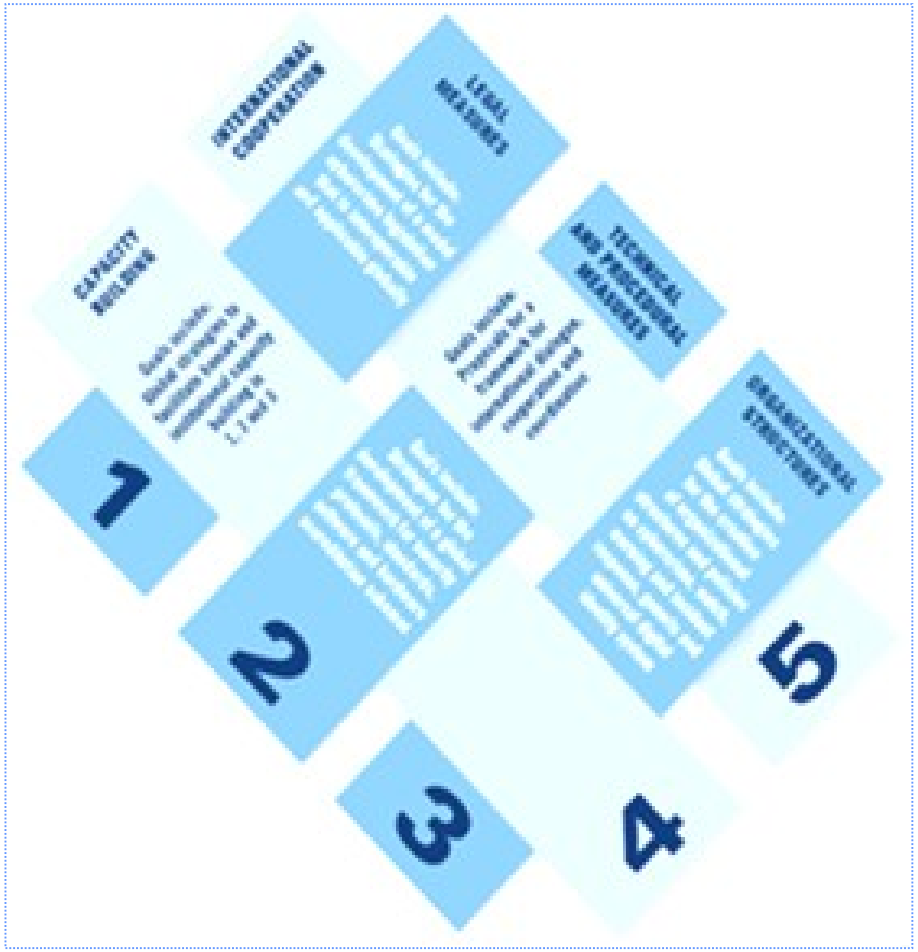
GCA GLOBAL CYBERSECURITY AGENDA

Building confidence and security in the use of ICTs is widely present in PP and Conferences' resolutions. In particular WTSA 16, PP 14 and WTDC 14 produced (revised) Resolutions (WTSA 16 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-D 1992 2017 CELEBRATING 25 YEARS OF ACHIEVEMENTS

