INDEX

OF CYBERSECURITY INDICES

2017

1 Table of contents

2 INDEX OF CYBERSECURITY INDICES 2017

The increase of recent incidents and breaches of cybersecurity demonstrates the challenge all users of the Internet (governments, organizations and citizens alike) face to keep up with the speed of ICT evolution. To embrace this technology progress, cybersecurity must form an integral and indivisible part of the process. Therefore, various factors must be taken into consideration, as the application of cybersecurity is a continuous process that needs to match ongoing cybercriminal activities and threat campaigns.

As such, in 2015 and in collaboration with ABI Research, ITU compiled and published some of the outstanding cybersecurity indices. As cybersecurity issues continue to compound with time, new indices regarding cybersecurity challenges need to be established. This year, ITU has identified new indices and updated the previous Index of Cybersecurity Indices of 2015. The index of indices presented below is not an exhaustive list. It is a presentation of existing surveys, indices and publications from private and public organizations. These indexes can be broadly split into three major groups: indices for assessing countries' national postures, indices for assessing organizations, and indices for assessing threats. The three groups are presented below alongside current relevant indices.

2.1 DEFINITIONS

The table below proposes a snapshot of the content and the methods used by the various indexes examined. This content is briefly detailed in the following pages. A short explanation of each indicator's meaning is presented at the end of this section.

Scores: The score is based on an individual result using the total score of all indicators. This type of scale allows participants to have a view on their individual status regarding the different capabilities measured. The indices examined use different rating methods - percentages, ratios etc.

Ranking: Each participant is ranked compared to the others. The ranking scale allows participants to be aware of their level in relation to the other participants.

Information Society Development: Is a society where the creation, distribution, use, integration and manipulation of information is a significant economic, political, and cultural activity. The people who have the means to partake in this form of society are sometimes called digital citizens.

Cyber Maturity: An assessment providing an in-depth review of an organization's ability to protect its information as well as its efforts and readiness against cyber threats.

Cyber Threats: The potential of a malicious attempt to damage or disrupt a computer network or system with unauthorized access to a control system device using a data communications pathway. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.

Cyber Vulnerabilities: Is a weakness which reduces a system's security assurance. Vulnerability is a system susceptibility or flaw that is accessible to an attacker or not otherwise mitigated by a countermeasure.

Organizational: The measurement of policy coordination institutions and strategies for cybersecurity development within countries and companies in order to secure the organization's smooth running and longevity while reducing cyber-attacks.

Technical: The measurement of technical institutions, terms, or frameworks dealing with cybersecurity. In this aspect, some indices check the commitment of countries/organizations on their available technical measures while others provide a technical guide on software to enhance security.

Economical: This notion represents the presence of an economic impact, cost or management measurement in the index while others present it as a business alignment and investment efficiency of an organization in accordance to cybersecurity.

Legal Framework: The measurement of legal institutions and frameworks dealing with cybersecurity and cybercrime. It also involves rules, legal trainings, standardizations and regulations related to cybersecurity.

Cooperation: The existence of partnerships, cooperative frameworks and information sharing networks between countries and organizations.

Capacity Building: The existence of research and development, good practices, education and training programmes; intended to enforce better understanding, approach and awareness towards cybersecurity.

Recommendations: A recommendation is a proposal or list of suggestions normally provided by competent bodies or authorities. An index may provide recommendations on what measures or steps ought to be taken to better the cybersecurity of the countries/organizations studied.

Profiles: The index presents a short description of the activities undertaken by the different organizations and countries examined.

Website: The survey has an official Website where the majority of the information regarding the index can be found.

PDF: The survey proposes a Portable Document Format (PDF) with survey's detailed report and outputs.

Visualization: The representation of information through graphical references, images, scorecards, interactive images, heat maps, videos or others.

