Telecommunication
Development Bureau (BDT)

Ref.: BDT/IEE/CYB/DM/365

Geneva, 27 September 2013

To: Administrations of ITU Member States
National Regulatory Authorities
ITU-D Sector Members

Subject: Global Cybersecurity Index

Dear Sir/Madam,

The International Telecommunication Union has initiated the development of a Global Cybersecurity Index (GCI), a project that aims to effectively measure each nation state's level of cybersecurity development. The project is based on the current mandate of the ITU and the related projects and activities of the ITU's Telecommunication Development Bureau (BDT).

The ITU is the lead facilitator for World Summit on the Information Society Action Line C5 which encourages stakeholders in "building confidence and security in the use of information and communication technologies" at national, regional and international levels. In this framework, the Global Cybersecurity Agenda was launched by the ITU Secretary-General as ITU's framework for international multi-stakeholder cooperation towards a safer and more secure information society, and focuses on the following five work areas:

- Legal Measures
- Technical and Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation.

These five designated areas will form the basis of the indicators for the GCI. The GCI project will be a joint effort between the ITU, specifically the Cybersecurity and ICT Applications Division of the BDT and ABI Research, a market intelligence company specializing in global technology markets through quantitative forecasting and analysis of key metrics and trends. ITU will act as focal point and owner of the project, and ABI Research will bring in its core skill sets in strategy development, competitive intelligence, business planning, technology assessment, and industry benchmarking for the realization of the project.

The index will allow nation states to better address their cybersecurity needs and drive development of national capabilities in all five areas. The ultimate goal is to help foster a global culture of cybersecurity and its integration at the core of information and communication technologies.

You are kindly invited to participate in the benchmarking exercise aimed at assessing the current situation of your country against the GCI. A questionnaire is provided for data collection and is also available on the

GCI website: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx. Please fill out the questionnaire via the website or email your responses to the contact points for the project:

Mr. Marco Obiso, ITU - marco.obiso@itu.int

Ms. Michela Menting, ABI Research - menting@abiresearch.com

Your responses are much appreciated. The deadline for receipt of the responses is end of December 2013. In the event that we do not receive a reply before the stipulated deadline, we will pre-populate the questionnaire for you and submit this for your review for inclusion into the benchmarking process.

Both contact points are available to respond to any questions or to provide further information about the project.

Yours faithfully,

[Original signed]

Brahima SANOU
Director

Annex

QUESTIONNAIRE

For the

GLOBAL CYBERSECURITY INDEX

Please fill this questionnaire out electronically

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

or email your responses

to:

Ms Michela Menting, ABI Research menting@abiresearch.com

Mr Marco Obiso, ITU marco.obiso@itu.int

International Telecommunication Union • Place des Nations • CH-1211 Geneva 20 • Switzerland
Tel: +41 22 730 5111 • Fax: +41 22 730 5545/730 5484 • E-mail: bdtmail@itu.int • www.itu.int/itu-d

QUESTIONNAIRE

GLOBAL CYBERSECURITY INDEX

The Global Cybersecurity Index (GCI) project aims to effectively measure each nation state's level of cybersecurity development. The ultimate goal is to help foster a global culture of cybersecurity and its integration at the core of information and communication technologies (ICT). The project is based on the current mandate of the International Telecommunication Union (ITU) and the related projects and activities of the ITU's Telecommunication Development Bureau, the BDT.

The ITU is the lead facilitator for WSIS (World Summit on the Information Society) Action Line C5 for assisting stakeholders in building confidence and security in the use of ICTs at national, regional and international levels. In this framework, the Global Cybersecurity Agenda (GCA) was launched by the ITU Secretary-General as ITU's framework for international multi-stakeholder cooperation towards a safer and more secure information society, and focuses on the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. These five designated areas will form the basis of the indicators for the GCI.

The GCI project will be a joint effort between the BDT, specifically the Cybersecurity and ICT applications Division (CYB) and ABI Research.

You are kindly invited to participate in a benchmarking exercise aimed at assessing the current situation of your Country against the Global Cybersecurity Index (GCI).

Your responses to this questionnaire are much appreciated. The ITU will prepare a compilation and comparative overview of responses to the benchmarking exercise once completed.

