Global Cybersecurity Index (GCI) 2018 Questionnaire Guide

This document is for information only. The GCI measures the commitment of countries in cybersecurity according to 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 2017/18 Score together with those required by ITU-D Study Group 2 Question 3. The questionnaire is composed of five separate sections, where questions in all sections have yes/no responses accompanied by ticking the boxes placed before each element. 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.

1. Legal measures

1.1. Do you have law related to cybercrime?

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.*

☐ *YES*
☐ *No*
☐ *Partial (These can **only** be drafts in advanced stage and ready to be adopted or verified)*

1.1.1 Do you have Substantive law on…

***EXP**: Substantive law refers to public and private law, including the law of contracts, real property, tort, wills, and criminal law that creates, defines and regulates rights.* (**Specify by ticking into the box of an article that applies to your country and mark pages and the number of articles where the following articles are found in your documents)**

☐ unauthorized access of computers, systems and data?

☐ unauthorized interference/interception / modification/destruction of computers, systems and data?

☐ data/privacy protection?

Provide links/url

Provide documents

Explanation of a partial law or article by providing the drafts of only the above articles.

1.1.2 Procedural cybercriminal law on…

EXP: *The rules by which a court determines what happens in civil lawsuits, criminal or administrative proceedings and designed to ensure a fair and consistent application of due process or fundamental justice to all cases that come before a court. .* **(Specify by ticking into the box of an article that applies to your country and mark pages and the number of articles where the following articles are found in your documents).**

☐ articles on expedited preservation of stored computer data,
☐ Production orders,
☐ Search and seizure of stored computer data,
☐ Real-time collection of computer data,
☐ Extradition of cyber perpetrators,
☐ Mutual assistance,
☐ Confidentiality and limitation of use.)

Provide links/url

Provide documents

Explanation of a partial law or article by providing the drafts of only the above articles

1.2. Is there any cybersecurity regulation related to…

Exp: *Regulation: rules based on, and meant to carry out, a specific piece of legislation. Regulations are enforced by* ***a regulatory agency*** *mandated to carry out the purpose or provisions of a legislation. Cybersecurity regulation would thus designate principles abided by stakeholders, emanating from and being part of the implementation of laws dealing with.* **(Specify by ticking into the box of a regulation that applies to your country and mark pages and the number of the article where the following regulations are found in your documents**) Please not that this section is only dedicated to regulations not laws/legislation mentioned in question 1.1.1

☐ *YES*
☐ *No*
☐ *Partial*

☐ *Data protection?*
☐ *breach notification?*
☐ *cybersecurity audit requirements and cybersecurity certification/standardization*
☐ *privacy protection,*
☐ *digital signatures and e-transactions?*
☐ *Liability of Internet service providers?*
☐ System and network protection?

Provide links/url

Provide documents

Explanation of a partial law or article by providing the drafts of only the above articles.

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

Exp: *refers to legislation/regulations related to the protection against unwanted emails as a result of internet use. (Please provide either the regulation or the legislation (law) or both)*

☐ *YES*
☐ *No*
☐ *Partial*

Provide links/url

Provide documents

Explanation of a partial law or article by providing the drafts of only the above articles.

1.4 Please provide some of the best practices/achievements/progress your country has/is being involved in pertaining to the legal areas as part of cybersecurity activities? (N.B best practices only applies to countries with cybersecurity laws or regulations)

Provide links/url

Provide documents

List down best practices here if no link or document above

2. Technical measures

2.1. Is there a CIRT, CSIRT or CERT?

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.*

- ☐ Yes
- ☐ No

2.1.1 Indicate which of the following CERT, CSIRT OR CERT below applies to your country.

Exp: *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.*

- ☐ A national CIRT, CSIRT or CERT
- ☐ A Government CIRT, CSIRT or CERT
- ☐ Sectoral CIRT, CSIRT or CERT

