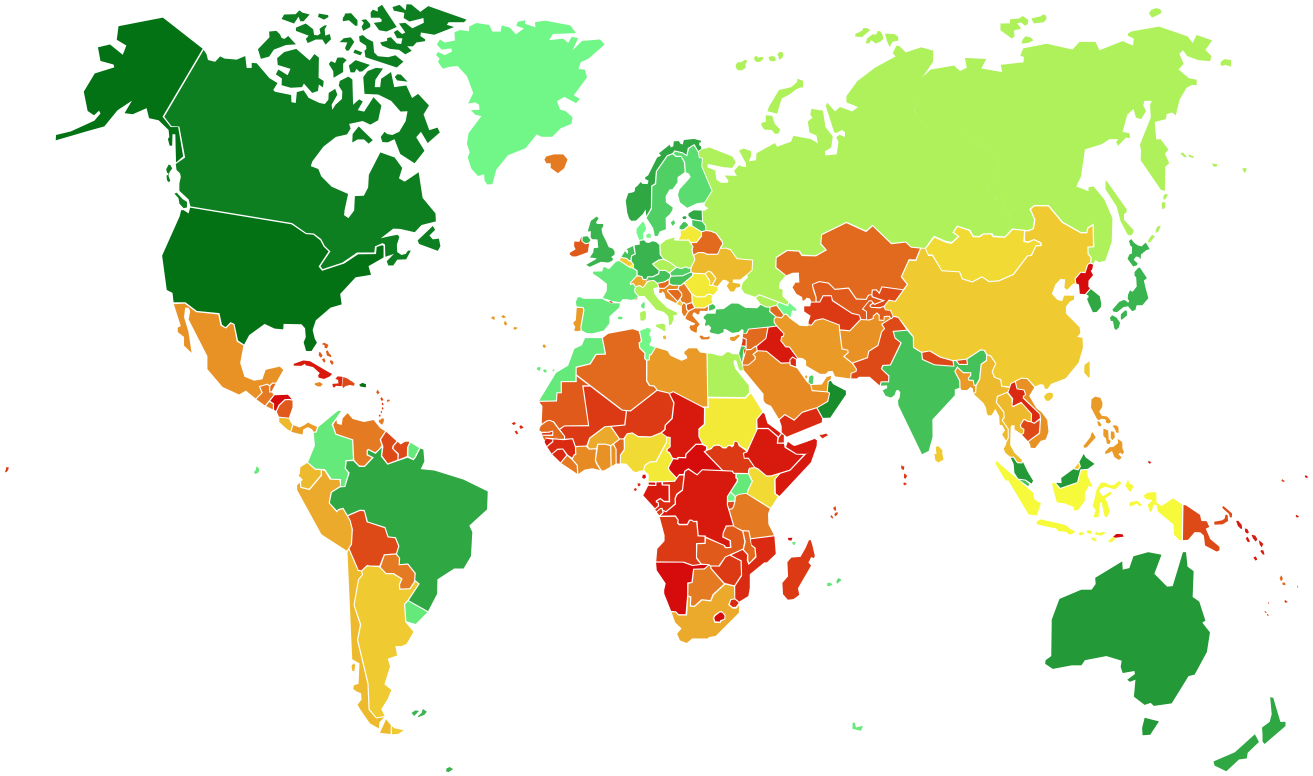
GLOBAL CYBERSECURITY INDEX



National Cybersecurity Commitment HIGHEST LOWEST

ABIresearch ITU Global Cybersecurity Index

Introduction

The Global Cybersecurity Index (GCI) is born of a cooperative partnership between the private sector and an international organization to drive the issue of cybersecurity to the forefront of national agendas. A joint project undertaken by ABI Research and the International Telecommunication Union (ITU), the GCI provides 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 readiness. The GCI does not seek to determine the efficacy or success of a particular measure, but simply the existence of national structures in place to implement and promote cybersecurity.

The project is a result of intensive primary and secondary research by both the ITU and ABI Research. Country-level surveys, complemented by in-depth qualitative research, were sent out to all ITU member states. Information was collected on laws, regulations, CERTs and CIRTs, policies, national strategies, standards, certifications, professional training, awareness raising, and cooperative partnerships.

