Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Country-level cybersecurity posture assessment:Study and analysis of practices

Ashutosh Bahuguna , R. K. Bisht & Jeetendra Pande

To cite this article: Ashutosh Bahuguna , R. K. Bisht & Jeetendra Pande (2020): Country-level cybersecurity posture assessment:Study and analysis of practices, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2020.1767239

To link to this article: https://doi.org/10.1080/19393555.2020.1767239

Published online: 22 May 2020.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2020.1767239

Country-level cybersecurity posture assessment:Study and analysis of practices

Ashutosh Bahuguna[a], R. K. Bisht[b], and Jeetendra Pande[c]

[a]Scientist- Indian Computer Emergency Response Team, Ministry of Electronics and IT, Government of India, New Delhi, India; [b]Department of Mathematics and Computing, Graphic Era Hill University, Dehradun, India; [c]School of Computer Science & IT, Uttarakhand Open University, Haldwani, India

ABSTRACT

Along with positive impacts, ICT transformation also increases the exposure of critical infrastructure to cyber-attacks. Keeping in view the constantly evolving cyber-threat landscape, it is vital for a country to continuously assure the cybersecurity of its ICT infrastructure. Recently the security of the cyberspace has got a much-needed emphasis from Governments and International Agencies. To generate assurance, actions initiated by a country to counter cyber threats need to be continuously assessed for implementation & effectiveness.

This study aims to offer a new perspective on country-wide cybersecurity benchmarking and assurance. The paper presents the study and analysis of the methods and practices adopted by countries for cybersecurity posture assessment and generating assurance on the implemented cybersecurity measures. In this paper, the cybersecurity posture assessment and assurance practices implemented by 37 countries are studied with an objective of understanding the global scenario and identification of different methods adopted for a cybersecurity posture assessment.

KEYWORDS

Cybersecurity Assurance; cybersecurity Benchmarking; cybersecurity Measurement; cybersecurity Maturity Model; cyber Threat Assessment

1. Introduction

Cyberspace and digitization emerged as the growth catalyst for the economies and its citizens around the world. While on bright side cyberspace has immense potential for growth and benefits, on the dark side vulnerability in cyberspace can lead to adverse impacts on the critical infrastructure of a country. Cyber-attacks and cybercrimes can jeopardize the wellbeing of the nation & its citizens. Cyber-attacks that target the critical infrastructure of a nation-state can effectively reduce available state resources, and undermine confidence in their supporting structures (Ministry of Electronics and IT, 2013). A cybersecurity attack such as a malware attack, cyber espionage, targeted attack, attack on critical information infrastructure and other related incidents can have an adverse impact on a nation's critical parameters such as national security, economy, and public safety.

Due to a surge in malicious attacks and the possibility of cyber-attacks impacting a country's well-being, nation-states around the globe came up with a variety of initiatives to improve their cybersecurity posture for countering cyber-attacks. Some widely acknowledged initiatives are:

a. National Cybersecurity Strategy: 73 out of 193 members of the International Telecommunication Union (ITU) have made national cybersecurity strategies publicly available (ITU) [ITU, n.d.].
b. Setting up of National Computer Security Incident Response Teams (CSIRTs) & sectoral CSIRTs such as Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), United States (ICS-CERT) [ICS-CERT, n.d.]
c. Legal and Regulatory measures such as the Indian Information Technology Act 2000 (Ministry of Electronics and IT, 2000)
d. Critical Information Infrastructure Protection Plans (European Union Agency for Network and Information Security, 2015a) and
e. National and International Cybersecurity exercises (European Union Agency for Network and Information Security, 2015b).

CONTACT Ashutosh Bahuguna bahuguna.a@meity.gov.in Indian Computer Emergency Response Team, Ministry of Electronics and IT, 6 CGO Complex, Lodi Road, New Delhi, 110003, India

Country-level cybersecurity benchmarking efforts are undertaken by some countries and international & regional bodies to assess & measure cybersecurity preparedness of a particular country. Countries such as Australia and Austria implemented cybersecurity audits and cybersecurity exercises as methods for assessment and benchmarking of cybersecurity efforts at the national level (ITU, ABI Reserach., 2015). Similar assessments of the cybersecurity state of a country were also conducted by International/Regional bodies such as ITU.

In India, the National Cybersecurity policy 2013 emphasized the need for creating an assurance framework assisted by conformity assessment. One of the objectives mentioned in the policy is: *"To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people)"* (Ministry of Electronics and IT, 2013). The policy also listed strategies for creating the assurance framework. Some of the activities for benchmarking such as national cybersecurity drills, sectoral drills, impanelment of information security organizations, security auditing has been implemented at national and sectoral levels in India (Ministry of Electronics and IT, 2017).

Grass-root level data collection and analysis are needed for country-level assurance framework. Latest research and cutting edge solutions such as using machine learning for attack detection (Kozik & Choraś, 2014), automatic clustering of attacks in Intrusion Detection Systems (IDS) (Shojafar et al., 2019), similarity-based malware detection (Taheri et al., 2020) has promising potential for country-wide grass-root data collection & analysis.

This paper presents the detailed study and analysis of the methods and practices adopted by countries for the cybersecurity assessments and assurance at country-level. Findings were drawn from the analysis of data collected for 37 countries. Data for each of 37 countries were collected for following parameters (i) Types of cybersecurity posture assessment activities conducted in a country, (ii) Methods and tools used for conducting assessment activities, (iii) Frequency of assessment activities, (iv) Name & type of agency responsible for conducting assessment and (v) Output of assessment activities. The key contribution of this study to presents a new perspective in understanding methods adopted by countries for cybersecurity posture assessment and generating assurance on implemented cybersecurity measures.

The organization of the paper is as follows: Section 2 presents the methodology and techniques used for the study and analysis, Section 3 presents the experimental results, Section 4 analyzes & discusses the results and finally, Section 5 concludes the paper along with future research directions.

2. Methodology

Search and selection for benchmarking models was followed by the data collection and data enrichment. Further, Qualitative analysis techniques were applied to identify significant assessment categories. This section details the methodology adopted for the study.