	Metrics			Content										Presentation Format				
	Score	Ranking	Information Society Development Score (ISD) score)	Cyber Maturity	Cyber Threats	Cyber Vulnerabilities	Organizational	Technical	Economical	Legal Framework	Cooperation	Capacity Buiding	Recommandations	Profiles	Website	PDF	Visualization	No. of Iterations
Cyber Maturity in the Asia-Pacific Region	x			x					x	x	x			x	x	x		2
National Cyber Security Index	x	x	x	x	x		x	x		x	x	x			x	x	x	1
Global Cybersecurity Index	x	x					x	x		x	x	x		x	x	x	x	2
Kaspersky Cybersecurity Index	x				x				x					x	x	x	x	1
Asia-Pacific Cybersecurity Dashboard		x		x			x			x	x	x		x	x	x		2
Cyber Readiness Index 2.0	x	x		x		x	x		x	x	x			x	x	x		2
Cybersecurity Poverty Index	x			x			x	x							x		x	1
CyberGreen Index	x	x			x			x							x		x	1
The Accenture Security Index	x	x			x		x	x	x		x		x		x	x	x	1
Global Cybersecurity Assurance Report Cards	x				x	x		x							x		x	1
Index of Cybersecurity					x			x							x	x	x	73
Cybersecurity Capability Maturity Model				x			x	x		x	x	x			x	x		2
Cyber Power Index	x	x		x			x	x		x		x			x	x	x	1
IBM X-force Threat Intelligence Index					x			x							x			3

3 INDICES FOR ASSESSING COUNTRIES

Indices for assessing countries have been developed by international organizations and think tanks, often in partnership with private sector organizations. At the highest level, these indices look at, among others, policy and regulatory aspects, organizational measures, national strategies, and cooperative efforts. Some indices simply compare and contrast measures amongst countries, while others provide an index scoring based on indicators. Others provide rankings based on the scoring. All offer valuable information on cybersecurity practices and gaps at the nation state level.

3.1 Cyber Maturity in the Asia-Pacific Region[1]

Number of countries:

23

Research Method:

Secondary data

Rank or Score:

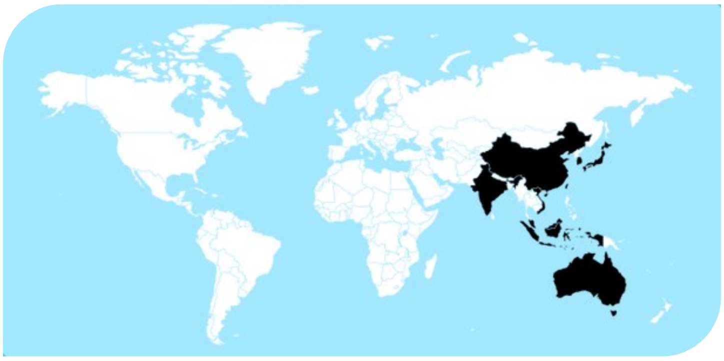
Scores

Indicators:

11

Developer:

The Australian Strategic Policy Institute



This index, developed by the Australian Strategic Policy Institute, is the third edition of an annual report providing information on Asia and the Pacific nation state's levels of cyber maturity.

A total of 23 countries in the Asia and the Pacific region have been analyzed; with the US being used as the reference point for overall cyber maturity. The index is focused on government policies and legislative structures of cybersecurity. The methodology uses a cyber maturity metric to assess the various facets of nations' cyber capabilities. A set of 11 indicators has been produced and each state's level of cyber maturity has been measured against the benchmark provided with each indicator. The scores are based on data provided by the International Telecommunication Union (ITU). The publication includes an overall ranking of cyber maturity for each state within the region, as well as an individual score and short profile. A color reference base allows for quick assessment. The publication is classified as an index since it has indicators, scoring and ranking mechanisms. The color-coded reference base is a neat addition. The individual country profiles are helpful and provide a snapshot of national activities. The focus is primarily on organizational structures, legislation, international cooperation, CERTs and military capabilities. However, it is only a regional index based

[1] https://www.aspi.org.au/publications/cyber-maturity-2016

on open source and publicly available information, and could benefit from a survey based data collection exercise