RESPONDING COUNTRY *(including contact information):*	
QUESTIONS	*RESPONSES*
1A. Is there any criminal legislation regarding cyber activities? If so, please specify *Include URL, title of laws/acts/articles, and/or wording*	
1B. Is there any regulation regarding cybersecurity and compliance requirements? If so, please specify *Include URL, title of laws/acts/articles, and/or wording*	
2A. Is there one (or more) officially approved national or sector-specific CERT, CIRT or CSIRT team(s)? If so, please specify the names and number and whether they are legally mandated or not *Include URL, official name, and contact details*	
2B. Is there any officially-approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards? If so, please specify *Include URL, official name of framework, responsible agency (and contact details) and short description*	
2C. Is there any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals? If so, please specify *Include URL, official name of framework, responsible agency (and contact details) and short description*	
3A. Is there any officially recognised national or sector-specific cybersecurity strategy and/or policy? If so, please specify *Include URL, official name of strategy/policy, responsible agency (and*	

contact details) and short description	
3B. IS there any officially recognised national or sector-specific governance roadmap for cybersecurity? If so, please specify *Include URL, official name of roadmap, responsible agency (and contact details) and short description*	
3C. IS there any officially recognised national or sector-specific agency responsible for implementing a national cybersecurity strategy/policy/roadmap? If so, please specify *Include URL, official name of responsible agency (and contact details) and short description of responsibilities*	
3D. Is there any officially recognised national or sector-specific benchmarking exercises or referential used to measure cybersecurity development? If so, please specify *Include URL, official name of benchmarking exercise, responsible agency (and contact details) and short description*	
4a. Is there any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector? If so, please specify *Include URL, official name(s) of programs/projects/best practices/guidelines, responsible agency(ies) (and contact details) and short description*	
4B. Is there any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector? If so, please specify *Include URL, official name(s) of programs/projects, responsible agency(ies) (and contact details) and short description*	
4C. Are there any public sector professionals certified under internationally recognized certification programs in cybersecurity? If so, please specify the number	

Include type of certification and certificating agency	
4D. Are there any certified government and public sector agencies certified under internationally recognized standards in cybersecurity? If so, please specify the number *Include type of certification and certificating agency*	
5A. Are there any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states? If so, please specify *Include URL, official name of partnership, responsible national agency (and contact details), participating countries, and short description*	
5B. Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector? If so, please specify *Include URL, official name of program, responsible agency (and contact details), participating organizations, and short description*	
5C. Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets between the public and private sector? If so, please specify *Include URL, official name of program, responsible national agency (and contact details), participating organizations, and short description*	
5D. Are there any officially recognized participation in regional and/or international cybersecurity platforms and forums? If so, please specify *Include URL, official name of platform/forum, responsible national agency (and contact details), participating countries, and short description*	
THANK YOU!	

Categories and Performance Indicators

The GCI will be a benchmark ranking measuring the cybersecurity development capabilities of sovereign nation states. The index is essentially a composite indicator, aggregating a number of individual indicators. The process of cybersecurity development can be analyzed within five important broad categories. The following indicators and sub-groups have been identified, and nations will be ranked against the benchmark provided in each indicator.

1. Legal Measures

Legislation is a critical measure for providing a harmonized framework for entities to align themselves to a common regulatory basis, whether on the matter of prohibition of specified criminal conduct or minimum regulatory requirements. Legal measures also allow a nation state to set down the basic response mechanisms to breach: through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. A legislative framework sets the minimum standards of behavior across the board, applicable to all, and on which further cybersecurity capabilities can be built. Ultimately, the goal is to enable all nation states to have adequate legislation in place in order to harmonize practices supranationally and offer a setting for interoperable measures, facilitating international combat against cybercrime.

The legal environment can be measured based on the existence and number of legal institutions and frameworks dealing with cybersecurity and cybercrime. The sub-group is composed of the following performance indicators:

A. Criminal Legislation

Cybercrime legislation designates laws on the unauthorized (without right) access, interference, interception of computers, systems and data. The laws can be ranked by level: none, partial or comprehensive. Partial legislation refers to the simple insertion of computer-related wording in an existing criminal law or code, with language limited to extending for example fraud or forgery, or surveillance and theft to cyberspace. Comprehensive legislation refers to the enactment of a dedicated law or act dealing with the specific aspects of computer crime (i.e. the UK Computer Misuse Act 1990). This category can include partial legislation where the case law or jurisprudence is extensively developed. Please specify the types of laws and regulations and whether there are none or whether they are partial or comprehensive.

B. Regulation & Compliance

Cybersecurity regulation designates laws dealing with data protection, breach notification and certification/standardization requirements. The laws can be ranked by level: none, partial or comprehensive. Partial regulation refers to the insertion of computer-related wording in existing or new criminal or civil law, so that the law extends applicability to cyberspace in regulation not specifically or uniquely related to cybersecurity (i.e. the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data). Comprehensive regulation refers to the enactment of a dedicated law, act or directive requiring cybersecurity compliance (i.e. the US Federal Information Security Management Act

2002). Please specify the types of laws and regulations and whether there are none or whether they are partial or comprehensive.