2.1. Identification of models

For the purpose of identifying cybersecurity benchmarking models and studies, a search was performed for the keywords derived from "information security or cybersecurity benchmarking and assurance" on research databases, Google scholar and Google operator search. Results of the search were segregated into 3 categories based on the level (organization, sector & nation) of applicability of the benchmarking & assurance methods. Since the scope of the study was limited to national-level benchmarking & assurance efforts in cybersecurity, the following seven unique, national-level cybersecurity maturity assessment models & studies were found for further enquiry:

a. Cyber Index – United Nations (UN) report (United Nations, 2013).
b. Community Cybersecurity Maturity Model (CCSMM) (White, 2011).
c. Cyber Readiness Index (Hathaway, 2015).
d. National Cybersecurity Maturity Model (NCSecMM) (Mohamed Dafir Ech-cherif El Kettani, 2008).

e. Global Cybersecurity Index (GCI) & Cyberwellness Profiles – International Telecommunication Union (ITU) (ITU, ABI Reserach., 2015).
f. National Information Security Index (Korea Internet & Security Agency, 2008).
g. Cyber Power Index (Economist Intelligence Unit and Booz Allen Hamilton, 2011).

2.2. Data sources

Global Cybersecurity Index (GCI) & Cyberwellness Profiles of 195 countries published by International Telecommunication Union (ITU) were found most suitable for this study, as it covers the maximum number of countries and has a specific indicator for national benchmarking activity. Cyberwellness profiles of 195 countries had been studied and country-wide data reported in sub-category 'National Benchmarking' under the domain 'Organizational Measures' was collected. 37 countries among a total of 195 countries were identified as having activities listed under the national benchmarking indicator. Data was collected for 37 countries from the ITU cyberwellness profile. Since ITU wellness profiles have only brief descriptions of the benchmarking related activities of a country, collected data was further enriched from the following sources:

a. Government reports.
b. Statistics and reports from Computer Security Incident Response Teams (CSIRTs).
c. Websites of Government and benchmarking agencies.
d. Reports of international bodies and regional forums.
e. Assessment report and findings of third party auditors.
f. Media reports and press release.

Government reports, statistics and reports from Computer Security Incident Response

Teams (CSIRTs), websites of Government and benchmarking agencies were considered internal sources of data while reports of International Bodies & regional forums, assessment reports of auditors and media reports were considered as external sources.

2.3. Data enrichment and categorization

Data available from internal sources was considered valid data, as it is from trusted agencies like government reports. Data available from external sources such as media reports were validated using 'Method of Data Triangulation' (Duchon, 1988). The Method of Data Triangulation is a technique used for the validation of data from two or more sources. Further, country-level details of benchmarking & assurance activities were summarized. Summarized data were further coded and analyzed using methods of qualitative data coding (Shannak & Aldhmour, 2009). Data Coding as a method was used on summarized benchmarking data for sorting, analyzing, and identification of significant assessment categories adopted by countries for benchmarking activities. Code labels were assigned during the open coding phase followed by creating the categories in the axial coding phase and finally in the selective coding phase insignificant categories were eliminated. Figure 1 summarizes the steps involved in data collection and analysis for this study.

3. Experimental results

We have collected the related data for benchmarking activities of 37 countries using the ITU

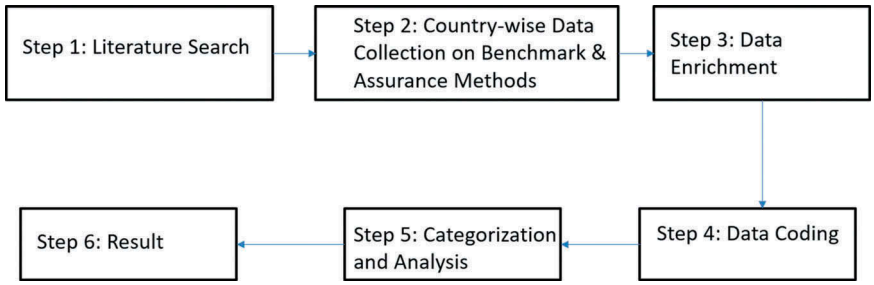

Figure 1. Data collection and analysis steps.

cyberwellness profile of each country. Country-wide data was further enriched from other sources as described in Section 2 and finally data was summarized as depicted in annexure-I. Country-wide benchmarking activities related data was segregated under five attributes of the benchmarking activity, described as follows:

(i) **Types of Activities for Cybersecurity Posture Benchmarking**: This column provides a short description of the nature of the benchmarking programs undertaken by the country, such as surveys, annual reports, and exercises.
(ii) **Specific Methods and Tools used for conducting Benchmarking**: Methodology and tools adopted by each country for benchmarking activities are listed under this column.
(iii) **Frequency of Benchmarking Activities**: Frequency with which benchmarking activity is conducted.
(iv) **Benchmarking conducted by (Type & Name of Agency)**: This column lists name and type of organization conducting the benchmarking activity.
(v) **Output Format of Benchmarking Activities**: This column listed output data characteristics of the benchmarking activity such as trend reports and incidents statistics.

4. Analysis and discussion

Summarized country-wide benchmarking data of the 37 countries as given in Annexure-I were analyzed and data coding techniques were applied to identify categories of practices adopted by the countries for cybersecurity assurance and benchmarking. On data of Annexure-I, qualitative data coding techniques were applied, first unique codes were assigned to the benchmarking activities as per characteristics of activities using open coding followed by creating the categories for benchmarking activities as per the assigned codes and finally insignificant categories were removed from the list. Table 1 summarizes the unique 7 categories of cybersecurity assurance and benchmarking activities identified in the data analysis and coding of data.

After summarizing the cybersecurity benchmarking & assurance categories and benchmarking activities, the following is the discussion and analysis on the usage of each activity.

Table 1. Significant categories of country-level assurance and benchmarking activities identified in the analysis.

S. No.	Category – Benchmarking Activity	Description of Activity	Among surveyed countries, no. of countries implemented the activity	References (S.No. of Table at Annexure-I)
1	Cybersecurity Development Report	Periodic or Annual stocktaking reports to review cyber threats and benchmark the cybersecurity development in the country and/or sectors.	8	2,6,7,11,14,16,19,26
2	Cybersecurity Exercises	Multilateral, Bilateral and domestic (national and sector-specific) cyber security exercises with objectives such as gaps identification, benchmarking, confidence building, improving coordination, improving incident resolution activities and others.	14	5,8,13,15,16,17,21,23,27, 29,30,32,35,37
3	Statistical data and Trend Reports	Periodic review of the statistical data such as Incident reported to national CSIRT, ICT development in sectors, cyber-attacks and others	4	1,3,17,25
4	Cybersecurity compliance and Audits	Cybersecurity Compliance and audits of critical sectors and organizations against security best practices.	9	1,9,17,22,27,28,31,35, 37
5	Maturity Models and Indexes	Maturity Models and indices such as Cybersecurity Maturity Model (CSMM) and KAMI index (Setiadi, Sucahyo, & Hasibuan, 2012a) for benchmarking the cyber security preparedness of the country or sector.	9	6,10,16,18,20,31,33, 36,37
6	Cybersecurity Surveys	Survey of citizens, businesses and government entities to measure cyber security developments and identification of priority areas.	3	13,23,27
7	Cybersecurity related Laws & Regulations and setup of supervisory agency	Cybersecurity specific laws, regulations and supervisory agency for enforcing and ensuring cyber security-related actions.	3	1,9,16