The aim of the GCI is to provide a snapshot of where countries stand in their cybersecurity engagements at the national level. The vision, as seen by ABI Research and the ITU, is to promote cybersecurity awareness and the important role governments have to play in integrating appropriate mechanisms to both support and promote this crucial discipline. Safeguarding the integrity of cyberspace must involve the development of cybersecurity.

Conceptual Framework

Information and communication technologies (ICTs) are the driving force behind the evolution of modern societies. They underpin the social, economic, and political growth of individuals, organizations, and governments alike. ICTs have become not only ubiquitous, but essential for progress. Smart devices, M2M communications, and cloud-based services, among many other technologies, are advancing the next-generation of networked societies. Digital technology and internet connectivity are being systematically integrated into all verticals of the private and public sectors because they offer significant advantages: productivity, speed, cost reduction, and flexibility. As a result, ICTs are progressively being deployed in new platforms, such as retail RFID systems and vehicular telematics . More significantly, they are being used to upgrade critical infrastructures, including energy grids, transport networks, and healthcare systems.

Cybersecurity is paramount for sustaining a technologically sound model. The disruption of electricity or impairment of financial systems through interference with ICT networks is a reality; these events constitute national security threats. Malicious online agents are numerous, organized, and of diverse persuasions: political, criminal, terrorist, hacktivist. The tools at their disposal become more sophisticated and complex over time and with experience; the growing number of connected platforms only serves to offer new attack vectors . There is no going back to simpler times. In embracing technological progress, cybersecurity must form an integral and indivisible part of that process.

Unfortunately, cybersecurity is not yet at the core of many national and industrial technology strategies. Although cybersecurity efforts are numerous, they are eclectic and dispersed. Differences in internet penetration, technological development, private sector dynamics, and government strategies mean that cybersecurity is emerging as a bottom-up approach, a natural occurrence when disparities exist among nation states, public and private sectors, and industries. Yet a global culture of cybersecurity can be more successfully initiated from the top down. Information sharing and cooperation are key to tackling cross-border threats. Such elements require a certain measure of organization in a multitude of disciplines: legal, technical, educational. Though a particular country or sector may develop and adopt a highly effective cybersecurity framework, the knowledge will rarely be shared outside of that circle.

The primary obstacle is that cybersecurity is a sensitive issue, whether from a government or private sector perspective. Admission of vulnerabilities can be seen as a weakness. This is a barrier to the discussion and sharing of threat information and best practices. Yet security through obscurity is not a viable defense model

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

against modern cyber threats. The answer is to implement cybersecurity mechanisms at all layers of society. However, the drive and the incentive to do so are inadequate, either due to cost constraints or a simple lack of awareness. A first step toward remedying this situation lies in comparing the cybersecurity capabilities of nation states and publishing an effective ranking of their status. A ranking system reveals shortcomings and motivates states to intensify their efforts in cybersecurity. It is only through comparison that the real value of a nation's cybersecurity capability can truly be weighed.

The Global Cybersecurity Index (GCI) project aims to effectively measure each nation state's level of commitment to cybersecurity. The ultimate goal is to help foster a global culture of cybersecurity and its integration at the core of information and communication technologies. The project has been launched by the International Telecommunication Union (ITU) and private sector company ABI Research. The GCI project finds its basis in the current mandate of the ITU and the related projects and activities of the ITU's Telecommunication Development Bureau (BDT).

The ITU is the lead facilitator for the World Summit on the Information Society (WSIS) Action Line C5 on assisting stakeholders in building confidence and security in the use of ICTs at national, regional, and international levels. The ITU's mandate in cybersecurity is further supported by Resolution 69 on the "creation of national computer incident response teams (CIRTs), particularly for developing countries, and cooperation between them" adopted at the fifth World Telecommunication Development Conference (WTDC-10) and by Resolution 130 (Guadalajara, 2010) "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies." In this context , the Global Cybersecurity Agenda (GCA) was launched by the ITU's Secretary General, Dr Hamadoun Toure, as its framework for international multi-stakeholder cooperation toward a safer and more secure information society that focuses on the following five work areas:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- Cooperation

These five designated areas will form the basis of the indicators for the GCI. These five indicators are critical for measuring national capabilities in cybersecurity because they form the inherent building blocks of a national culture. Cybersecurity has a field of application that cuts across all industries and sectors both vertically and horizontally. Enabling the development of national capabilities therefore requires investment by political, economic, and social forces. This can be done by law enforcement and justice departments, educational institutions and ministries, private sector operators and developers of technology, public-private partnerships, and intra-state cooperation.