Provide links/url

Provide documents

2.2. Does the CIRT, CSIRT or CERT conduct continuous 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?*

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

2.3. Is the above selected CIRT, CSIRT or CERT affiliated/associated with

- ☐ FIRST
- ☐ *Regional CERTS (APCERT, ICCERT, AFRICACERT, TFCCERT)*

☐ Any other CERT Associations

Provide links/url
Provide documents

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.*

☐ In the public sector
☐ In the private sector

Provide links/url
Provide documents

2.5. Do you have standardization body within the country that

☐ provides its own standard on cybersecurity
☐ Or adopts to the international standards
Provide links/url
Provide documents

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

Exp: Are there certain tools and technical measures related to providing cybersecurity, such as anti-virus or anti-spam software

☐ Yes
☐ No
Provide links/url
Provide documents

2.7. Does your government/organization use cloud for cybersecurity in the public sector?

Exp: *A Software to ensure data backup in case of unwanted internet or computer interference apart from the use of antivirus software, Internet Security Software suites, anti-malware and encryption to improve on government's cybersecurity systems. The cloud system allows one to use and access their documents/data or any saved materials anywhere and at any time without the damages caused by computer interference on one end. (Again the aim of the question is to*

get an understanding on the potential use of cloud to improve cybersecurity posture at the national level without any specification of a particular software in cloud)

☐ Yes
☐ No
Provide links/url
Provide documents

2.8. **Please provide some of the best practices/ achievements/progress your country has/is being involved in pertaining to the technical areas as part of cybersecurity activities? (**N.B best practices only applies to countries with **CIRT, CSIRT or CERT**)

Provide links/url
Provide documents

3. Organizational measures

3.1. Is there a national strategy (Policy) 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. (If one is still being developed then tick the partial box and go directly to qtn 3.8 and if strategy is not available, go directly to question 3.8 as well)*

- ☐ Yes
- ☐ No
- ☐ *Partial (These can only be drafts in advanced stage and ready to be adopted or verified)*

Provide links/url

Provide documents

Explanation of a partial draft by providing the drafts of the national strategy.

3.2. Is your national strategy

Exp: *The national strategy for cybersecurity may be contained in a document separate from a national information, technology or security strategy* (If you have uploaded the strategy in the above question, there is no need to upload the document twice, just indicate the page number that has proofs relevant to the questions below till 3.5)

- ☐ Standalone
- ☐ Or included as part of another broader national strategy

Page number

3.3. Does it address

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

- ☐ The private sector
- ☐ The public sector

Page number

3.4. Is there a section on:

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

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.*

- ☐ the protection of critical information infrastructure?
- ☐ a national resiliency plan

Provide Page number

3.5. Is there a clear action plan for government implementation on cybersecurity governance?

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

- ☐ Yes
- ☐ No

Provide Page number

3.6. Is the strategy

- ☐ revised on a continuous basis?
- ☐ open to public consultation?

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

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

Provide Page number or

Link indicating open consultation

3.7. Is there a national body/agency responsible for:

- ☐ cybersecurity and critical information infrastructure protection
- ☐ initiatives in combating Spam related issues?

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.*

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

3.8. 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

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

3.9. Are cybersecurity risk assessments performed periodically?

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

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

3.10. Is there a cybersecurity benchmark for assessing risk?

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

3.11. Are general 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

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

3.12. Please provide some of the best practices/achievements/progress your country has/is being involved in pertaining to the organizational measures as part of cybersecurity activities

Provide links/url

Provide documents

4. Capacity building activities

4.1. 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.*

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

4.2. *Does the public awareness campaigns target:*

- ☐ Organizations
- ☐ Civil society
- ☐ Adults
- ☐ *Youth &* Children
- ☐ *Other related bodies*