4.1. Cybersecurity development report

Cybersecurity reports of countries such as the annual report of cybersecurity development in Austria (ITU, 2015b) (Federal Chancellery of the Republic of Austria, 2014a), annual report of Indian Computer Emergency Response Team (CERT-In) (Indian Computer Emergency Response Team (CERT-In), 2015) are used for cybersecurity benchmarking. Periodic (usually annual) reports generally present cybersecurity-related threats, incidents, and developments in a country. In some cases, it also includes study related to the review of the cyber threat landscape in the country, an overview of activities such as participation in cyber exercises & audits, major incidents and incident statistics, case studies, cooperation in cybersecurity and future actions for improving the cybersecurity readiness of the country. It was observed that periodic cybersecurity status reports are mostly prepared by Government agencies such as the National Computer Emergency Response Teams.

4.2. Cybersecurity exercises

In our study, we found that the Cybersecurity exercises are a widely adopted activity by the countries. According to the European Union Agency for Network and Information Security (ENISA) cybersecurity exercises stocktaking report 2015, there has been an exponential growth in the number of cybersecurity exercises over the past decade with the trend expected to accelerate in the coming years (European Union Agency For Network And Information Security (ENISA), 2015). Cybersecurity exercises are used for benchmarking the cybersecurity readiness of the participating entity and improving coordination & cooperation among entities. Around the globe, different types of cybersecurity exercises with different objectives and frequency are regularly conducted. Depending on the objectives, exercises could be sector-specific drills, national cybersecurity exercises such as Cyber Storm (U.S. Department of Homeland Security, 2016), bilateral exercises or multilateral exercises such as Asia Pacific Computer Emergency Response Team (APCERT) drills (Asia Pacific Computer Emergency Response Team (APCERT), 2017). Cybersecurity exercises also vary in technical, operational, and strategic scenarios and the nature of execution from table-top exercises to full-simulated drills. International and regional entities also conduct the exercises for improving incident handling, sharing best practices, and improving regional cooperation in cybersecurity. ITU-IMPACT ALERT (International Telecommunication Union (ITU) and International Multilateral Partnership Against Cyber Threats (IMPACT), 2013), and Cyber Europe by ENISA (European Union Agency for Network and Information Security (ENISA), 2016) are examples of such exercises. Cybersecurity exercises are recognized for providing opportunities for countries to benchmark their cybersecurity posture and generate assurance on the existing cybersecurity measures.

4.3. Statistical data and trend report

Statistical data such as cybersecurity incidents data is also used for benchmarking cybersecurity developments and threat landscape in the countries. For example, the Cybersecurity Assessment Netherlands (CSAN) program provides statistics of incidents handled, vulnerabilities, and sector-specific assessment of cybersecurity in the Netherlands (The National Cyber Security Centre (NCSC), 2016). Cybersecurity statistical data and trend reports are generated at country-level to draw a cyber threat landscape for the country and identify priority areas to tackle. These statistics and reports are mostly generated by Computer Security Incident Response Teams (CSIRT) and Information Sharing & Analysis Centers (ISAC). Trends of incidents, targeted attacks, attacks on critical infrastructure, type of cyber-attacks, vulnerabilities exploited, and security assessments are used for benchmarking cybersecurity capabilities of the country.

4.4. Cybersecurity compliance and audits

Compliance and audit against the cybersecurity standards and best practices are adopted to assess the cybersecurity posture of the organizations. Compliance and audit exercises are adopted by countries for benchmarking the cybersecurity preparedness of key organizations. These cybersecurity compliance exercises and audits are generally initiated by Government agencies & regulatory bodies and used to have assurance on the controls

implemented for cybersecurity. Since it is tedious to perform the audit and compliance assessment for an entire country under a single program, these activities are conducted for selected organizations such as critical sector organizations, Government systems, businesses like "cybersecurity health checks" for Australian Securities Exchange 100 (ASX100) listed businesses in Australia (Australian Government, ASIC, KPMG, Deloitte, EY, Pwc., 2017). Compliance and audit exercises are generally proactive (before incidents occur). However, in some instances audits & compliance exercises of targets (specific systems, organizations or sector) were also initiated on post-occurrence of the cybersecurity incident to assess the vulnerabilities of the targets. These exercises are conducted using the method of self-assessment, regulation-driven or by an independent third-party auditor and involves activities such as checklist-based compliance against security best practices and standards, vulnerability assessment, penetration testing, risk assessment, and workshop assessments. In the cases of some countries, audit and compliance is also enacted by the act or regulation which mandate periodic cybersecurity compliance reporting of the critical sector organizations.

4.5. Maturity models and indexes

International organizations such as the Potomac Institute for Policy Studies, ITU, and a few countries such as South Korea and Indonesia have adopted formal Cybersecurity Maturity Models and measurement indices for benchmarking the cybersecurity posture. One such measurement index, National Information Security Index (NISI) was developed by Korea Internet & Security Agency (KISA), South Korea (Korea Internet & Security Agency, 2008) [Korea Internet and Security Agency, n.d.] with the objective of measuring current cybersecurity posture and identification of priority areas. The NISI is calculated from three-component indices generated from 12 low-level indices. Cybersecurity index and wellness profiles by ITU and Cyber Readiness Index (CRI) and country reports by the Potomac Institute for Policy Studies assess the country-level cyber/information security preparedness on parameters such as governance, incident response capabilities, organizational setup, law & regulations, capacity building, research & Development, coordination & cooperation and other similar parameters at an abstract level. The cyber posture scorecard is based on the National Institute of Standards & Technology (NIST) standards & best practices (National Institute of Standards and Technology (NIST), 2011a).The National Cybersecurity Standard (NCSec Referential) (Mohamed Dafir Ech-cherif El Kettani, 2008) derived from ISO 27002 standard (ISO/IEC, 2012), and the Cyber Power Index which measures 39 indicators developed jointly by the Economist's Intelligence Unit & Booz Allen are other examples of indices & models for cybersecurity benchmarking at the country-level (Economist Intelligence Unit and Booz Allen Hamilton, 2011).

