Telecommunication
Development Bureau (BDT)

Ref.: BDT/IEE/CYB/DM/119

Geneva, 21 December 2015

To:
Administrations of ITU Member States

Subject: Invitation to participate in the 2016 Edition of the Global Cybersecurity Index (GCI)

Dear Sir/Madam

In 2013 the International Telecommunication Union (ITU) launched the Global Cybersecurity Index (GCI) in partnership with ABI Research, an initiative aimed at measuring the commitment of Member States of the ITU to cybersecurity. The results of the GCI were published in 2014 (see http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx). A total of 105 countries responded to this first iteration of the GCI, a significant engagement for an effort of this type and an indication of interest in measuring cybersecurity.

Following the support expressed by Member States of the ITU for the GCI at the ITU Plenipotentiary Conference 2014 in Busan, Korea, I am happy to inform you that a second iteration of the Index has been initiated, and I hereby invite you to participate. Key outputs planned for this next round of the GCI include index values for each of the 193 Member States of the ITU, updates to their cyber-wellness profiles, and the publication of best practices and regional reports with focused analysis. For this next iteration, as well as for the ones that will surely follow, I am also happy to inform you that I have expanded the partnership and taken a multi-stakeholder approach that leverages the expertise of different organizations, with the objectives of improving the quality of the GCI, instigating international cooperation, and promoting knowledge exchange on this topic.

In order to proceed efficiently, I kindly request you to appoint by **18 January 2016** a focal point who will be responsible for completing the online 2016 GCI questionnaire for your country. Our GCI team will contact your assigned focal point and provide further instructions on how to access the online questionnaire, which will close on 11 March 2016. You will find attached a guide to the questionnaire to give you a better appreciation of the scope of the GCI to assist you in identifying your focal point. Additional information and details can be found on the dedicated GCI 2016 website: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

Furthermore, with a view to promoting synergy and helping optimise your information gathering efforts, we wish to apprise you of a complementary annual endeavour from our colleagues at the United Nations Office in New York performed under Resolution 69/28 “Developments in the field of information and telecommunications in the context of international security”. We expect the “note verbale” inviting all

Member States to continue to inform the Secretary-General of the United Nations on the matters highlighted in the resolution to be issued in February 2016. Hopefully your efforts for the GCI will facilitate this complementary process.

To support your focal point in answering the GCI questionnaire, I have appointed as ITU focal points for the GCI Mr Marco Obiso (marco.obiso@itu.int) and Mrs Rosheen Awotar-Mauree (rosheen.awotar@itu.int).

I firmly believe that the GCI is a very important tool for the fulfilment of the ITU-D’s mandate. I wish to thank Member States that have contributed to the GCI 2014 and I hope to receive even greater support from you for the GCI 2016.

Yours faithfully,

[Original signed]

Brahima Sanou
Director

Annex: Guide to the 2016 GCI Questionnaire

Global Cybersecurity Index (GCI) 2015/16 Questionnaire Guide

This document is for information only. The GCI measures the commitment of countries to cybersecurity in the five pillars of the Global Cybersecurity Agenda: Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation.

This questionnaire has merged questions elaborated for establishing the GCI 2015/16 Score together with those required by ITU-D Study Group 2 Question 3. The questionnaire is composed of three separate sections, where questions in the first two sections have yes/no responses whilst the questions in the last section are open ended. The questionnaire should be completed online. Each respondent will be provided (via an official email from ITU) a unique url for his/her safekeeping. The online questionnaire enables the respondents to upload relevant documents (and urls) for each question as supporting information.

Information being provided by respondents to this questionnaire is not expected to be of confidential nature.