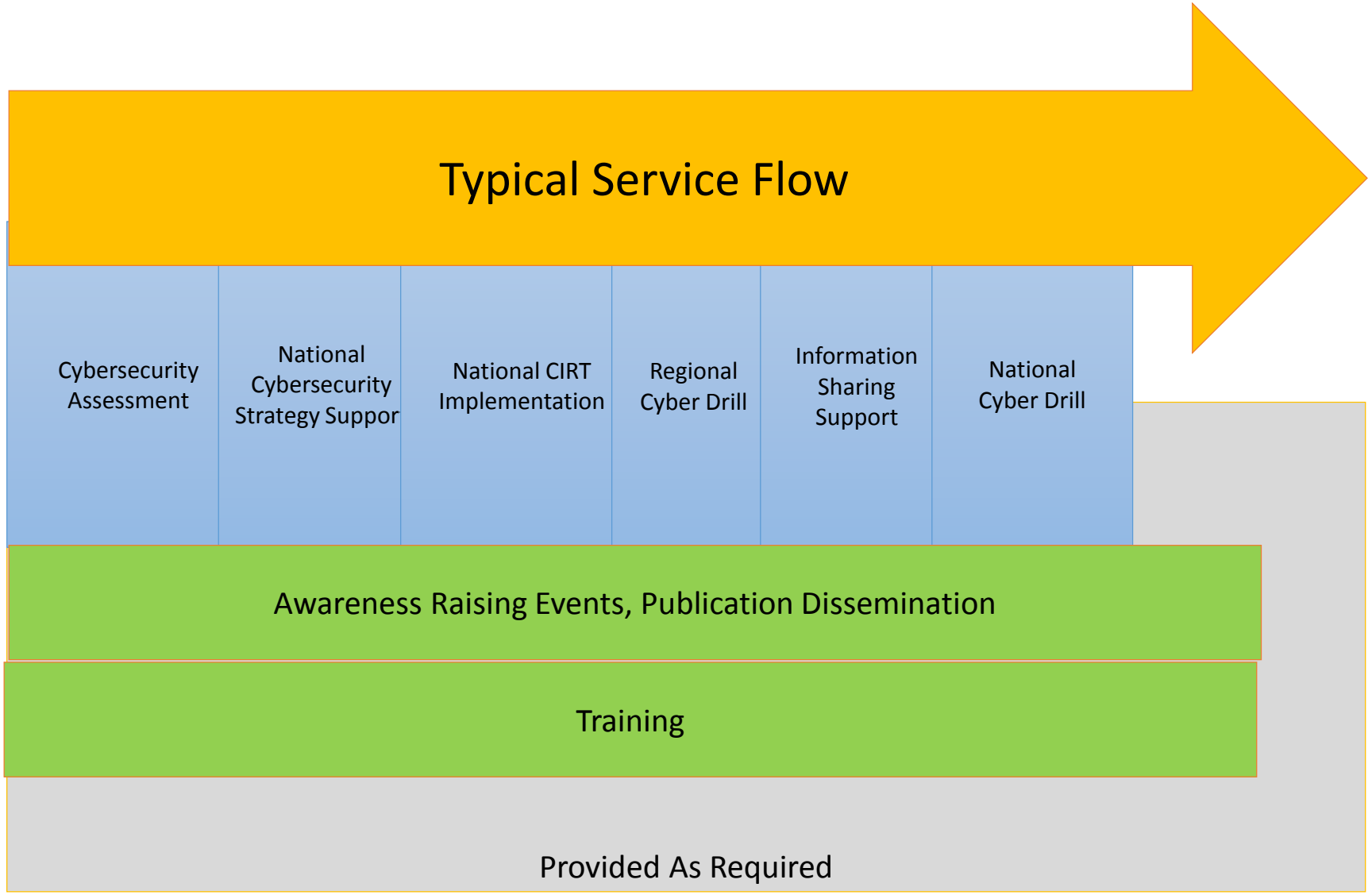
Global Cybersecurity Agenda (GCA)

- 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.



CELEBRATING 25 YEARS OF ACHIEVEMENTS

ITU Cybersecurity Services



National Cyber Security Strategy ITU Cyber Security Toolkit

The aim – create a toolkit to help states to create or improve cyber security strategies

Examples of Topics To Be Addressed

- The role, objectives and scope of a National Cyber Security Strategy in a line with the UN SDGs
- The definition/publication/review process: the Governance Model
- National and International Standards and government compliance program
- Critical Infrastructure Protection and integration with other national security/emergency programs
- National Risk Management program
- National Incident Response/CERT - integration/alignment with Military/Intelligence
- Implementation strategies for the Government
- Implementation strategies for Private Sector
- The definition/publication/review process: the Awareness Programme
- Aspects not typically covered by public strategies that should be considered and addressed