4.6. Cybersecurity surveys

We found that three countries (Georgia, Mauritius, and Oman) that used surveys as a tool for benchmarking the current state of the cybersecurity in the country. A nationwide survey was conducted in Georgia for an e-readiness study. A survey of Information Security State in business was conducted by Mauritius. A Global Information Security Survey (GISS) in Oman was conducted by Ernst & Young (Times of Oman, 2015). Survey targets and collects data from citizens, businesses, critical sectors, and government to assess cybersecurity development in the country and focus areas.

4.7. Cybersecurity related laws & regulations

Cybersecurity related laws and regulations are also adopted for enforcing cybersecurity requirements by countries or sector. In some instances, benchmarking and assessment of cybersecurity postures are enacted with laws and regulations. For instance, the Public Information Act of Estonia mentions inspection of the security of the information systems of state and local government agencies and providers of vital services (Government of Estonia, 2016). Supervisory entities for periodic assessment of cybersecurity readiness are also created for ensuring compliance to regulations, for example. Hungarian information security law created Assessment and Supervision

Agency National Electronic Information Security Authority (NEISA) (National Electronic Information Security Authority, 2019) with the goal of handling and controlling the data of central and local government agencies regarding their cybersecurity policies and compliance against the declared security posture.

In Section 4.1 we discuss the important points observed from the above study.

4.8. Key observations

The following are the key observations derived from analysis of categories of activities adopted for assurance & benchmarking by countries:

a. There is a lack of an overarching framework for cybersecurity assurance and compliance at the national level, and benchmarking activities are currently conducted on an ad-hoc basis. Hence there is a lack of visibility of the cybersecurity posture of a country.
b. Cybersecurity exercises are widely adopted for cybersecurity posture improvement but there is a lack of metrics for benchmarking the performance.
c. Compliance and audit activities have been thoroughly adapted for benchmarking but the focus of these activities are limited in scope for key organizations only.
d. In statistical and survey methods there is a need to improve the method of collection of data, interpretation of data, and standardization of the representation format to deduce the effective posture of the country.
e. Laws, regulations, and setup of supervisory agencies are well intended, but there is a need to be regular updates regarding the changing threat landscape. Also, there is a need to ensure that activity is not conducted for compliance sake only.
f. Few countries and international organizations have implemented formal maturity models and scales for the measurement at the country-level. However, measurement indicators are only at an abstract level and sufficient data from a grass-roots level is not included in the measurement exercises.
g. There was no available data for the comparison of the effectiveness of different assessment methods, before the selection of a particular method of assessment by a country.
h. There is the need for refinement especially of the development of quantitative matrices for all 7 identified significant categories.
i. Although formal methods for benchmarking cybersecurity posture were developed by a few countries, the implementation and success of these models is not known.
j. A national cybersecurity assurance framework with a dedicated government cybersecurity benchmarking agency needs to be set up to assess & present the cybersecurity posture of a country and its critical sectors on a continuous basis.

4.9. Limitations

Since limited research was available on the topic, the following two factors may have affected the coverage of data collection and identification of any new assessment method:

a. Cybersecurity activities are sometimes treated & labeled as they are held as confidential by governments and hence data with respect to such initiatives may not be available in the public domain.
b. There is a possibility that cybersecurity issues are catered for by the laws and regulations of a country. However, cybersecurity is not the primary objective & title of that law/regulation and hence it will not appear using our search method.

5. Conclusion and future work

With the objective to study and analyze practices adopted by various countries for benchmarking and generating assurance on implemented cybersecurity measures, we had considered 37 countries as benchmarking data was available for them. Survey and analysis of cybersecurity assurance & benchmarking exercises of these countries provided some interesting methods initiated for generating confidence in cybersecurity measures. We have identified the 7 significant categories of activities adopted for the benchmarking by countries. Further, key observations on cybersecurity

benchmarking practices adopted by countries have been presented.

It was observed in the study that there is a lack of a country-level overarching framework for cybersecurity assurance & benchmarking. It was also observed that activities are mostly limited in the scope of implementation across a nation, and also lack effective measurement indicators. In few cases where formal models are implemented, measurement is only at an abstract level; data from the grassroots level is not included in benchmarking efforts.

Nation-states are trending toward the wide applications of 5 G communication technology and variety of Cyber-Physical Systems such as the Internet of Things (IoT) in smart cities. Application of emerging technologies for the physical, social, institutional and economic infrastructure of a community would lead to increased attack surface via cyberspace. In such smart environments, cybersecurity assurance is vital for continuing safe and secure operations.

To generate sufficient confidence in the cybersecurity measures implemented and provide priority areas for aligning the resources there is a need to develop and implement a cybersecurity assurance framework at the country-level.

Through this study and analysis, we have listed activities adopted for benchmarking by various countries and have identified opportunities to improve country-level cybersecurity benchmarking efforts. The analysis also suggests some key properties such as the need for quantitative measurement of the cybersecurity preparedness at the country-level and inclusion of best practices & activities from other countries. Benchmarking activities to work in tandem and data to be gathered from the grass-roots level to generate confidence at the national level. The holistic architecture of Cyber-Physical System including hardware, software and humans needs to mapped for generating benchmarking indicators. These key properties may be considered during the development of a national-level cybersecurity assurance framework.

This study is the first step in tendering efforts to develop a cybersecurity assurance & benchmarking framework for India, which may be further extended and customized for other economies. The possibility of engaging government for the development and implementation of a nationwide cybersecurity assurance framework will be explored. Based on this study and analysis, the authors are looking forward to developing the cybersecurity assurance framework for India.

References

Asia Pacific Computer Emergency Response Team (APCERT). (2017). *APCERT media release*. Retrieved May 30, 2017, from. www.apcert.org: http://www.apcert.org/documents/

Australian Government. (2013). *Public governance, performance and accountability act 2013*. Australian Government.

Australian Government. (2020, March 16). Department of Home Affairs: https://cybersecuritystrategy.homeaffairs.gov.au/

Australian Government, ASIC, KPMG, Deloitte, EY, Pwc. (2017). *ASX 100 cyber health check report*. Austalian Government.

CERT Bulgaria. (2020, March 16). *Home page*. CERT Bulgaria. https://www.govcert.bg/EN/Pages/default.aspx

CERT-In. (2020, March 16). *CERT-In*. Indian Computer Emergency Response Team. https://www.cert-in.org.in/

Cybersecurity Malaysia. (2020, March 16). *Cybersecurity Malaysia*. https://www.cybersecurity.my/cybernews/2013/Q4/eng/nov.html

Data Exchange Agency. (2020, March 14). *Data exchange agency*. https://dea.gov.ge/?web=0&action=news_archive&p_num=8&lang=eng

Department of Information and Communications Technology, Republic of the Philippines. (2019). *National cybersecurity plan 2022*.