SECTION 1

1. Is there any Cyber related legislation?

1.1. Is there any cybercriminal law?

Exp: *Cybercrime legislation designates laws on the unauthorized access, data and system interference or interception and misuse of computer systems. This includes procedural law, and any existing articles on the expedited preservation of stored computer data, production orders, real-time collection of computer data, extradition, mutual assistance, confidentiality and limitation on use; as well as any case law on cybercrime or computer misuse, it also includes content related offences. Provisions may be part of the national Penal law, Data Protection Act, Freedom of Information Act, Copyright / Intellectual Property Legislation.*

1.1.1. Is there any substantive cybercriminal law?

Exp: *Substantive law refers to all categories of public and private law, including the law of contracts, real property, tort, wills, and criminal law that essentially creates, defines and regulates rights.*

1.1.1.1. Are there any articles on the unauthorized access of computers, systems and data?

Exp : *Unauthorized access refers to gaining access to computer, system and data using someone else's account or through devious means including password guessing/cracking and identity theft.*

1.1.1.2. Are there any articles on the unauthorized interference / modification of computers, systems and data?

Exp: *Unauthorized interference/modification refers to illegal meddling with a system, computer or data whereby changes are brought to the initial state of the system, computer or data which may include inputting, damaging, deleting, or generally altering computer data.*

1.1.1.3. Are there any articles on the unauthorized interception of computers, systems and data?

Exp: *Unauthorized interception refers to illegal capture of non-public transmissions of computer data.*

1.1.2. Is there any procedural cybercriminal law?

Exp: *The rules by which a court hears and determines what happens in civil lawsuits, criminal or administrative proceedings. The rules are designed to ensure a fair and consistent application of due process or fundamental justice to all cases that come before a court.*

1.1.2.1. Are there any articles on the expedited preservation of stored computer data?

Exp: *Data preservation is an obligation imposed on a person or organization by a state authority, requiring the safekeeping of a specified type of data from loss or modification for a specific period of time*.

1.1.2.2. Are there any articles on production orders?

Exp: *A production order is an obligation imposed on a person or organization by a state authority, requiring delivery of available and a specified type of computer data to law enforcement officials within a specified period of time.*

1.1.2.3. Are there any articles concerning search and seizure of stored computer data?

Exp: *Search and seizure of computer data refers to measures, including legislative ones, empowering authorities to search and access a computer system and computer data stored in its territory.*

1.1.2.4. Are there any articles concerning real-time collection of computer data?

Exp: *Real-time collection of data refers to measures, including legislatives ones, empowering authorities to collect or record traffic data in real time, in its territory, transmitted by means of a computer system.*

1.1.2.5. Are there any articles related to extradition of cyber perpetrators?

Exp: *Extradition is a procedure by which a state or nation, upon receipt of a formal request by another state or nation, turns over to that second jurisdiction an individual charged with or convicted of a cyber-crime in that jurisdiction.*

1.1.2.6. Are there any articles relating to mutual assistance?

Exp: *An agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.*

1.1.2.7. Are there any articles related to confidentiality and limitation of use?

Exp: *A Party may use the data provided it adheres to certain confidentiality clauses or uses the data only for specific agreed usage.*

1.1.3. Is there any case law on cybercrime or computer misuse?

Exp: *Offences under computer misuse may include hacking, unauthorized access to computer systems and purposefully spreading malicious and damaging software (malware). Unauthorized access to modify computers may include altering software and data, changing passwords and settings to prevent others accessing the system, and interfering with the normal operation of the system to its detriment.*

1.2. Is there any cybersecurity legislation or regulation?

Exp: *Regulation is a rule based on, and meant to carry out, a specific piece of legislation. Regulations are usually enforced by a regulatory agency formed or mandated to carry out the purpose or provisions of a legislation. Cybersecurity regulation would thus designate principles, to be abided by various stakeholders, emanating from and being part of the implementation of laws dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection, digital signatures and e-transactions, and the liability of Internet service providers.*

1.2.1. Is there any data protection legislation or regulation ?

Exp: *Regulations pertaining to protection of personal, commercial, and governmental data from unauthorized access, alteration, destruction or use.*

1.2.2. Is there any system and network protection legislation or regulation?

Exp: *Legal measures designed to protect systems and networks from harmful interference.*

1.2.3. Is there any breach notification legislation or regulation?

Exp: *Breach notification laws or regulations are ones that require an entity that has been subject to a breach to notify the authorities, their customers and other parties about the breach, and take other steps to remediate injuries caused by the breach. These laws are* *generally enacted in response to an escalating number of breaches of consumer databases containing personally identifiable information.*