Components of Toolkit

Reference Guide

- A **single resource** for any country to gain a clear understanding of National Cyber Security Strategy in terms of:
  - the **purpose and content**
  - how to go about **developing a strategy,** including **strategic areas and capabilities**
  - the relevant **models and resources** available
  - the **assistance available** from various organisations and their contact details
- FORMAT: 15-20 page Word / PDF

Evaluation Tool

- A **simple tool** that allows national governments and stakeholders to:
  - Evaluate their **current status in each of the strategic areas** identified in the reference guide
  - Evaluate their **current status in cyber security lifecycle management**
  - Easily **identify key areas** for improvement
  - Provide a means for **measuring improvements** over time
- FORMAT: Excel or web-based worksheet

CELEBRATING 25 YEARS OF ACHIEVEMENTS

Global Cybersecurity Index (GCI)

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

134 Member States responded

Final Global and Regional Results 2017 are on ITU Website

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

ABIresearch | Global Cybersecurity Index

CELEBRATING 25 YEARS OF ACHIEVEMENTS

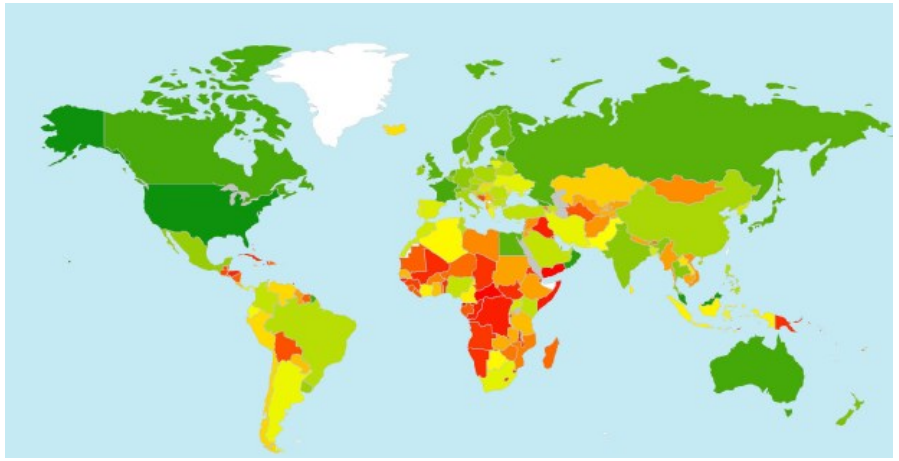
25 Indicators based on Five Pillars of ITU-GCA

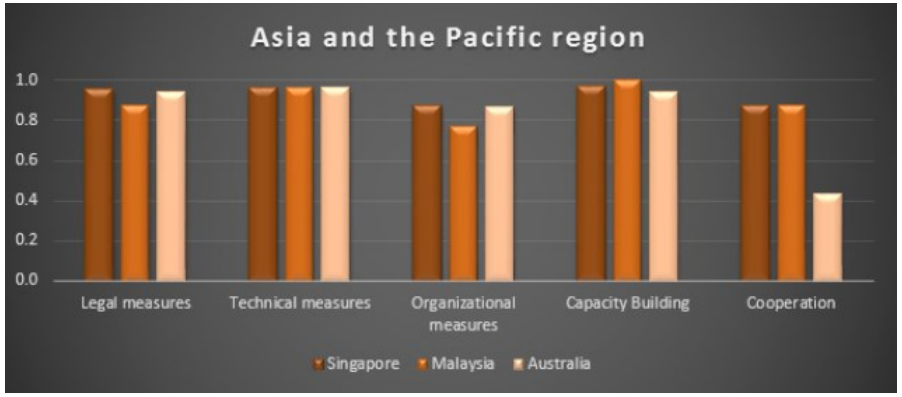
Legal	Technical	Organizational	Capacity Building	Cooperation
• Cybercriminal legislation • Cybersecurity regulation • Cybersecurity training	• National CIRT • Government CIRT • Sectoral CIRT • Standards implementation framework for organizations • Standards and certification for professionals • Child online protection	• Strategy • Responsible agency • Cybersecurity metrics	• Standardization bodies • Best practices • R & D programmes • Public awareness campaigns • Professional training courses • National education programmes and academic curricula • Incentive mechanisms • Home-grown cybersecurity industry	• Bilateral agreements • Multilateral agreements • International fora participation • Public-private partnerships • Interagency partnerships