2. Technical Measures

Technology is the first line of defense against cyberthreats and malicious online agents. Without adequate technical measures and the capabilities to detect and respond to cyberattacks, nation states and their respective entities remain vulnerable to cyberthreats. The emergence and success of ICTs can only truly prosper in a climate of trust and security. Nation states therefore need to be capable of developing strategies for the establishment of accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be accompanied by the creation of a national entity focused on dealing with cyber incidents at a national level, at the very least with a responsible government agency and with an accompanying national framework for watch, warning and incident response.

Technical measures can be measured based on the existence and number of technical institutions and frameworks dealing with cybersecurity endorsed or created by the nation state. The sub-group is composed of the following performance indicators:

A. CERT/CIRT/CSIRT

The establishment of a national CIRT (Computer Incident Response Team), CERT (Computer Emergency Response Team) or CSIRT (Computer Security incident Response Team) which provides the capabilities to identify, defend, respond and manage cyber threats and enhance cyberspace security in the nation state. This ability needs to be coupled with the gathering of its own intelligence instead of relying on secondary reporting of security incidents whether from the CIRT's constituencies or from other sources. Please specify the names and number of officially approved national or sector-specific CERT or CSIRT teams, and whether they are legally mandated or not. The level of development will be ranked based on if there are any national teams and whether they are legally mandated or not.*

B. Standards

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within the critical infrastructure (even if operated by the private sector). These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc. Please specify any officially-approved national (and sector specific) frameworks for implementing internationally recognized cybersecurity standards.

C. Certification

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of national (government) agencies and public sector professionals by internationally recognized cybersecurity standards. These certifications, accreditations and standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), (No Suggestions) Certification, Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute, CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc. Please specify any officially approved national (and sector specific) frameworks for the certification and accreditation of national agencies and public sector professionals.

3. Organizational Measures

Organization and procedural measures are necessary for the proper implementation of any type of national initiative. A broad strategic objective needs to be set by the nation state, with a comprehensive plan in implementation, delivery and measurement. Structures such as national agencies need to put in place in order to put the strategy into effect and evaluate the success or failure of the plan. Without a national strategy, governance model and supervisory body, efforts in different sectors and industries become disparate and unconnected, thwarting efforts to reach national harmonization in terms of cybersecurity capability development.

The organizational structures can be measured based on the existence and number of institutions and strategies organizing cybersecurity development at the national level. The creation of effective organizational structures is necessary for promoting cybersecurity, combating cybercrime and promoting the role of watch, warning and incident response to ensure intra-agency, cross-sector and cross-border coordination between new and existing initiatives. The sub-group is composed of the following performance indicators:

A. Policy

The development of a policy to promote cybersecurity is recognized as a top priority. A national strategy for Security of Network

and Information Systems should maintain resilient and reliable information infrastructure and aim to ensure the safety of citizens; protect the material and intellectual assets of citizens, organizations and the State; prevent cyber-attacks against critical infrastructures; and minimize damage and recovery times from cyber-attacks. Policies on National Cybersecurity Strategies or National Plans for the Protection of Information Infrastructures are those officially defined and endorsed by a nation sate, and can include the following commitments: establishing clear responsibility for cybersecurity at all levels of government (local, regional and federal or national), with clearly defined roles and responsibilities; making a clear commitment to cybersecurity, which is public and transparent; encouraging private sector involvement and partnership in government-led initiatives to promote cybersecurity. Please specify any officially recognized national or sector-specific cybersecurity strategy.

B. Roadmap for Governance

A roadmap for governance in cybersecurity is generally established by a national strategy /policy for cybersecurity, and identifies key stakeholders. The development of a national policy framework is a top priority in developing high-level governance for cybersecurity. The national policy framework must take into account the needs of national critical information infrastructure protection. It should also seek to foster information-sharing within the public sector, and also between the public and private sectors. Cybersecurity governance should be built on a national framework addressing challenges and other information security and network security issues at the national level, which could include: national strategy and policy; legal foundations for transposing security laws into networked and online environments; involvement of all stakeholders; developing a culture for cybersecurity; procedures for addressing ICT security breaches and incident-handling (reporting, information sharing, alerts management, justice and police collaboration); effective implementation of the national cybersecurity policy; cybersecurity programme control, evaluation, validation and optimization. Please specify any officially recognized national or sector-specific governance roadmap for cybersecurity.

C. Responsible Agency

A responsible agency for implementing a national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils or cross-disciplinary centers. Most national agencies will be directly responsible for watch and warning systems and incident response, and for the development of organizational structures needed for coordinating responses to cyber-attacks. Please specify any officially recognized national or sector-specific cybersecurity agency.