Duchon, B. K. (1988). Combining qualitative and quantitative methods in information systems research: A case study. *MIS Quarterly*, *12*(4), 571–586. https://doi.org/10.2307/249133

Economist Intelligence Unit and Booz Allen Hamilton. (2011) . *Cyber power index*. Booz Allen Hamilton.

Egypt CERT - Home. (2020, March 15). *Egypt CERT*. https://www.egcert.eg/

ENISA. (2011). *Hungary Country Report*. European Union Agency for Cybersecurity.

European Union Agency for Network and Information Security. (2015a) . *Critical information infrastructures protection approaches in EU*.

European Union Agency for Network and Information Security. (2015b) . *Report on national and international cyber security exercises*.

European Union Agency for Network and Information Security (ENISA). (2016, October 20). *Cyber Europe 2016. (ENISA)* Retrieved May 30, 2017, from. www.enisa.europa.eu: https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016

European Union Agency For Network And Information Security (ENISA). (2015) . *The 2015 report on national and international cyber security exercises - survey, analysis and recommendations*. ENISA.

Federal Chancellery of the Republic of Austria. (2014a). *Cyber security report*. Republic of Austria.

Federal Office for Information Security (BSI). (2018). *The state of IT security in Germany*. Federal Office for Information Security (BSI), Germany.

French Government. (2020, March 14). *The French internet resilience observatory*. French Government: The French Internet Resilience Observatory. https://www.ssi.gouv.fr/en/strategic-committee/the-french-internet-resilience-observatory/

Government Communications Security Bureau. (2020). *Annaul reports*. New Zealand Government: https://www.gcsb.govt.nz/publications/annual-reports/

Government of Estonia. (2016) . *Public information act*.

Government of Finalnd. (2013). *Finland´s cyber security strategy*. Government of Finalnd.

Government of Kenya. (2014). *National cybersecurity strategy*.

Government of the United Kingdom. (2018). *FTSE 350 cyber governance health check 2018*.

Hathaway, M. (2015). *CYBER READINESS INDEX 2.0*. Potomac Institute for Policy Studies.

ICS-CERT. (n.d.). *Home*. Retrieved April 24, 2017, from. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): https://ics-cert.us-cert.gov/

Indian Computer Emergency Response Team (CERT-In). (2015). *Annual report*. CERT-In.

International Telecommunication Union (ITU) and International Multilateral Partnership Against Cyber Threats (IMPACT). (2013). *ITU-IMPACT ALERT*. ITU.

ISO/IEC. (2012) . *ISO/IEC TR 15443-1:2012*. International Organization for Standardization.

ITU. (2013). *cyberwellness profile mauritania. In ITU, Cyberwellness Profile*. International Telecommunication Union.

ITU. (2014). *Cybersecurity in Burkina Faso: Situation and initiatives*.

ITU. (2015c). Cyberwellness profile of Singapore.

ITU. (2015d). Cyberwellness profile of Turkey.

ITU. (2020a, March 16). https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Oman-third-best-prepared-in-world-to-thwart-cyber-attacks.aspx

ITU. (2020b, March 16). *ITU ALERT (Applied Learning for Emergency Response Teams)*. ITU ALERT (Applied Learning for Emergency Response Teams). International Telecommunication Union: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBDRILL/ITU-ALERT-Cyber-drill.aspx

ITU. (n.d.). *National strategies repository*. Retrieved April 24, 2017, from. International Telecommunication Union: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

ITU, ABI Reserach. (2015) . *Global cybersecurity index & cyberwellness profiles*. ITU.

ITU. (2015a). *Cyberwellness profile - United Kingdom*.

ITU. (2015b) . *CyberWellness profile Austria*

ITU-Impact. (n.d.). Cyberwellness Profile of Rwanda. International Telecommunication Union.

Korea Internet & Security Agency. (2008). *national information security index*. Retrieved May 2, 2017, from. https://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/weon-national-information-security-index-brisbane-july-08.pdf

Korea Internet and Security Agency. (n.d.). *Korea internet and security agency*. Retrieved May 30, 2017, from. http://www.kisa.or.kr

Kozik, R., & Choraś, M. (2014). Machine learning techniques for cyber attacks detection. *In Image processing and communications challenges 5* (pp. 391–398). Heidelberg: Springer.

Ministry of Electronics and IT. (2000) . *Information technology act*. Goverment of India.

Ministry of Electronics and IT. (2013) . *National cyber security policy*. Goverment of India.

Ministry of Electronics and IT. (2017). *Annual Report 2016-2017*.

Mohamed Dafir Ech-cherif El Kettani, T. D. (2008). NCSec: A national cyber security referential for the development of a code of practice in national cyber security management. *ICEGOV '08 Proceedings of the 2nd international conference on Theory and practice of electronic governance 2*. Cairo, Egypt: ACM.

National Computer Board. (2020, March 16). *National computer board*. National Computer Board. Government of mauritius: http://www.ncb.mu/English/News/Pages/National-Cybersecurity-Drill.aspx

National Coordinator for Security and Counterterrorism (NCTV). (2019). *Cyber security assessment Netherlands*.

National Electronic Information Security Authority. (2019). *NEISA. (National Electronic Information Security Authority)* National electronic information security authority. Hungarian Government: Retrieved May 30, 2017, from. http://www.neih.gov.hu/en

National Institute of Standards and Technology (NIST). (2011a) . *Information security continuous monitoring (ISCM) for federal information systems and organizations*. National Institute of Standards and Technology (NIST).

National Cyber Security Index, Republic of Korea. (2020, March 16) *National cyber security index*. National Cyber Security Index. Republic of Korea: https://ncsi.ega.ee/country/kr/

National Institute of Standards and Technology (NIST). (2020, March 16). *National checklist program repository*. National Vulnerablity Database. https://nvd.nist.gov/ncp/repository

NATO Cooperative Cyber Defence Center of Excellence (CCDCOE). (2015). *National cyber security organisation: Hungary*.

Potomac Institute for Policy Studies. (2019) . *Slovak republic - cyber readiness at a glance*.