1.2.3.1. For data?

Exp: *Breach notification laws concerning data breaches.*

1.2.3.2. For systems and networks?

Exp: *Breach notification laws concerning systems and networks breaches. Those can include a standard of cybersecurity care or other basic requirements to safeguard consumer data such as encryption.*

1.2.4. Is there any cybersecurity certification/standardization legislation or regulation?

Exp: *Cybersecurity regulation in terms of certification/standardization requires that entities operating within the territory of a country obtain certain, minimum requirement certification/standardization. This requirement may differ depending on the sector of the economy. 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.*

1.2.4.1. For public sector?

Exp: A *regulation referring to obligatory cybersecurity certification/standardization in a public sector.*

1.2.4.2. For private sector?

Exp: *A regulation referring to obligatory cybersecurity certification/standardization in a private sector.*

1.2.5. Does the legislation or regulation impose the implementation of cybersecurity measures?

Exp: *Cybersecurity measures may include, but are not limited to, technical and organizational measures, such as: firewall, access control list, establishing security roles and responsibilities, cybercrime insurance (own).*

1.2.5.1. On the public sector?

1.2.5.2. On the critical infrastructure operators?

Exp: *Critical infrastructures are key systems crucial for safety, security, economic security and public health of a nation. These systems may include, but are not limited to: Defense systems, Banking and Finance, Telecommunications, Transport, Health, Energy etc.*

1.2.5.3. On the private sector?

1.2.6. Does the legislation or regulation impose cybersecurity audits?

Exp: *A security audit is a systematic and periodic evaluation of the information system's security. Typical audit may include assessment of the security of the system's physical configuration and environment, software, information handling processes, and user practices.*

1.2.6.1. On the public sector?

1.2.6.2. On the critical infrastructure operators?

1.2.6.3. On the private sector?

1.2.7. Is there a legislation or regulation detailing the protection of privacy?

Exp: *Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. An example of such legislation may be in the Data Protection Act.*

1.2.8. Is there a legislation or regulation related to digital signatures and e-transactions?

Exp*: A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. An electronic transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated* *networks; examples of such legislative documents include Electronic Commerce Act, Law on Electronic Signatures, E-Transaction Law etc. which may include regulations on the establishment of a controller of certificate authorities.*

1.2.9. Is there a legislation or regulation related to the liability and responsibility of Internet Service Providers?

***Exp**: Internet Service Providers liable for the copyright infringement resulting from the acts of their users. Providers obliged to notify the police, CERT or other responsible agency/national authority of the illegal cyber operation originating from their infrastructure, a requirement of proactive network monitoring.*

1.2.10 Is there a legislation or regulation related to the containment or curbing of spam?

1.3. Is there any cybersecurity training for law enforcement officers, judicial and other legal actors?

***Exp**: Formal process for educating legal actors about computer security.*

1.3.1. For law enforcement (police officers and enforcement agents)?

1.3.2. For judicial and other legal actors (judges, solicitors, barristers, attorneys, lawyers, paralegals, etc.)?

1.3.3. Is the training recurring?

Exp: Tr*aining organized periodically or repeatedly.*

2. Do you have any technical measures?

2.1. Is there a CIRT, CSIRT or CERT with national responsibility?

Exp: *CIRT refers to Computer Incident response. CSIRT refers to Computer Security Incident Response Team and CERT refers to Computer Emergency Response Team. These terms are used interchangeably to indicate an entity that receives reports of security breaches, conducts analyses of the reports and responds to the senders. A national CSIRT/CIRT/CERT refers to an entity which has been mandated with the national responsibility to monitor, manage and handle cybersecurity incidents with its local constituencies including academia, law enforcement, civil society, private sector (in economic groups or criticality groups, critical information infrastructures (energy, health, transport, finance etc.) and Government. It also interacts with national CIRTs of other countries as well as regional and international players for relevant and effective coordination in case of attacks.*

2.1.1. Does it have a government mandate?

Exp: S*upported by a government's decision or is part of governmental structures.*

2.1.2. Does the CIRT, CSIRT or CERT conduct recurring cybersecurity exercises?

Exp: *A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption. Is the exercise organized periodically or repeatedly?*

2.1.3. Is the CIRT, CSIRT or CERT affiliated with FIRST?

Exp: A *Full Member or Liaison Member of the Forum of Incident Response and Security Teams.*