3.2 National Cyber Security Index[2]

Number of countries:

25

Research Method:

Primary & Secondary

Rank or Score:

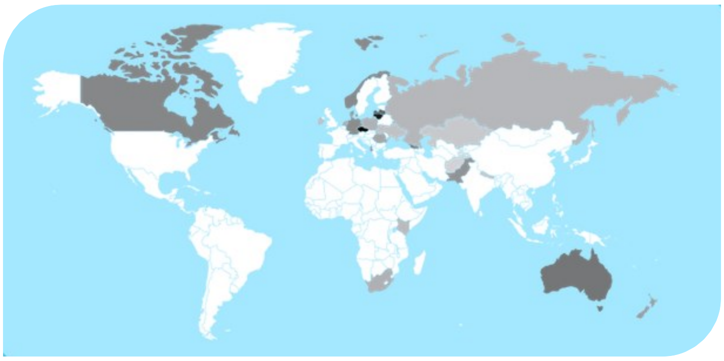
Rank & Score

Indicators:

12

Developer:

Estonian e-Governance Academy & Estonian Foreign Ministry



This is the first version of an index developed by the Estonian e-Governance Academy in cooperation with the Estonian Foreign Ministry. The index is focused on the public aspects of national cybersecurity, which are implemented by the central government. The aim of the index is to measure the cybersecurity level of countries, especially their preparedness to prevent cyber threats and their readiness to manage cyber incidents, crime and crises on a large scale.

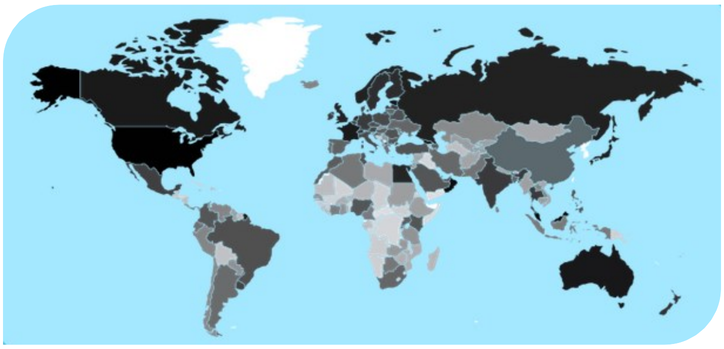
A total of 25 countries have been analyzed with data collected using both primary and secondary research. The index has 12 main indicators, which are divided into four groups: General Cyber Security Indicators, Baseline Cyber Security Indicators, Incident and Crisis Management Indicators and International Incident Indicators. These 12 indicators have sub-indicators and aspects that can be measured in points (0 to 100). The indicators have been tied to cybersecurity and information society as e-identity, digital signature and the existence of a secure environment for e-services. The index has a score and ranking mechanism.

The advantage of this index is that it has an online global database and it shows what countries can do to improve their cybersecurity. It also gives an overview of the preparedness of countries to prevent cyberattacks and crimes as well as how to manage them. The goal is to have a global reach by the end of 2017.

[2] http://ncsi.ega.ee/methodology-description

3.3 GLOBAL CYBERSECURITY INDEX[3]

Number of countries:
194
Research Method:
Primary and Secondary
Rank or Score:
Rank and score
Indicators:
25
Developer:
International Telecommunication Union



An index developed by the International Telecommunication Union (ITU), which aims to provide insight into the cybersecurity engagement of sovereign nation states. Rooted in the ITU's Global Cybersecurity Agenda (GCA), the GCI looks at the level of commitment in five areas: legal measures, technical measures, organizational measures, capacity building, and cooperation. The result is a country-level index and global ranking of cybersecurity commitment. A total of 194 countries have been analyzed, 135 of which have been subjected to both primary and secondary research and only 59 a subject of secondary research. The publication includes an overall ranking, as well as six regional rankings and an individual score for each country. The 2017 publication is the second report produced and there will continue to be further updated iterations.