Provide numbered links/url respectively to each of the above box you choose

Provide numbered documents respectively to each of the above box you choose

4.3. 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.*

- ☐ In the public sector
- ☐ In the private sector

Provide links/url

Provide documents

4.4. Does your organization/government develop or support 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.*

- ☐ For law enforcement (police officers and enforcement agents
- ☐ For judicial and other legal actors (judges, solicitors, barristers, attorneys, lawyers, paralegals, etc.)
- ☐ For organizations
- ☐ For the public sector
- ☐ For civil society
- ☐ *others*

Provide numbered links/url respectively to each of the above box you choose

Provide numbered documents respectively to each of the above box you choose

4.5. Does your organization/government develop or support 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.*

- ☐ In primary school
- ☐ In secondary school
- ☐ In higher education
- ☐ *others*

Provide numbered links/url respectively to each of the above box you choose

Provide numbered documents respectively to each of the above box you choose

4.6. 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.*

- ☐ In the public sector
- ☐ *In the private sector*
- ☐ In higher education institutions (Academia)

☐ a nationally recognized institutional body overseeing cybersecurity R&D activity
☐ *a* recognized institutional body overseeing cybersecurity capacity building activities
☐ *others*

Provide numbered links/url respectively to each of the above box you choose

Provide numbered documents respectively to each of the above box you choose

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.*

☐ Yes
☐ No

Provide links/url

Provide documents

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.*

☐ Yes
☐ No

Provide links/url

Provide documents

4.9. 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.*

☐ Yes
☐ No

Provide links/url

Provide documents

4.10. Is there any support provided to cybersecurity startups and development?

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).*

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

4.11. Please provide some of the best practices/achievements/progress your country has/is being involved in pertaining to the capacity building measures as part of cybersecurity activities

Provide links/url

Provide documents

List down best practices here if no link or document above

5. Cooperative measures

5.1. Are there any bilateral agreements for cybersecurity cooperation with:

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).*

- ☐ Nation states or member states
- ☐ International organizations
- ☐ None of the above

5.2. Is/are the agreement/s

- ☐ legally binding
- ☐ For information sharing
- ☐ For asset sharing
- ☐ non-legally binding, informal
- ☐ pending ratification

5.3. Are there any multilateral 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.*

- ☐ Yes
- ☐ No

Provide links/url

Provide documents

5.4. Is the agreement

- ☐ legally binding
- ☐ For information sharing
- ☐ For asset sharing
- ☐ non-legally binding, informal
- ☐ pending ratification

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

- ☐ Yes

☐ No

Provide links/url

Provide documents

5.6. 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.*

☐ With local companies

☐ With foreign companies

5.7. Are there any partnerships in place as:

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.*

☐ *Inter-agency partnerships*

☐ *Intra-agency partnerships*

Provide links/url

Provide documents

5.8. Please provide some of the best practices/ achievements/progress your country has/is being involved in pertaining to the cooperation measures as part of cybersecurity activities

Provide links/url

Provide documents

6. Supplementary survey: Child online protection

6.1. Are there any measures for protecting Children Online?

☐ *Yes*

☐ *No*

6.1.1. 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).*

☐ *YES*

☐ *No*

☐ *Partial (These can **only** be drafts in advanced stage and ready to be adopted or verified)*

Provide links/url

Provide documents

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

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

☐ *YES*

☐ *No*

Provide links/url

Provide documents

6.2.1. 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.*

☐ *YES*

☐ *No*

Provide links/url

Provide documents

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

☐ *YES*
☐ *No*

Provide links/url

Provide documents

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

☐ *YES*
☐ *No*

Provide links/url

Provide documents

6.2.4. Are there any child online protection education programs?

☐ *For educators*
☐ *for parents*
☐ *For children*

Provide links/url

Provide documents

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

☐ *YES*
☐ *No*

Provide links/url

Provide documents

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

☐ *For adults*
☐ *For youth*
☐ *For children*

Provide links/url

Provide documents

7. Addendum: opinion based survey

7.1. 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

7.2. 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

7.3. 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

7.4. 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

7.5. 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

7.6. 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?