Republic of Estonia. (2020, March 15). *Republic of Estonia - information system authority (RIA)*. Information System Authority (RIA). https://www.ria.ee/en/cyber-security/supervision.html

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012a). An overview of the development indonesia national cyber

security. *International Journal of Information Technology & Computer Science (IJITCS)*, *6*(November/December), 108. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.3095&rep=rep1&type=pdf

Shannak, R. O., & Aldhmour, F. M. (2009). Grounded theory as a methodology for theory generation in information systems research. *European Journal of Economics, Finance and Administrative Sciences*, (15), 32–50. http://www.eurojournals.com/EJEFAS.htm

Shojafar, M., Taheri, R., Pooranian, Z., Javidan, R., Miri, A., & Jararweh, Y. (2019). Automatic clustering of attacks in intrusion detection systems. *16th ACS/IEEE international conference on computer systems and applications*. Abu Dhabi, United Arab Emirates, United Arab Emirates: ACS/IEEE.

Taheri, R., Ghahramani, M., Javidan, R., Shojafar, M., Pooranian, Z., & Conti, M. (2020). Similarity-based Android malware detection using Hamming distance of static binary features. *Future Generation Computer Systems*, *105*, 230–247. https://doi.org/10.1016/j.future.2019.11.034

Telecommunication Unit, Government of barbados. (2017). *How can Barbados shape the future of internet*.

The National Cyber Security Centre (NCSC). (2016) . *Cyber security assessment Netherlands (CSAN)*. Ministry of Security and Justice, Government of Netherland.

Times of Oman. (2015, July 26). *Oman third best prepared in world to thwart cyber attacks*. Times of Oman Retrieved May 30, 2017, from. http://timesofoman.com/: http://timesofoman.com/article/64332/Oman/Education/Oman-was-cited-as-a-country-with-some-of-the-best-organisational-practices-thanks-to-its-High-Level-Cyber-Security-Strategy-and-Master-Plan

U.S. Department of Homeland Security. (2016, October 4). *Cyber storm: Securing cyber space*. (U.S. Department of Homeland Security) Retrieved May 30, 2017, from. www.dhs.gov: https://www.dhs.gov/cyber-storm

United Nations. (2013) . *The Cyber index - international security trends and realities*.

United Nations Institute for Disarmament Research. (2020, March 16). *Cyber policy portal*. Cyber Policy Portal. https://cyberpolicyportal.org/en/states/israel

United States Agency for International Development. (2016). *E-Readiness study in Georgia -Nationwide survey*.

US Department Homeland Security. (2020, March 16). *CYBER STORM: Securing cyber space*. CYBER STORM: Securing Cyber Space. https://www.cisa.gov/cyber-storm-securing-cyber-space

Voeller, J. G. (2010). Handbook of science and technology for Homeland Security. In *Handbook of science and technology for homeland security* edited by John G. Voeller, (pp. 850). Wiley.

White, G. B. (2011). The community cyber security maturity model. *2011 IEEE international conference on technologies for homeland security (HST)*. Waltham, MA, USA.

Appendix

Table A1. Country-wise summary of the national level cyber security posture benchmarking.

S. No.	Country	Types of Activities for Cyber Security Posture Benchmarking	Specific Methods and Tools used for conducting Benchmarking	Frequency of Benchmarking Activities	Benchmarking conducted by (Type & Name of Agency):	Output Format of Benchmarking Activities
	Australia	a. ICT Benchmarking introduced under Public Governance, Performance and Accountability Act 2013 (Australian Government, 2013) b. Cybersecurity Strategy mentions cyber security 'health checks' for ASX100 listed businesses (Australian Government, 2020)	a. Statistical data for benchmarking the ICT Expenditure, Personnel and Infrastructure b. The 'health check' assessment process to be conducted by an online questionnaire and interviews	a. Annual b. The first report was released in March 2017	a. Government (Department of Finance) b. Assessment by 4 audit firms	a. Trend Report b. Public report and one-to-one report to participants
	Austria	A consolidated report of cybersecurity development in Austria (Federal Chancellery of the Republic of Austria, 2014a)	Includes analysis of Threats to country, The National review of developments in cybersecurity, Participation in cyber exercises, Study of International development in Cybersecurity	Annual	Government (Federal Chancellery of the Republic of Austria)	Cyber Security Report
	Barbados	Analysis of data on cyber attacks (Telecommunication Unit, Government of barbados, 2017)	Cyber-attack data is used for understanding threat landscape, frequency and mitigation techniques implemented at the national level	-	Telecommunication unit, Government of Barbados	Report
	Brazil	IT audit exercises to measure IT management including cybersecurity developments in Government Organizations (ITU, ABI Reserach., 2015)	Compliance based audit of Government departments	-	The Bureau of Information Technology Audit (Sefti/TCU)	Organization specific audit report along with recommendations for improvement
	Bulgaria	Cybersecurity exercises	National cyber exercises and regional cyber exercises to measure the cybersecurity preparedness	-	CERT Bulgaria (National CERT) participated in regional exercises (CERT Bulgaria, 2020) (European Union Agency For Network And Information Security (ENISA), 2015)	Report on Cyber Exercise
	Burkina Faso	A study was done by ITU (ITU, 2014)	Assessment of situation and initiatives	-	ITU	Report restricted for circulation
	Denmark	Cybersecurity related developments in the country (Denmark)	Reactive Actions, Proactive efforts, events and legislation related to cybersecurity developments in a year	Annual	Center for cyber Security Denmark	Report on cybersecurity-related developments in country
	Egypt	Cybersecurity Exercises	Participation in Asia Pacific Computer Emergency Response Team (APCERT) Drills, Organization of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) Drills, ITU IMPACT Exercise, Arab Regional Cyber Drills	-	Egypt CERT (EG-CERT) (Egypt CERT – Home, 2020)	Exercise learning, improvement in incident analysis, response and coordination

(*Continued*)

Table A1. (Continued).