The publication is classified as an index since it has indicators, scoring and a ranking mechanism. The main advantage of this publication is its global character (the only publication with such a broad geographical range). It is based on both a survey among ITU Member States and open sourced material. It is also worth noting the publication focuses on five broad cybersecurity application areas, which include 25 indicators and is further refined with additional sub-indicators.

[3] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

3.4 Kaspersky Cybersecurity Index[4]

Number of countries:

21

Research Method:

Primary

Rank or Score:

Score

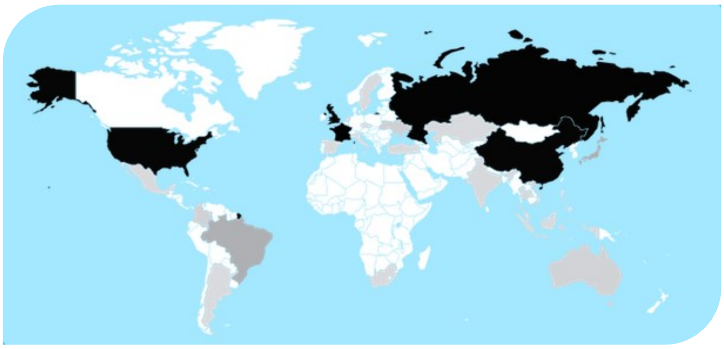
Indicators:

3

Developer:

Kaspersky Lab &

B2B International



An index developed by Kaspersky Lab in cooperation with B2B International. Its focus is to evaluate, through a multi-dimensional concept, the level of risk internet users are exposed to on a daily basis in cyber space. The Kaspersky Cybersecurity Index is a survey that occurs twice a year. 21 countries across the globe have been analyzed and a total of 17,377 respondents participated in the survey in the second half of 2016.

The sample includes thousands of adult Internet users around the world classified by age and gender. The index has three key indicators, namely: "Unconcerned" (the proportion of people not believing that they could be a target for cybercrime), "Unprotected" (the number of users who fail to protect themselves from cyber threats with the help of antivirus or Internet security software across all their desktops, laptops and mobile devices) and the "Affected" (the people who have experienced different cybersecurity incidents during the previous months). These indicators provide information needed to monitor the degree of risk to the average internet user. The selected countries are scored by percentage in each of the categories.

To evaluate the online environment for internet users, some additional statistics are presented in a variety of graphs such as users' online behavior, their concerns, what issues they face and how they defend themselves against possible threats.

[4] https://www.kaspersky.no/about/press-releases/2016_21-29-60-kaspersky-lab-presents-the-first-cybersecurity-index

3.5 Asia-Pacific Cybersecurity Dashboard[5]

Number of countries:

10

Research Method:

Secondary

Rank or Score:

None

Indicators:

31

Developer:

BSA, Software Alliance

The Dashboard is a publication developed by BSA | The Software Alliance. The publication is focused on policy and organizational aspects of cybersecurity, with strong reference to legal foundations as well as cooperation between public and private sector. The aim of this cybersecurity dashboard is to provide a reference base which allows the evolution of countries' cybersecurity policies by comparing them with the other Asia and the Pacific countries.

This publication was developed based on publicly available information with no targeted interviews conducted and covers ten countries from the Asia and the Pacific region.

The methodology of the publication is based on 31 indicators including: legal foundations, operational entities, public private partnerships, sector-specific cybersecurity plans, education and additional cyber law indicators. Each indicator is given one of four statuses: Yes, No, Partial and N/A. The publication does not offer scoring or ranking mechanisms.

What is interesting about this publication is a graphical reference base, which allows for a quick evaluation of countries' cybersecurity stance. The individual country profiles are helpful and provide a snapshot of national activities. The focus is primarily on policy, legal and organizational aspects of cybersecurity with strong reference to public private partnerships. However, it is limited in geographic range to Asia and the Pacific and could strongly benefit from a survey based data collection exercise.