2.1.4. Is the CIRT, CSIRT or CERT affiliated with any other CERT communities? (regional CERT)

Exp: Any *formal or informal relation with any other CERT within, or outside the country, part of any regional CERT group.*

2.2. Is there a Government CERT?

Exp: *A government CERT/CIRT/CSIRT is an entity that responds to computer security or cybersecurity incidents which affect solely governmental institutions. Apart from reactive services, it may also engage in proactive services such as vulnerability analysis and security audits. Unlike the national CERT which services both the private and public sectors, the government CERT provides its services to constituents from the public sector only.*

2.3. Are there any sectoral CERTs?

Exp: *A sectoral CERT/CIRT/CSIRT is an entity that responds to computer security or cybersecurity incidents which affect a specific sector. Sectoral CERTs are usually established for critical sectors such as healthcare, public utilities, emergency services and the financial sector. Unlike the government CERT, which services the public sector, the sectoral CERT provides its services to constituents from a single sector only.*

2.4. Is there any framework for the implementation of cybersecurity standards?

Exp: *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.*

2.4.1. In the public sector?

2.4.2. In the private sector?

2.5. Is there a framework for the certification and accreditation of cybersecurity professionals?

Exp: *Existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of 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), , 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.*

2.5.1. In the public sector?

2.5.2. In the private sector?

2.6. Are there any technical mechanisms and capabilities deployed to address spam?

2.7. Are there certain tools and technical measures related to providing cybersecurity, such as anti-virus or anti-spam software, available to the persons with disabilities?

3. Do you have any organizational measures?

3.1. Is there a national strategy for cybersecurity?

Exp: *Policies on national cybersecurity strategies or national plans for the protection of information infrastructures are those officially defined and endorsed by a nation state, 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; a roadmap for governance that identifies key stakeholders.*

3.1.1. Is your national strategy standalone?

Exp: *The national strategy for cybersecurity may be contained in a document separate from a national information, technology or security strategy.*

3.1.1.1. Does it address the private sector?

Exp: *The strategy defines the cybersecurity roles and responsibilities for actors within a* *private sector.*

3.1.1.2. Does it address the public sector?

Exp: *The strategy defines the cybersecurity roles and responsibilities for actors within public sector.*

3.1.1.3. Is there a section on the protection of critical information infrastructure?

Exp: *The strategy includes plans for the protection of critical information infrastructure.*

3.1.1.4. Is there a roadmap for governance?

Exp: *The strategy includes a roadmap with milestones for the achievement and completion of the strategy.*

3.1.1.5. Is the strategy revised on a recurring basis?

Exp: *The strategy is updated according to national, technological, social, economic and political developments that may affect it.*

3.1.1.6. Is the strategy open to public consultation?

Exp: *The strategy is open for consultation by all relevant stakeholders, including operators of infrastructure, ISPs, academia etc.*

3.1.1.7. Does the strategy include a national resiliency plan?

Exp: *A national resiliency plan ensures that the country recovers from the effects of any disaster (natural or man-made) in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions.*

3.1.2. Is your national cybersecurity strategy included as part of another broader national strategy?

3.1.2.1. Is there a section on the protection of critical information infrastructure?

Exp: *Critical infrastructures are key systems crucial for safety, security, economic security and public health of a nation. These systems may include, but are not limited to: Defense systems, Banking and Finance, Telecommunications, Transport, Health, Energy etc.*

3.1.2.2. Is there a roadmap for governance of the cybersecurity section?

3.1.3. Does it define priorities for the public sector?

3.1.4. If there is not a cybersecurity strategy in place, is one currently in development?

3.1.5. Does the existing strategy or the one in development, include actions pertaining to persons with disabilities?

3.2. Is there a national body/agency responsible for cybersecurity?

Exp: *A responsible agency for implementing a national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils or cross-disciplinary centres. Such a body may also be directly responsible for the national CIRT. The responsible agency may exist within the government and may have the authority to compel other agencies and national bodies to implement policies and adopt standards.*