Global Cybersecurity Index 2017:Asia-Pacific

ASIA AND THE PACIFIC Region	Score	Global Rank
Singapore	0.925	1
Malaysia	0.893	3
Australia	0.824	7
Japan	0.786	11
Republic of Korea	0.782	13
New Zealand	0.718	19
Thailand	0.684	20
India	0.683	23
China	0.624	32
Philippines	0.594	37
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Iran	0.494	60
Pakistan	0.447	67
Indonesia	0.424	70
Sri Lanka	0.419	72
Lao	0.392	77
Tonga	0.292	91
Cambodia	0.283	92
Nepal	0.275	94

ASIA AND THE PACIFIC Region	Score	Global Rank
Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Mongolia	0.228	104
Fiji	0.222	106
Bhutan	0.199	110
Nauru	0.140	127
Vanuatu	0.134	131
Kiribati	0.123	133
Solomon Islands	0.095	142
Papua New Guinea	0.067	150
Maldives	0.056	155
Palau	0.053	156
Samoa	0.048	157
Marshall Islands	0.048	157
Micronesia	0.044	158
Timor-Leste	0.034	162
Tuvalu	0.034	162





CELEBRATING 25 YEARS OF ACHIEVEMENTS

COP Five Strategic Pillars & COP Guidelines

Updated version of the Guidelines for Industry

COP Guidelines

CELEBRATING 25 YEARS OF ACHIEVEMENTS

5 key areas for protecting and promoting children's rights in the online environment

Policies and management processes	Child sexual abuse content	Safer and age appropriate environment	Educate children, parents and teachers	Promote positive use of ICTS
Integrate children's rights in policies and management processes	Develop processes for handling child sexual abuse content	Develop safer and age appropriate online environments	Educate children, parents and teachers on children's safety	Promote digital technology as a mode to further good citizenship

Purpose of the Guidelines is to provide:

- ✓ A blueprint that can be adapted locally for various industry players
- ✓ Establish a benchmark for recommended actions
- ✓ Guidance on identifying, prevent and mitigating risks
- ✓ Guidance on supporting children's rights

Initiative of Australia on Cyberbullying https://www.youtube.com/watch?v=TtEGAcLBTTA

CELEBRATING 25 YEARS OF ACHIEVEMENTS

ITU-UNODC-INTERPOL Cooperation on Cybercrime investigation for secure cyberspace

Objectives

- Build the capacity of law enforcement agencies on technical and legal aspects of cybercrime
- Share international best practices
- Harness the expertise and cooperation of ITU, UNODC and INTERPOL

Target Audience

The training is aimed to build capacity for law enforcement agencies, police and other relevant stakeholders in Nepal who are responsible for ensuring safety and security for the citizens of Nepal while using ICTs. The target audiences are as follows:

- Nepal Police
- Ministry of Law
- Others

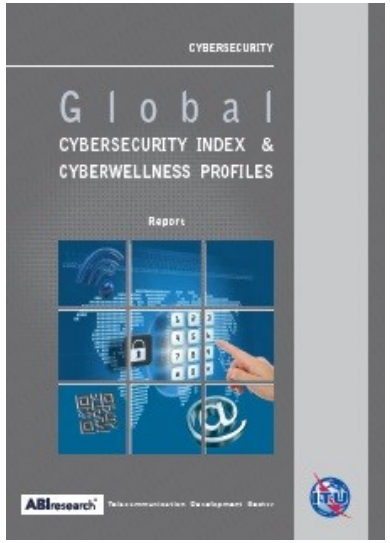
8-10 August, 2017
Kathmandu, Nepal

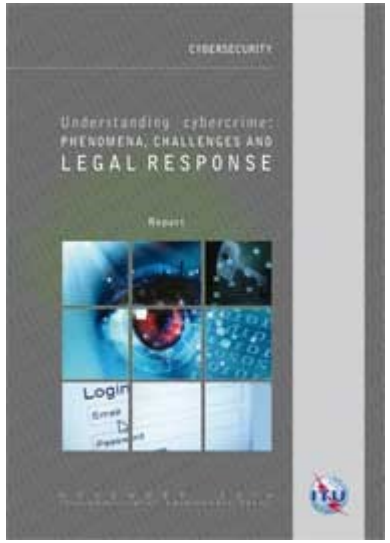
CELEBRATING 25 YEARS OF ACHIEVEMENTS

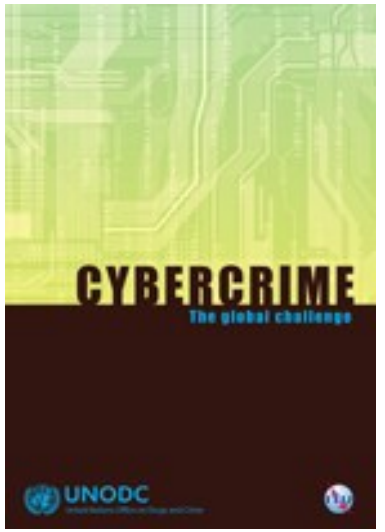
Cybersecurity in Asia-Pacific region

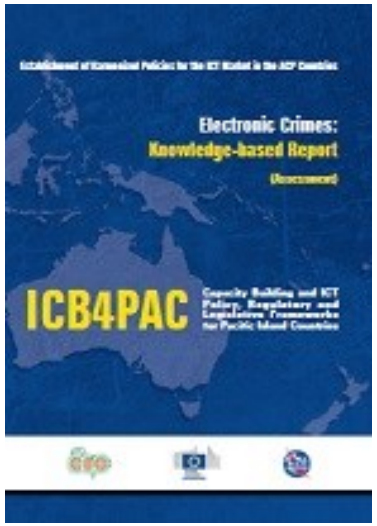
- National Cybersecurity Strategy & Cybersecurity Awareness : Nepal (2016-2015)
- Readiness Assessment to Establish a National CIRT for Fiji (2014-2015)
- Workshop on Cybersecuirty and Cybercrime Legislation & Cybersecurity Incident Simulation Bangkok 23 March 2015
- INTERPOL-ITU Cybercrime Investigation Seminar,19-21 Feb 2014, Malaysia
- First Pacific Islands Capacity Building Workshop on Child Online Protection and Commonwealth National Cybersecurity Framework Regional Workshop, 22-24 September 2014, Vanuatu
- Establishment of Pac CIRT, Fiji
- Readiness assessment National Cybersecurity Strategy, Bangladesh (2013)
- ITU Cyber Security Forum & Cyber Drill, 9-11 Dec 2013, Vientiane, Lao P.D.R
- Enhancement of cybersecurity capabilities (CIRT) Bhutan (2013)
- CIRT Capacity Building for Afghanistan (2014 and 2015)

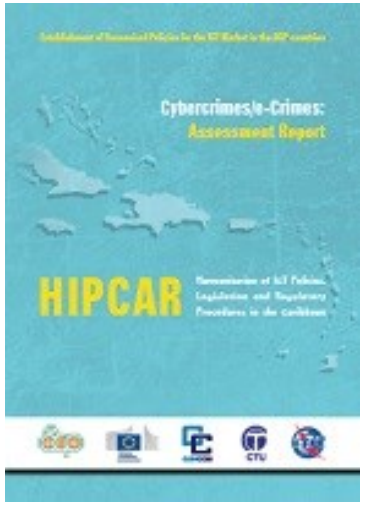
ITU Resources / Publications on Cybersecurity