[5] http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study_apac_cybersecurity_en.pdf

3.6 Cyber Readiness Index 2.0 (CRI 2.0)[6]

Number of countries:

125

Research Method:

Primary & secondary

Rank or Score:

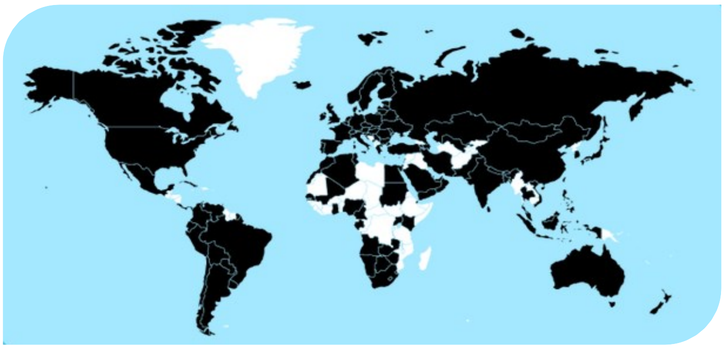
Score

Indicators:

7

Developer:

Potomac Institute for Policy Studies



The CRI 2.0 is developed by the Potomac Institute for Policy Studies. The publication evaluates nation state's cyber maturity as well as their overall commitment to cyber issues. The aim of the publication is also to define the meaning of being "cyber ready" while proposing actionable blueprints to follow. The publication is mainly focused on policy and economic aspects of cybersecurity and includes fact-based assessments of countries' cyber readiness. 125 countries were studied. Individual country profiles are being prepared, based on the CRI 2.0 results.

The index uses a set of seven indicators. The publication is expected to be updated periodically. CRI 2.0 has a broad geographic range and touches upon similar pillars as those enshrined by the ITU's Global Cybersecurity Agenda (GCA). Each country has a scoring, and the addition of military capabilities goes beyond that covered by the ITU GCI. However, it does not offer any ranking despite its scoring mechanism.

[6] http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

3.7 Cyber Power Index[7]

Number of countries:

19

Research Method:

Secondary

Rank or Score:

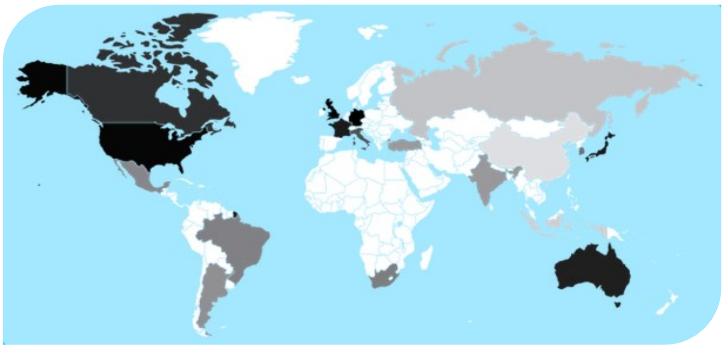
Rank and Score

Indicators:

39

Developer:

The Economist's Intelligence Unit & Booz Allen Hamilton



An Index developed jointly by the Economist's Intelligence Unit and sponsored by Booz Allen Hamilton focusing on policy, organizational and technical aspects of cybersecurity. The publication covers 19 countries of the G20. The aim of the publication is to provide a benchmark of cybersecurity to withstand and resist cyberattacks by measuring the understanding of the digital world and the development of the legal environment.

The methodology is based on 39 indicators and sub-indicators grouped into four categories: legal and regulatory framework, economic and social context, technology infrastructure and industry application. The Index includes a scoring and ranking mechanism and focuses primarily on the technical aspects and on industry application. The sub-indicators are weighted according to two different sets. The indicators and categories are modeled according to scores of 0 to 100, where zero represents the least cyber power and 100 the greatest. The overall score is the result of a normalized score averaged for each indicator. However, it is not a global index and the geographical range is limited to the G20.