3.2.1. Is there an agency responsible for critical information infrastructure protection?

3.2.2. Is there a national agency acting as focal point for Spam related issues?

3.3. Are there any metrics used to measure cybersecurity development at a national level?

Exp: *Existence of any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development, risk-assessment strategies, cybersecurity audits, and other tools and activities for rating or evaluating resulting performance for future improvements. For example, based on ISO/IEC 27004 which is concerned with* measurements relating to information security management

3.3.1. Are cybersecurity risk assessments performed periodically?

Exp: *A systematic process comprising risk identification,* risk *analysis and risk evaluation.*

3.3.1.1. Is there a cybersecurity benchmark for assessing risk?

3.3.1.2. Are the results rated or evaluated for future improvements?

3.3.2. Are recurring cybersecurity audits performed?

Exp: *A security audit is a systematic evaluation of the security of an information system by* *measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices*

3.3.2.1. Are they mandatory?

Exp: *Imposed by internal, sectoral regulations or adherence to certification standards ISO270001*

4. Do you have any capacity building activities?

4.1. Is there a standardization body within the country?

Exp: *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 is 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. This indicator measures the existence of a national cybersecurity standardization body and activities in the development and implementation of cybersecurity standards.*

4.1.1. Does it develop its own cybersecurity standards?

Exp: *Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization. This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including prevention or mitigation of cybersecurity attacks*; some countries adopt international standards and adapt it to their local environment and brand them as a national standard. Others (with advance R&D) create standards that are depending on uptake, gain international recognition and feed in new international standards.

4.1.2. Does it adopt existing international cybersecurity standards?

Exp: *Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization. This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including prevention or mitigation of cybersecurity attacks*; some countries adopt international standards and adapt it to their local environment and brand them as a national standard. Others (with advance R&D) create standards that are depending on uptake, gain international recognition and feed in new international standards.

4.2. Are national or sectoral cybersecurity best practices collected or guidelines created?

Exp: *Best practices are methods or procedures which have a proven track record of success. Adopting best practices will not only reduce the probability of failure but also increase efficiency.*

4.3. Is there investment in cybersecurity research & development programs?

Exp: *Cybersecurity research programmes include, but are not limited to, malware analysis, cryptography research and research into system vulnerabilities and security models and concepts. Cybersecurity development programmes refer to the development of hardware or software solutions that include but are not limited to firewalls, intrusion prevention systems, honey-pots and hardware security modules. The presence of an overarching national body will increase coordination among the various institutions and sharing of resources.*

4.3.1. In the public sector?

4.3.2. In higher education institutions?

4.3.3. Is there a nationally recognized institutional body overseeing cybersecurity R&D activity?

4.4. Are public awareness campaigns in cybersecurity developed and implemented?

Exp: *Public awareness includes efforts 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 centres, computer stores, community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behaviour on line. This includes actions such as setting up portals and websites to promote awareness, disseminating support material and establishing cybersecurity adoption.*

4.4.1. For organizations?

Exp: *Public awareness campaigns targeting organizations.*

4.4.2. For civil society?

Exp: *Awareness campaigns targeting the public at large.*

4.4.2.1. For adults (>18 yrs)?

4.4.2.2. For youth (12-17 yrs)?

4.4.2.3. For children (<12yrs)?

4.4.3. As a part of public awareness campaigns, is the public informed about the benefits of using cybersecurity software, hardware or service-based solutions?

4.4.4. Are any such cybersecurity software, hardware or service-based solutions made available to the public?

Exp: *Available to the public free of charge, for example, as a part of an awareness campaign or provided at a reduced fee.*

4.5. Does your organization/government develop or support the development of any professional training courses in cybersecurity?

Exp: *Existence of national or sector-specific educational and professional training programmes, promoting cybersecurity courses in the workforce (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector.*

4.5.1. For organizations?

4.5.2. For the public sector?

4.5.3. For civil society?

4.6. Does your organization/government develop or support the development of any educational programs or academic curricula in cybersecurity?