S. No.	Country	Types of Activities for Cyber Security Posture Benchmarking	Specific Methods and Tools used for conducting Benchmarking	Frequency of Benchmarking Activities	Benchmarking conducted by (Type & Name of Agency):	Output Format of Benchmarking Activities
	Estonia	Supervision of entities: Inspection of the security of the information systems of state and local government agencies and providers of vital services	Enabled by Legislations – Acts (Public Information Act and Emergency Act)	-	Republic of Estonia – Information System Authority (RIA) (Republic of Estonia, 2020)	Annual report of RIA cybersecurity branch
	Finland	National Cyber Security Strategy and implementation Plan put emphasis on the need for benchmarking of the cybersecurity preparedness (Government of Finalnd, 2013)	Use of cybersecurity capability maturity model for benchmarking and Sector-specific cybersecurity exercises and self-assessment tool	Annual	Secretariat of the Security Committee, Ministry of Defense	Reports for the Government on the state of cyber security preparedness
	France	Study of the resilience of internet w.r.t to actors operating within the boundary of France (French Government, 2020)	Study and analysis of the internet protocols from France perspective such as BGP, DNS	-	French Internet Resilience Observatory, ANSSI	Report
	Gabon	National or sector-specific benchmarking exercises (European Union Agency For Network And Information Security (ENISA), 2015)	-	-	-	-
	Georgia	a. E-readiness study: National wide survey (United States Agency for International Development, 2016) b. Cyber-Exe Georgia 2016 (Data Exchange Agency, 2020)	a. Survey b. Simulated Cybersecurity exercise for the representatives of Public and Private Organizations Red and Blue Team-based exercises scenarios	-	a. United States Agency for International Development and Data Exchange Agency, Georgia b. Data Exchange Agency and its subsidiary unit CERTGOVGE (Computer Emergency Response Team – Georgia's National CERT)	a. Survey Report on population response related to data security
	Germany	The Current state of IT security in Germany- Study Report by the Federal Office for Information Security in Germany (BSI) (Federal Office for Information Security (BSI), 2018)	Study of the threat landscape, assessment of threats & conclusions with respect to Germany also includes action taken for cybersecurity in state, business and society	Annual	Federal Office for Information Security in Germany (BSI)	Report
	Guatemala	Benchmarking exercise for major sectors	-	Conducted in 2014	CSIRT-GT with Support from the Organization of American States (OAS)	-

(*Continued*)

Table A1. (Continued).

S. No.	Country	Types of Activities for Cyber Security Posture Benchmarking	Specific Methods and Tools used for conducting Benchmarking	Frequency of Benchmarking Activities	Benchmarking conducted by (Type & Name of Agency):	Output Format of Benchmarking Activities
	Hungary	a. The Hungarian information security law created Assessment and Supervision Agency (NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), 2015) b. The country report is prepared by ENISA (ENISA, 2011) c. Vulnerability assessment and cybersecurity exercises are identified as activities	a. NEISA dedicated with the goal to handle and control the data of central and local government agencies regarding their cybersecurity policies and compliance against declared security posture b. Governance structure, trends, good practices inspiring cases and statistics Report is prepared based on publicly available, comments received from National Liaison Officers and ENISA experts	a. Last conducted in 2011	a. National Electronic Information Security Authority (NEISA), National Cyber Security Center b. ENISA c. GovCERT-Hungary	a. Country Report
	India	a. Self-assessment by organizations (Indian Computer Emergency Response Team (CERT-In), 2015) b. National and sector-specific cyber security exercises (CERT-In, 2020) c. Incident Trends (CERT-In, 2020)	a. Cybersecurity posture is self-evaluated by entities as per checklist b. Simulated attack-based and hypothetical scenario based exercises are conducted c. Based on the incident reported to the national CERT	a. Annual b. Annual c. Annual	a. Self-assessment by entity b. National CERT (CERT-In) c. National CERT (CERT-In)	a. Report on Cyber security posture of organizations b. Performance and gap report c. Annual Threat/Incident report
	Indonesia	Information Security Index-KAMI Index (Setiadi, Sucahyo, & Hasibuan, An Overview of the Development Indonesia National Cyber Security, 2012)	Measures Information security as per SNI ISO 27001 within government agencies in five domains, (1) Governance, (2) Risk Management, (3) Management Framework, (4) Asset Management, (5) Technology & Information Technology The maturity level is developed based on the Capability Maturity Model Integration (CMMI)	Annual	Directorate of Information Security, Ministry of Communication and Information Technology (MCIT)	The KAMI index report act as an indicator of the maturity of information security of entity. Consolidated report leads to security indicator at the national level.
	Israel	Cyber situation assessment of the country (United Nations Institute for Disarmament Research, 2020)	Government resolution identified one of the activity of the National Cyber Bureau (NCB) as "To assemble the national situation status regarding cybersecurity from all relevant parties"	-	National Cyber Bureau, Advisory body for the government in cyber field.	-

(*Continued*)

Table A1. (Continued).

S. No.	Country	Types of Activities for Cyber Security Posture Benchmarking	Specific Methods and Tools used for conducting Benchmarking	Frequency of Benchmarking Activities	Benchmarking conducted by (Type & Name of Agency):	Output Format of Benchmarking Activities
	Kenya	Cybersecurity Governance Maturity Analysis (Government of Kenya, 2014)	National cybersecurity strategy includes cybersecurity Governance Maturity Analysis, Legal/Regulatory Maturity Analysis, Capacity Building Maturity Analysis, Harmonization Maturity Analysis, Financial Maturity Analysis	-	Ministry of Information, Communications and Technology, Government of Kenya	Part of the National Cyber Security Strategy
	Malaysia	X-Maya: Benchmarking exercise for critical sector organizations (Cybersecurity Malaysia, 2020)	Benchmarking of national policy and procedures on national cyber crisis management by cybersecurity exercises for critical sector organizations	Annual	CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI)	Evaluation report of the exercise
	Mauritania	Security audit of infrastructure (ITU, 2013)	-	Annual	-	-
	Mauritius	a. Cybersecurity drills to be conducted as per the national cybersecurity strategy (National Computer Board, 2020) b. Survey of Information Security State in business was conducted	a. National and organization level exercise to evaluate the security posture and level of preparedness in resisting and dealing with cybersecurity incidents	a. Last exercise (ITU ALERT Cybersecurity Drill) conducted jointly with ITU in 2016	a. National CERT (CERT-MU)	-
	Morocco	Initiated project for classification, identification of the national information systems and measuring the maturity of these systems (ITU, ABI Reserach., 2015)	-	-	-	-
	Netherlands	CSAN- Cybersecurity Assessment Netherlands (National Coordinator for Security and Counterterrorism (NCTV), 2019)	Provide insight to threat actors, threat tools, vulnerabilities, resilience, and developments in the field of cybersecurity Provide statistics of Incident handled, vulnerabilities (responsible discloser) and sectoral assessment of cybersecurity in terms of manifestation, threat actors and threat tools	Annual	National Cyber Security Center, National Coordinator for Security and Counterterrorism	Annual assessment statistics related to cybersecurity
	New Zealand	Annual report of GCSB (Government Communications Security Bureau, 2020)	Annual report provide development related to the cybersecurity, operation summary related to cybersecurity and related developments	Annual	Government Communications Security Bureau (GCSB)	The sanitized unclassified version of the report is released in public domain and classified version is submitted to the Government

(*Continued*)

Table A1. (Continued).