[7] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

3.8 THE CYBERGREEN INDEX[8]

Number of countries:

245

Research Method:

Secondary

Rank or Score:

Rank and Score

Indicators:

6

Developer:

CyberGreen initiative

An index developed by CyberGreen Initiative supported by JPCertCC, CSASingapore and Foreign & Commonwealth Office. The CyberGreen Initiative is a global non-profit organization helping to improve the health of the global cyber Ecosystem. The project aims to gather and presents data on vulnerable systems on the Internet's infections.

CyberGreen Index is based on open source intelligence (secondary data) collection then put into the CIF framework and stored in an elastic search database. The metrics are defined by the number of infected and vulnerable systems within the six risks indicators.

The publication includes ranking and scoring mechanisms presented at a global level (245 countries) that can be read as an incremental snapshot. The second version is being elaborated, which takes into account different limitations observed in the first version.

[8] http://www.cybergreen.net/statistics/

4 INDICES FOR ASSESSING ORGANIZATIONS

4.1 THE ACCENTURE SECURITY INDEX[9]

Number of countries:

15

Research Method:

Primary

Rank or Score:

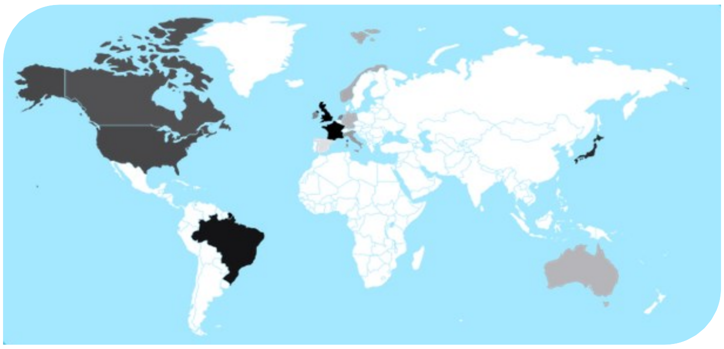
Score

Indicators:

33

Developer:

The Accenture



An index developed by Accenture, a leading global professional services company providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. The aim of the survey is to understand the extent to which companies prioritize security, how comprehensive security plans are, how resilient companies are with regard to security, and the level of spend for security. It surveyed 2,000 executives from 12 industries and 15 countries across North and South America, Europe and Asia and the Pacific.

The publication includes 33 cybersecurity capabilities classified into seven cybersecurity domains: business alignment, cyber response readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem. Each criteria is characterized by levels of competence: No/limited competence; Average competence; and High competence. The advantage of this index is the comparison resulting from a scoring and ranking mechanism of industries' and countries' cybersecurity capabilities.

[9] https://www.accenture.com/t20170213T002042__w__/us-en/_acnmedia/PDF-43/Accenture-The-Acn-Security-Index.pdf

4.2 CYBERSECURITY POVERTY INDEX[10]

An Index developed by RSA, a business-driven security solutions company which links security incidents with business context, to enable effective response and protection.

The RSA Cybersecurity Poverty Index is the result of an annual maturity self-assessment completed by 878 worldwide organizations and industries of all sizes across 24 countries. The self-assessment was supported by the NIST Cybersecurity Framework (CSF). It measures how organizations rate their overall cybersecurity maturity and practices related to five key functions (Identification, Protection, Detection, Response and Recovering). The self-assessment use a 5-point scale from 1 to 5, where 1 represents “no capability” and 5 the most mature practices. The significant increase of new participants and the increase in the percentage of organizations with mature cybersecurity programs reinforce the fact that cybersecurity is an urgent matter. Thus, the index serves as an excellent baseline to assess any organization's core cybersecurity and cyber risk management capabilities.

4.3 GLOBAL CYBERSECURITY ASSURANCE REPORT CARDS[11]

A publication developed by Tenable Network Security in partnership with Cyber Edge Group. The Global Cybersecurity Assurance report cards measures the attitudes and perception of 700 IT security practitioners employed by an organization with more than 1000 employees in 2017, including and comparing the findings of the 504 participants from the Risk Assessment Index of 2016. The 2017 sample comes from 19 industries across nine countries from three different regions. The Index consists of a 12-question web-based assigning the indices and grades by country and industry. A minimum of 25 responses was required to appear in the details of the report. Information contained in questionnaires with less than 25 responses was reported in the global and by countries data. This survey assesses how security professionals rate the ability to assess cybersecurity risks and threats and how they mitigate them in their enterprise.