Exp: *Existence and the promotion of national education courses and programmes to train the younger generation in cybersecurity-related skills and professions in schools, colleges, universities and other learning institutes. Cybersecurity-related skills include, but are not limited to, setting strong passwords and not revealing personal information on line. Cybersecurity-related professions include, but are not limited to, cryptanalysts, digital forensics experts, incident responders, security architects and penetration testers.*

4.6.1. In primary school?

4.6.2. In secondary school?

4.6.3. In higher education?

4.7. Are there any government incentive mechanisms to encourage capacity building in the field of cybersecurity?

Exp: *Any incentive efforts by government to encourage capacity building in the field of cybersecurity, whether through tax breaks, grants, funding, loans, disposal of facilities, and other economic and financial motivators, including dedicated and nationally recognized institutional body overseeing cybersecurity capacity-building activities. Incentives increase the demand for* *cybersecurity-related services and products, which improves defences against cyberthreats.*

4.7.1. Is there a nationally recognized institutional body overseeing cybersecurity capacity building activities?

4.8. Is there a homegrown cybersecurity industry?

Exp: *A favourable economic, political and social environment supporting cybersecurity development will incentivize the growth of a private sector around cybersecurity. The existence of public awareness campaigns, manpower development, capacity building and government incentives will drive a market for cybersecurity products and services. The existence of a home-grown cybersecurity industry is testament to such a favourable environment and will drive the growth of cybersecurity start-ups and associated cyber-insurance markets.*

4.8.1. Is there a cyber-insurance market?

Exp: *Cyber-insurance is an insurance product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities.*

4.8.1.1 Do you provide subsidies to businesses and other entities that are unable to acquire cyber risk insurance on the open market?

4.8.2. Are there any incentives provided for the development of a cybersecurity industry?

Exp: *This indicator looks at any incentive efforts by government to encourage capacity building in the field of cybersecurity, whether through tax breaks, grants, funding, loans, disposal of facilities, and other economic and financial motivators, including a dedicated and nationally recognized institutional body overseeing cybersecurity capacity-building activities. Incentives increase the demand for cybersecurity-related services and products, which improves defences against cyberthreats.*

4.8.2.1. Is there any support provided to cybersecurity startups?

Exp*: Mechanisms in place to support development of cybersecurity start-ups (tax incentives, technology parks, free trade zones etc.) and for SMEs (Small and Medium Size Enterprises).*

5. Do you have any cooperative measures?

5.1. Are there any bilateral agreements for cybersecurity cooperation?

Exp: *Bilateral agreements (one-to-one agreements) refer to any officially recognized national or sector-specific partnerships for sharing cybersecurity information or assets across borders by the government with one other foreign government, regional entity or an international organization (i.e. the cooperation or exchange of information, expertise, technology and other resources).*

5.1.1. With nation states?

5.1.1.1. Is the agreement legally binding?

Exp: *Common legal phrase indicating that an agreement has been consciously made and certain actions are now either required or prohibited by law.*

5.1.1.1.1. For information sharing?

Exp: *Information-sharing refers to the sharing of threat intelligence.*

5.1.1.1.2. For asset sharing?

Exp: *Asset-sharing designates the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.*

5.1.1.2. Is the agreement non-legally binding, informal or pending ratification?

5.1.1.2.1. For information sharing?

5.1.1.2.2. For asset sharing?

Exp: *Assets may include human resources, facilities, equipment, etc.*

5.1.2. With international organizations?

5.1.2.1. Is the agreement legally binding?

5.1.2.1.1. For information sharing?

5.1.2.1.2. For asset sharing?

Exp: Assets may include human resources, facilities, equipment, etc.

5.1.2.2. Is the agreement non-legally binding, informal or pending ratification?

5.1.2.2.1. For information sharing?

5.1.2.2.2. For asset sharing?

Exp: Assets may include human resources, facilities, equipment, etc.

5.2. Are there any multilateral or international agreements on cybersecurity cooperation?

Exp: *Multilateral agreements (one to multiparty agreements) refers to any officially recognized national or sector-specific programmes for sharing cybersecurity information or assets across borders by the government with multiple foreign governments or international organizations (i.e. the cooperation or exchange of information, expertise, technology and other resources). It may also include ratification of international agreements regarding cybersecurity, such as African Union Convention on Cyber Security and Personal Data Protection, Budapest Convention on Cybercrime and others.*

5.2.1. Is the agreement legally binding?

5.2.1.1. For information sharing?

5.2.1.2. For asset sharing?

Exp: Assets may include human resources, facilities, equipment, etc.