The long-term aim is to drive further efforts in the adoption and integration of cybersecurity on a global scale. A comparison of national cybersecurity strategies will reveal those states with high rankings in specific areas, and consequently expose lesser-known yet successful cybersecurity strategies. This can prompt increased information sharing on deploying cybersecurity for those states at different levels of development, as well. By measuring the level of cybersecurity preparedness in various areas, the index will allow states to assess where they are on a scale of development, where they need to make further improvements, and how far they are from implementing an acceptable level of cybersecurity. All states are moving toward a more digitized and connected environment, and adopting cybersecurity early on can enable the deployment of more secure and resilient infrastructure in the long term.

The GCI project will be a joint effort between the ITU's BDT (specifically the ICT Applications and Cybersecurity Division (CYB)) and ABI Research. The CYB will act as focal point and owner of the project, and ABI Research will bring in its core skill sets in strategy development, competitive intelligence, business planning, technology assessment, and industry benchmarking for the realization of the project. ABI Research is a market intelligence company specializing in global technology markets through the quantitative forecasting and analysis of key metrics and trends. Uniquely competent in providing forward-looking insights and actionable, timely, real-world data points in the technology sector, ABI Research will bring its expertise for the prompt development and production of a reliable index. Under this arrangement, the ITU and ABI Research aim to:

- Identify performance metrics
- Develop a global ranking mechanism
- Research and collect data on nation states' cybersecurity capabilities
- Contact and liaise with nation states and relevant organizations
- Identify and insert the relevant data into the index
- Publish a global cybersecurity index

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

Global Ranking

Country	Index	Global Rank
United States of America	0.824	1
Canada	0.794	2
Australia	0.765	3
Malaysia	0.765	3
Oman	0.765	3
New Zealand	0.735	4
Norway	0.735	4
Brazil	0.706	5
Estonia	0.706	5
Germany	0.706	5
India	0.706	5
Japan	0.706	5
Republic of Korea	0.706	5
United Kingdom	0.706	5
Austria	0.676	6
Hungary	0.676	6
Israel	0.676	6
Netherlands	0.676	6
Singapore	0.676	6
Latvia	0.647	7
Sweden	0.647	7
Turkey	0.647	7
Finland	0.618	8
Qatar	0.618	8
Slovakia	0.618	8
Uruguay	0.618	8
Colombia	0.588	9
Denmark	0.588	9
Egypt	0.588	9
France	0.588	9
Mauritius	0.588	9
Spain	0.588	9
Italy	0.559	10
Morocco	0.559	10
Uganda	0.559	10
Azerbaijan	0.529	11
Poland	0.529	11
Rwanda	0.529	11
Tunisia	0.529	11
Czech Republic	0.500	12
Georgia	0.500	12
Russia	0.500	12
Indonesia	0.471	13
Luxembourg	0.471	13
Romania	0.471	13
Belgium	0.441	14
Bulgaria	0.441	14
China	0.441	14
Lithuania	0.441	14
Nigeria	0.441	14
Sudan	0.441	14
Argentina	0.412	15
Cameroon	0.412	15
Croatia	0.412	15
Kenya	0.412	15
Mongolia	0.412	15
Sri Lanka	0.412	15
Thailand	0.412	15
Brunei Darussalam	0.382	16
Chile	0.382	16
Moldova	0.382	16
Montenegro	0.382	16