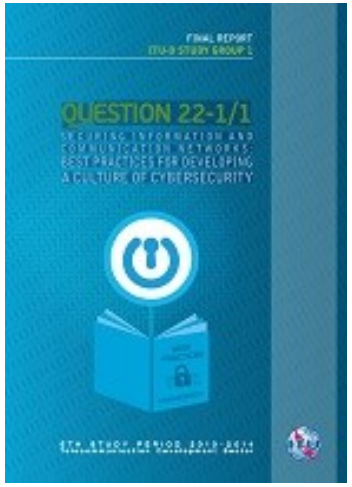


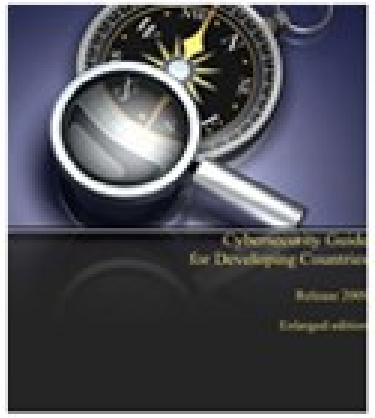












Ethics in business

- Ethics concern an individual's moral judgment about **right** and **wrong**
- Ethics helps you earn goodwill and create trust with the customers
- As an employer you need to pay minimum wage
- As an employer you need to abide by the laws and regulations of the land
- As employee you need to protect employers data and intellectual property

Ethics in ICT Business

Privacy Customer private data needs to be protected Customer private data should not be collected without their consent	**Accuracy** A professional should not misrepresent qualifications to perform a task
Property Who owns the data /information? Need to protect prosperity information/ IP from competitors	**Access** Access to information should be available to all Citizens should have access to information about government projects/ initiatives and the digital divide should be reduced

Because of ever changing environment, the ethics in IT cannot be the static set of rules. The company and people in IT have to constantly think of what falls in ethical or unethical, and evolve as the new things comes to surface

Ethical Dilemma

- Employee surveillance / work tracking. Is it Ethical ?
- Is it privacy intrusion ?
- Employees should be informed if there are tracking software installed
- Employees should not use company resources
- Employees should not waste time on Facebook/ Youtube