“Security by The Numbers” is a collaborative online forum for simple, practical, real-world metrics, and enables its members to take part in discussion to help understand IT good practices compared to other peers.

The Security Measurement Index is based on ISO 27000 international standards and input from an advisory board of security professionals. It provides benchmarking tools for assessing organizations’ security practices, a global assessment of IT and a basis for developing security measurement best practices to help make cybersecurity more effective and efficient.

[10] http://www.prnewswire.com/news-releases/rsa-research-75-of-organizations-are-at-significant-risk-of-cyber-incidents-300284168.html
[11] https://www.tenable.com/lp/2017-global-cybersecurity-assurance-report-card/

4.4 Cybersecurity Capability Maturity Model[12]

A publication developed by the University of Oxford's Global Cyber Security Capacity Centre. This report, deployed in 2015, is a revised version of its 2014 prototype. The report is not intended to be a static exercise. Its aims are to increase the effectiveness of capacity-building regarding cybersecurity internationally, assist nations to improve their cybersecurity capacity and help promote an innovative and healthy cyberspace for all. The publication defines five capacity dimensions related to cybersecurity, namely: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training, and skills; legal and regulatory framework; and organizations, technologies, and standards. The publication identifies a set of 49 indicators depicting varying levels of cybersecurity capacity development. The publication is mainly focused on policy and organizational aspects of cybersecurity.

5 INDICES FOR ASSESSING OTHER ASPECTS

5.1 IBM X-Force Threat Intelligence Index 2017[13]

An index developed by IBM security services. The publication includes an overview of cybersecurity threats based on cyberattack event data gathered by the company. X-Force uses both data from monitored security clients and data derived from non-customer assets such as spam sensors and honeynets. The publication provides a broad overview of technical challenges, case studies, and best cybersecurity practices in five main industries namely: Financial services, Health care, Manufacturing, Retail and Information and Communication.

The index does not score organizations or countries, nor does it include any specific indicators or formula for the calculation of an index but gives ranking of industries. It also provides the overall number of security events, attacks and incidents in the given year, as well as distribution by industry, category of incidents and category of attacks. The publication is expected to be updated periodically.

5.2 Index of Cybersecurity[14]

This is an individual effort developed by Dan Geer and Mukul Pareek and is focused on the technical aspects of cybersecurity. Published in April 2011, the aggregate index value is updated on the public website monthly. However, detailed statistics and individual sub-indices are shared only with respondents in a separate report.

It is an opinion-based measure of perceived risk to information infrastructures from a wide range of cybersecurity threats. It assesses, communicates the perceived level of risk of security practitioners and provides some key best practices for practitioners to compare. The survey gathers the views of information security professionals on the most current and most interesting threats.

[12] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition
[13] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&
[14] http://cybersecurityindex.org/index.php/calculation

A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite. The report is based on six key dimensions including 25 questions on a scale of five multiple choice answers from “falling fast” to “rising fast”.

5.3 Cybersecurity Index[15]

An index developed by Dell SecureWorks. The aim of the publication is to notify customers about threats and malicious activities, which may require the implementation of protective measures. The index uses a 4-level scoring system of overall network cybersecurity status, which in a simple and readable manner informs customers about the current level of overall cybersecurity threat. The index is evaluated daily by Counter Threat Unit researchers and updated when necessary. The index is not numerical but simply color-coded based on the following four cybersecurity levels: Guarded, Elevated, High and Critical. The threats are determined by a panel of experts at the Dell SecureWorks Counter Threat Unit Research Team and are based on information such as the release of security updates by companies such as Microsoft and Adobe. The publication is focused on technical aspects of cybersecurity.

[15] https://www.secureworks.com/about/counter-threat-unit