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

Myanmar	0.382	16
South Africa	0.382	16
Costa Rica	0.353	17
Ecuador	0.353	17
Malta	0.353	17
Philippines	0.353	17
Switzerland	0.353	17
Ukraine	0.353	17
United Arab Emirates	0.353	17
Burkina Faso	0.324	18
Mexico	0.324	18
Peru	0.324	18
Viet Nam	0.324	18
Bahrain	0.294	19
Bangladesh	0.294	19
Cyprus	0.294	19
Ghana	0.294	19
Iran	0.294	19
Libya	0.294	19
Panama	0.294	19
Portugal	0.294	19
Saudi Arabia	0.294	19
Afghanistan	0.265	20
Serbia	0.265	20
Togo	0.265	20
Cote d'Ivoire	0.235	21
Jamaica	0.235	21
Albania	0.206	22
El Salvador	0.206	22
Greece	0.206	22
Guatemala	0.206	22
Iceland	0.206	22
Ireland	0.206	22
Jordan	0.206	22
Liberia	0.206	22
Paraguay	0.206	22
Tanzania	0.206	22
Trinidad and Tobago	0.206	22
Venezuela	0.206	22
Algeria	0.176	23
Armenia	0.176	23
Barbados	0.176	23
Belarus	0.176	23
Belize	0.176	23
Benin	0.176	23
Bosnia and Herzegovina	0.176	23
Botswana	0.176	23
Kazakhstan	0.176	23
Malawi	0.176	23
Pakistan	0.176	23
Samoa	0.176	23
Senegal	0.176	23
Slovenia	0.176	23
Syria	0.176	23
Bahamas	0.147	24
Mauritania	0.147	24
Nicaragua	0.147	24
Saint Kitts and Nevis	0.147	24
State of Palestine	0.147	24
Tajikistan	0.147	24
Macedonia	0.147	24
Uzbekistan	0.147	24
Vanuatu	0.147	24
Zambia	0.147	24
Antigua and Barbuda	0.118	25
Bhutan	0.118	25
Bolivia	0.118	25
Burundi	0.118	25

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

Cambodia	0.118	25
Dominican Republic	0.118	25
Grenada	0.118	25
Guyana	0.118	25
Kyrgyzstan	0.118	25
Liechtenstein	0.118	25
Micronesia	0.118	25
Nepal	0.118	25
Papua New Guinea	0.118	25
Saint Lucia	0.118	25
Seychelles	0.118	25
Suriname	0.118	25
Angola	0.088	26
Gambia	0.088	26
Kiribati	0.088	26
Lebanon	0.088	26
Madagascar	0.088	26
Maldives	0.088	26
Mali	0.088	26
Monaco	0.088	26
Niger	0.088	26
South Sudan	0.088	26
Tonga	0.088	26
Turkmenistan	0.088	26
Zimbabwe	0.088	26
Andorra	0.059	27
Congo	0.059	27
Djibouti	0.059	27
Dominica	0.059	27
Fiji	0.059	27
Haiti	0.059	27
Kuwait	0.059	27
Lao	0.059	27
Mozambique	0.059	27
Sao Tome and Principe	0.059	27
Sierra Leone	0.059	27
Swaziland	0.059	27
Tuvalu	0.059	27
Yemen	0.059	27
Cape Verde	0.029	28
Chad	0.029	28
Comoros	0.029	28
Cuba	0.029	28
Democratic Republic of the Congo	0.029	28
Eritrea	0.029	28
Ethiopia	0.029	28
Gabon	0.029	28
Guinea	0.029	28
Guinea-Bissau	0.029	28
Iraq	0.029	28
Nauru	0.029	28
Palau	0.029	28
Solomon Islands	0.029	28
Somalia	0.029	28
Central African Republic	0.000	29
Democratic People's Republic of Korea	0.000	29
Equatorial Guinea	0.000	29
Honduras	0.000	29
Lesotho	0.000	29
Marshall Islands	0.000	29
Namibia	0.000	29
Saint Vincent and the Grenadines	0.000	29
Timor-Leste	0.000	29

(Source: ABI Research)