5.2.2. Is the agreement non-legally binding, informal or pending ratification?

5.2.2.1. For information sharing?

5.2.2.2. For asset sharing?

Exp: Assets may include human resources, facilities, equipment, etc.

5.3. Does your organization/government participate international fora/associations dealing with cybersecurity?

5.4. Are there any public-private partnerships in place?

Exp: *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 information (threat intelligence) and 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), whether nationally or internationally.*

5.4.1. With local companies?

5.4.1.1. For information sharing?

5.4.1.2. For asset sharing?

5.4.2. With foreign companies?

5.4.2.1. For information sharing?

5.4.2.2. For asset sharing?

Exp: *Assets may include human resources, facilities, equipment.*

5.5. Are there any interagency partnerships in place?

Exp: *This performance indicator refers to any official partnerships between the various government agencies within the nation state (does not refer to international partnerships). This can designate partnerships for information- or asset-sharing between ministries, departments, programmes and other public sector institutions.*

5.5.1. For information sharing?

5.5.2. For asset sharing?

Exp: *Assets may include human resources, facilities, equipment.*

SECTION 2

1. Do you have measures for protecting Children Online?

1.1. Is there legislation related to child online protection?

Exp: *It will generally be necessary for there to be in place a body of laws which makes it clear that any and every crime that can be committed against a child in the real world can, mutatis mutandis, also be committed on the Internet or on any other electronic network. It may also be necessary to develop new laws or adapt existing ones to outlaw certain types of behavior which can only take place on the Internet, for example the remote enticement of children to perform or watch sexual acts, or "grooming" children to meet in the real world for a sexual purpose (ITU Guidelines for Policy Makers on Child Online Protection).*

1.2. Is there an agency/entity responsible for Child Online Protection?

Exp: *Existence of a national agency dedicated to child online protection.*

1.2.1. Is there an established public mechanism for reporting issues associated with child online protection?

Exp: *Telephone number, email address, web form where the interested parties can report the incidents or concerns related to child online protection.*

1.2.2. Are there any technical mechanisms and capabilities deployed to help protect children online?

1.2.3. Has there been any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online?

1.2.4. Are there any child online protection education programs?

1.2.4.1. For educators?

1.2.4.2. For parents?

1.2.4.3. For children?

1.3. Is there a national strategy for child online protection?

1.4. Are there public awareness campaigns on child online protection?

1.4.1.1. For adults (>18 yrs)?

1.4.1.2. For youth (12-17 yrs)?

1.4.1.3. For children (<12yrs)?

SECTION 3

<u>Addendum: opinion based survey</u>

1. In your opinion, how important is raising awareness on cybersecurity as a basic step to achieving security in cyberspace?
   a. Not important
   b. Somewhat important
   c. Important
   d. Very Important
2. Which groups are targeted by cybersecurity awareness campaigns in your country ?
   a. Children
   b. Youth
   c. Students
   d. Elderly people
   e. Persons with disabilities
   f. Private institutions
   g. Government agencies
   h. Others

3. Which one of the groups identified below is more targeted? Please arrange in order of 1 to 6 for the highly targeted to the less targeted?

   a. Children
   b. Youth
   c. Students
   d. Elderly people
   e. Persons with disabilities
   f. Private institutions
   g. Government agencies
   h. Others

4. What are the cybersecurity issues that are addressed by existing awareness campaigns? (Replies to more than one item possible)

   a. Internet safety
   b. Privacy
   c. Fraud
   d. Phishing
   e. Malware
   f. Child Online Protection
   g. Others

5. What is the degree of importance of each issue? Please arrange in order of the most important to the less important and give reasons for such order?

   a. Internet safety
   b. Privacy
   c. Fraud
   d. Phishing
   e. Malware
   f. Child Online Protection
   g. Others

6. Have you been receiving assistance from or collaborating with ITU in Cybersecurity ?

   a. If yes, please give details and your opinion on the effectiveness of this assistance/collaboration and tell us how us any specific cybersecurity areas to be looked into
   b. If no, please inform us why and tell us how we can assist ?