S. No.	Country	Types of Activities for Cyber Security Posture Benchmarking	Specific Methods and Tools used for conducting Benchmarking	Frequency of Benchmarking Activities	Benchmarking conducted by (Type & Name of Agency):	Output Format of Benchmarking Activities
	Oman	a. Benchmarking exercise under the Global Information Security Survey (GISS) (ITU, 2020a) b. Participation in Regional Cyber Security Exercises (ALERT) (ITU, 2020b) c. National level Survey and cyber security audit & compliance against policies and frameworks are conducted	a. Survey based on responses of CIOs, CISOs and executives on 3 steps for resilience (i)Sense, (ii) Resist and (iii)React	-	a. Ernst & Young (E & Y) b. ALERT by ITU c. National CERT (OCERT)	a. Survey Report and statistics b. Post exercise report
	Philippines	National Assessment-National cybersecurity policy emphasizes on Policy monitoring, assessment of vulnerabilities of cyberspace and risk assessment of the organizations (Dpartment of Information and Communications Technology, Republic of the Philippines, 2019)	2 components identified under the National Assessment: (A) National Cyber Geography ● Inventory of digital infrastructure ● Cyber Geography to define national cyber space ● Risk Assessment ● National Threat assessment ● Vulnerability assessment ● Impact assessment	-	Task Force for the Security of Critical Infrastructure (TFSCI), CySWG, Risk and Vulnerability Assessment Committee (R/VAC), Formulation and Implementation of Cybersecurity Policies Committee (FISPOL) and other committees/ originations dealing with cyber security issues at national level	-
	Romania	Cyber Europe: Participation in the regional cybersecurity exercises conducted by ENISA (European Union Agency For Network And Information Security (ENISA), 2015)	Exercise includes Technical challenges and coordination in at different levels: local, organization, national, European	Biennial	Participation by National Computer Security Incident Response Team (CERT-RO)	Ranks of participants and learning from exercises
	Rwanda	a. Participation in cyber drills such as ITU-IMPACT [ITU-Impact, n. d.] b. Cybersecurity Plan (draft) also identified the need for policy implementation monitoring across government agencies and mandate an annual audit of service providers as per ISO 27001	-	-	a) and b) Rwanda Development Board (RDB)	a. Post drill report

(*Continued*)

Table A1. (Continued).

S. No.	Country	Types of Activities for Cyber Security Posture Benchmarking	Specific Methods and Tools used for conducting Benchmarking	Frequency of Benchmarking Activities	Benchmarking conducted by (Type & Name of Agency):	Output Format of Benchmarking Activities
	Singapore	a. Critical Infocomm Infrastructure Surety Assessment (CII-SA) (Voeller, 2010) b. The Infocomm Security Health Scorecard (ITU, 2015c)	a. National Cyber Security Masterplan 2018, Singapore aims to complete the Critical Infocomm Infrastructure Protection Assessment programme which will identify and assess the information communications systems that are critical to the operation of critical infrastructures b. Scorecard to assess the level of infocomm security preparedness of public sector agencies in areas such as policies, standards, security knowledge and physical & environment security	-	a) & b) Info-communications Media Development Authority of Singapore (IMDA) and the Government Technology Agency (GovTech)	-
	Slovakia	a. Participation in International cybersecurity exercise (Cyber Europe, Cyber Atlantic) b. Slovak Information Security Exercise (SISE) (Potomac Institute for Policy Studies, 2019)	a. SISE involves public institutions, as well as foreign CSIRT/CERT teams Exercises were focused on incident response capabilities	a. SISE conducted in 2011, 2012, 2013	a. Computer Security Incident Response Team Slovakia (CSIRTSK) in cooperation with the Ministry of Finance, Government of Slovakia	-
	South Korea	National Information Security Index: Quantitative measurement for assessing the information security level of an entity (e-Governance Academy, Estonia, 2020)	12 low-level indices statistical data leads to 3 component indices3 component indices merged into 1 index National Information Security Index	-	-	National Security Index
	Togo	2 Studies had been made on cybersecurity posture of the country	-	-	Togo Electronic Communication Regulator	-
	Turkey	a. National level cybersecurity exercises (ITU, 2015d) b. By-Law on Security of Electronic Communications mandate service providers to comply with ISO 27001. Audits for the assessment of cyber security development level of the electronic communications sector are conducted	a. Cyber exercises focus on improving the ability to respond to cyber-attacks, to improve organizational and interagency coordination against cyber-attacks and to increase the national awareness level of cyber security b. Service providers are obliged to prepare annual reports about security of electronic communications and ICTA has the power to audit the operators whether they meet the requirements of the By-Law or not	a. 3 national and 1 international cyber exercises were conducted since 2011	a. Information and communication technologies Authority (ICTA) b. ICTA	a. Participant-specific reports were prepared for each exercise participant

(*Continued*)

Table A1. (Continued).

S. No.	Country	Types of Activities for Cyber Security Posture Benchmarking	Specific Methods and Tools used for conducting Benchmarking	Frequency of Benchmarking Activities	Benchmarking conducted by (Type & Name of Agency):	Output Format of Benchmarking Activities
	United Kingdom	a. Cyber Governance Health Check ("the Tracker") (Government of the United Kingdom, 2018) b. Office of Cyber Security & Information Assurance (OCSIA) is also responsible for the benchmarking in the area of cybersecurity (ITU, 2015a)	a. Focused on FTSE 350 companies, it assesses the extent to which boards and audit committees understand and oversee risk management measures that address cyber security threats to their business The Tracker is a non-technical governance questionnaire comprised of 37 questions	a. Annual	a. Department for Business, Energy and Industrial Strategy (BEIS), UK Government)	a. Aggregated report and participants benchmarking report
	United States of America	(1) Cyber Posture Scorecard (2) -Federal Information Security Continuous Monitoring (ISCM) Evaluation (National Institute of Standards and Technology (NIST), 2011a) (3) National Cyber Security Exercise (Cyber Strom) (US Department Homeland Security, 2020) (1) National Checklist Program(NCP) (National Institute of Standards and Technology (NIST), 2020)	(1) Based on NIST standards/best practices assess the state of operational readiness and cybersecurity risk across Federal Civilian Executive Branch departments and agencies (2) Examine capability to prepare for, protect from, and respond to cyberattacks potential effects, Validate coordination & Communication among organizations (3) Based on NIST SP 800–70 Rev 2, NCP is the US government repository of publicly available security checklists that provides detailed guidance on setting the security configuration of operating systems and applications	(1) Biennial	(1) Cybersecurity Assurance Branch (CAB), Federal Network Resilience, Department of Homeland Security (DHS) (2) Department of Homeland Security (DHS) (3) National Institute of Standards and Technology (NIST), US Department of Commerce	(1) Health posture of organization, wellness plan and report of assessments (2) Post-exercise Report (3) Evaluation against checklist