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

Regional Ranking

Arab States	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Oman	0.7500	0.6667	1.0000	0.7500	0.6250	0.7647	1
Qatar	0.7500	0.8333	0.5000	0.6250	0.5000	0.6176	2
Egypt	0.5000	0.5000	0.3750	1.0000	0.5000	0.5882	3
Morocco	0.5000	0.6667	0.7500	0.5000	0.3750	0.5588	4
Tunisia	1.0000	0.5000	0.6250	0.2500	0.5000	0.5294	5
Sudan	0.7500	0.5000	0.5000	0.2500	0.3750	0.4412	6
United Arab Emirates	0.7500	0.3333	0.2500	0.5000	0.1250	0.3529	7
Bahrain	0.7500	0.1667	0.1250	0.3750	0.2500	0.2941	8
Libya	0.2500	0.3333	0.3750	0.1250	0.3750	0.2941	8
Saudi Arabia	0.7500	0.3333	0.1250	0.3750	0.1250	0.2941	8
Jordan	0.5000	0.0000	0.5000	0.0000	0.1250	0.2059	9
Algeria	0.7500	0.0000	0.0000	0.1250	0.2500	0.1765	10
Syria	0.2500	0.3333	0.1250	0.1250	0.1250	0.1765	10
Mauritania	0.2500	0.1667	0.2500	0.0000	0.1250	0.1471	11
State of Palestine	0.2500	0.0000	0.3750	0.1250	0.0000	0.1471	11
Lebanon	0.0000	0.0000	0.0000	0.2500	0.1250	0.0882	12
Djibouti	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
Kuwait	0.0000	0.0000	0.0000	0.1250	0.1250	0.0588	13
Yemen	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
Comoros	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
Iraq	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
Somalia	0.0000	0.0000	0.0000	0.1250	0.0000	0.0294	14

Europe	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Norway	1.0000	0.6667	0.7500	0.8750	0.5000	0.7353	1
Estonia	1.0000	0.6667	1.0000	0.5000	0.5000	0.7059	2
Germany	1.0000	1.0000	0.6250	0.6250	0.5000	0.7059	2
United Kingdom	1.0000	0.6667	0.7500	0.7500	0.5000	0.7059	2
Austria	1.0000	0.3333	0.8750	0.7500	0.5000	0.6765	3
Hungary	1.0000	0.6667	0.7500	0.6250	0.5000	0.6765	3
Israel	1.0000	0.6667	0.6250	0.7500	0.5000	0.6765	3
Netherlands	0.7500	0.5000	0.8750	0.6250	0.6250	0.6765	3
Latvia	1.0000	0.6667	0.7500	0.5000	0.5000	0.6471	4
Sweden	0.7500	0.6667	0.6250	0.6250	0.6250	0.6471	4
Turkey	0.5000	0.6667	0.7500	0.7500	0.5000	0.6471	4
Finland	0.5000	0.6667	0.8750	0.5000	0.5000	0.6176	5
Slovakia	1.0000	0.6667	0.8750	0.2500	0.5000	0.6176	5
Denmark	1.0000	0.6667	0.5000	0.5000	0.5000	0.5882	6
France	1.0000	0.1667	0.5000	0.7500	0.6250	0.5882	6
Spain	1.0000	0.6667	0.6250	0.6250	0.2500	0.5882	6
Italy	0.7500	0.3333	0.6250	0.6250	0.5000	0.5588	7
Poland	1.0000	0.3333	0.6250	0.6250	0.2500	0.5294	8
Czech Republic	0.7500	0.6667	0.6250	0.3750	0.2500	0.5000	9
Luxembourg	0.7500	0.3333	0.5000	0.3750	0.5000	0.4706	10
Romania	0.7500	0.3333	0.6250	0.2500	0.5000	0.4706	10
Belgium	0.7500	0.5000	0.2500	0.3750	0.5000	0.4412	11
Bulgaria	0.7500	0.6667	0.5000	0.3750	0.1250	0.4412	11
Lithuania	1.0000	0.3333	0.7500	0.1250	0.2500	0.4412	11
Croatia	0.7500	0.6667	0.2500	0.3750	0.2500	0.4118	12
Montenegro	1.0000	0.5000	0.5000	0.0000	0.2500	0.3824	13
Malta	0.7500	0.5000	0.2500	0.2500	0.2500	0.3529	14
Switzerland	0.5000	0.3333	0.2500	0.2500	0.5000	0.3529	14
Cyprus	0.7500	0.1667	0.3750	0.1250	0.2500	0.2941	15
Portugal	0.7500	0.5000	0.1250	0.1250	0.2500	0.2941	15
Serbia	0.7500	0.0000	0.3750	0.2500	0.1250	0.2647	16
Albania	0.7500	0.3333	0.1250	0.1250	0.0000	0.2059	17
Greece	0.5000	0.3333	0.1250	0.1250	0.1250	0.2059	17
Iceland	0.7500	0.3333	0.0000	0.0000	0.2500	0.2059	17
Ireland	0.5000	0.1667	0.0000	0.3750	0.1250	0.2059	17
Bosnia and Herzegovina	0.7500	0.0000	0.1250	0.1250	0.1250	0.1765	18
Slovenia	0.5000	0.3333	0.0000	0.1250	0.1250	0.1765	18
Macedonia	0.7500	0.1667	0.0000	0.0000	0.1250	0.1471	19
Liechtenstein	0.7500	0.0000	0.0000	0.0000	0.1250	0.1176	20
Monaco	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	21
Andorra	0.5000	0.0000	0.0000	0.0000	0.0000	0.0588	22