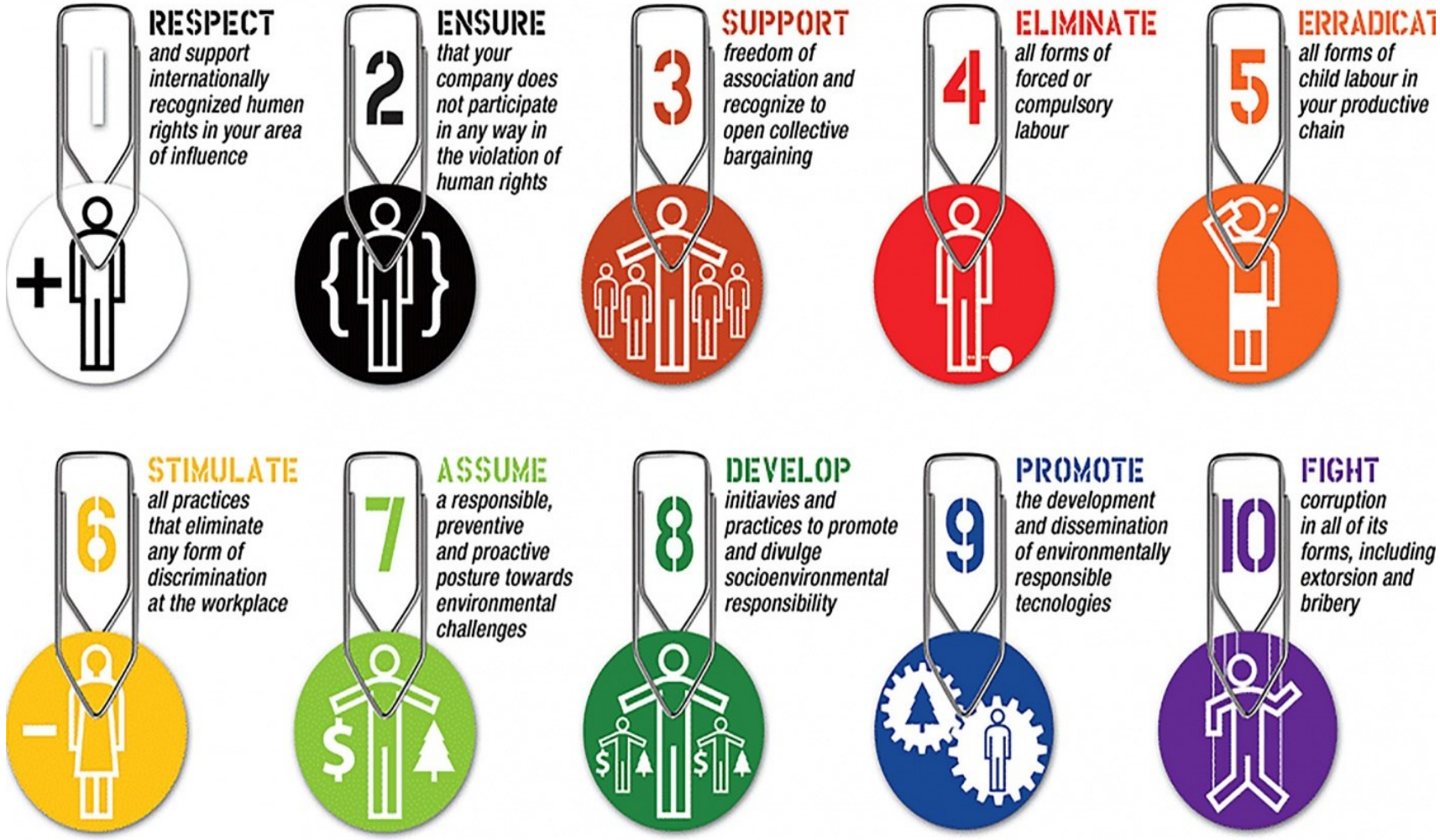
Case study of Bob - Software Developer

- Bob used to work at as a Software Developer in US firm
- The firms HR department gave him high performance reviews
- He outsourced his entire job to China and paid them a fifth of his salary
- He used to spend his time at office watching Youtube videos

Apple Case Study

- Famous for its innovative products (iPhone/iPad/ Macbooks)
- Apple maintained a culture of secrecy at the company
- Poor treatment of employees in Chinese factories (Foxconn)
- Employees are forced to work long hours
- Workers were paid low wages and were being exploited
- Some employees committed suicide due to work pressure

GLOBAL COMPACT PRINCIPLES



CELEBRATING 25 YEARS OF ACHIEVEMENTS

Conclusions

- While it will never be possible to completely remove all risks, drawing together an effective policies and practices, infrastructure & technology, awareness and communication can do a great deal to help.
- Cybersecurity and Critical National Information Infrastructure requiring political will and commitment to have clear National Cybersecurity Strategy , Cyber Crime Legislation , Child Online Protection, establishment / strengthening the CIRTs/ regular national / regional Cyber Drills
- Human and institutional capacity building critical to understand and take reactive / proactive response to address cyberthreats
- International cooperation, based on a multi-stakeholder approach, is the key and by working together with ITU and its partners, together we can make e- commerce transactions over Internet safe and secure!

ITU : I Thank U

CELEBRATING 25 YEARS OF ACHIEVEMENTS