D. National Benchmarking

This indicator measures the existence of any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. For example, based on ISO/IEC 27002-2005, a national cybersecurity standard (NCSec Referential) can help nation states respond to specify cybersecurity requirements. This referential is split into five domains: NCSec

Strategy and Policies; NCSec Organizational Structures; NCSec Implementation; National Coordination; Cybersecurity Awareness Activities. Please specify any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

4. Capacity Building

Capacity building is intrinsic to the first three measures (legal, technical and organizational). Understanding the technology, the risk and the implications can help to develop better legislation, better policies and strategies, and better organization as to the various roles and responsibilities. Cybersecurity is a relatively new area, not much older than the internet itself. This area of study is most often tackled from a technological perspective; yet there are numerous socio-economic and political implications that have applicability in this area. Human and institutional capacity building is necessary to enhance knowledge and know-how across sectors, to apply the most appropriate solutions, and promote the development of the most competent professionals.

A capacity building framework for promoting cybersecurity should include awareness-raising and the availability of resources. Capacity building can be measured based on the existence and number of research and development, education and training programs, and certified professionals and public sector agencies. The sub-group is composed of the following performance indicators:

A. Standardization Development

Standardization is a good indicator of the level of maturity of a technology, and the emergence of new standards in key areas underlines the vital importance of standards. Although cybersecurity has always been an issue for national security and treated differently in different countries, common approaches are supported by commonly recognized standards. These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc. Please specify any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

B. Manpower Development

Manpower development should include efforts by nation states to promote widespread publicity campaigns to reach as many people as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community

centers, computer stores, community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behavior online. This includes actions such as setting up portals and websites to promote awareness, disseminating support material for educators and establishing (or incentivizing) professional training courses and education programs. Please specify any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public (i.e. national cybersecurity awareness day, week, or month), promoting cybersecurity courses in higher education (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector.

C. Professional Certification

This performance indicator can be measured by the number of public sector professionals certified under internationally recognized certification programs standards including, but not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), (No Suggestions) Certification, Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute, CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc. Please specify the number of public sector professionals certified under internationally recognized certification programs.

D. Agency Certification

This performance indicator can be measured by the number of certified government and public sector agencies certified under internationally recognized standards. These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc. Please specify the number of certified government and public sector agencies certified under internationally recognized standards.

5. Cooperation

Cybersecurity requires input from all sectors and disciplines and for this reason needs to be tackled from a multi-stakeholder approach. Cooperation enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application. Information sharing is difficult at best between different disciplines, and within private sector operators. It becomes increasingly so at the international level. However, the cybercrime problem is one of a global nature and is blind to national

borders or sectoral distinctions. Cooperation enables sharing of threat information, attack scenarios and best practices in response and defense. Greater cooperative initiatives can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats, and enable better investigation, apprehension and prosecution of malicious agents.

National and international cooperation can be measured based on the existence and number of partnerships, cooperative frameworks and information sharing networks. The sub-group is composed of the following performance indicators:

A. Intra-state Cooperation

Intra-state cooperation refers to any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states (i.e. signed bi-lateral or multi-lateral partnerships for the cooperation or exchange of information, expertise, technology and/or resources). Intra-state cooperation also includes regional level initiatives such as (but not limited to) those implemented by the European Union, the Council of Europe, the G8 Group of States, Asian Pacific Economic Cooperation (APEC), Organization of American States (OAS), the Association of South East Asian Nations (ASEAN), the Arab League, the African Union, the Shanghai Cooperation Organization (SCO) and Network Operations Groups (NOG), etc. Please specify any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states.

B. Intra-agency Cooperation

Intra-agency cooperation refers to any officially recognized national or sector-specific programs for sharing cybersecurity assets (people, processes, tools) within the public sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources between departments and agencies). This includes initiatives and programs between different sectors (law enforcement, military, healthcare, transport, energy, waste and water management, etc.) as well as within departments/ministries (federal/local government, human resources, IT service desk, PR, etc.). Please specify any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

C. Public-Private Partnerships

Public-private partnerships (PPP) refer to ventures between the public and private sector. This performance indicator can be measured by the number of officially recognized national or sector-specific PPPs for sharing cybersecurity assets (people, processes, tools) between the public and private sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources). Please specify any officially recognized national or sector-specific programs for sharing

cybersecurity assets between the public and private sector.

D. International Cooperation

This performance indicator refers to any officially recognized participation in international cybersecurity platforms and forums. Such cooperative initiatives include those undertaken by (but not limited to): United Nations General Assembly; International Telecommunication Union (ITU); Interpol / Europol; The Organisation for Economic Cooperation and Development (OECD); UN Organizations on Drug and Crime Problems (UNODC); UN Interregional Crime and Justice Research Institute (UNICRI); Internet Corporation for Assigned Names and Numbers (ICANN); International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC); Internet Engineering Task Force; FIRST (Forum of Incident Response and Security Teams). Please specify any officially recognized participation in regional and/or/ international cybersecurity platforms and forums.