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

Asia Pacific	Legal	Technical	Organizational	Capacity	Cooperation	Index	Regional Rank
Australia	0.7500	0.6667	0.8750	0.8750	0.6250	0.7647	1
Malaysia	0.7500	0.8333	1.0000	0.6250	0.6250	0.7647	1
New Zealand	1.0000	0.8333	0.8750	0.6250	0.5000	0.7353	2
India	1.0000	0.6667	0.7500	0.8750	0.3750	0.7059	3
Japan	1.0000	0.6667	0.7500	0.6250	0.6250	0.7059	3
Republic of Korea	1.0000	0.6667	0.8750	0.6250	0.5000	0.7059	3
Singapore	0.7500	0.6667	0.7500	0.7500	0.5000	0.6765	4
Indonesia	1.0000	0.3333	0.2500	0.5000	0.5000	0.4706	5
China	0.7500	0.5000	0.2500	0.5000	0.3750	0.4412	6
Mongolia	0.5000	0.8333	0.6250	0.1250	0.1250	0.4118	7
Sri Lanka	0.5000	0.3333	0.2500	0.5000	0.5000	0.4118	7
Thailand	0.5000	0.3333	0.5000	0.2500	0.5000	0.4118	7
Brunei Darussalam	0.7500	0.3333	0.1250	0.3750	0.5000	0.3824	8
Myanmar	0.2500	0.5000	0.2500	0.5000	0.3750	0.3824	8
Philippines	1.0000	0.3333	0.3750	0.3750	0.0000	0.3529	9
Viet Nam	0.5000	0.3333	0.1250	0.5000	0.2500	0.3235	10
Bangladesh	0.5000	0.3333	0.1250	0.2500	0.3750	0.2941	11
Iran	0.5000	0.3333	0.5000	0.1250	0.1250	0.2941	11
Afghanistan	0.0000	0.5000	0.3750	0.2500	0.1250	0.2647	12
Pakistan	0.2500	0.1667	0.0000	0.3750	0.1250	0.1765	13
Samoa	0.5000	0.0000	0.1250	0.1250	0.2500	0.1765	13
Vanuatu	0.0000	0.0000	0.2500	0.1250	0.2500	0.1471	14
Bhutan	0.2500	0.3333	0.1250	0.0000	0.0000	0.1176	15
Cambodia	0.2500	0.3333	0.1250	0.0000	0.0000	0.1176	15
Micronesia	0.0000	0.0000	0.2500	0.1250	0.1250	0.1176	15
Nepal	0.5000	0.0000	0.1250	0.0000	0.1250	0.1176	15
Papua New Guinea	0.0000	0.0000	0.3750	0.0000	0.1250	0.1176	15
Kiribati	0.0000	0.0000	0.1250	0.0000	0.2500	0.0882	16
Maldives	0.0000	0.0000	0.1250	0.0000	0.2500	0.0882	16
Tonga	0.5000	0.0000	0.1250	0.0000	0.0000	0.0882	16
Fiji	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	17
Lao	0.0000	0.3333	0.0000	0.0000	0.0000	0.0588	17
Tuvalu	0.0000	0.0000	0.1250	0.0000	0.1250	0.0588	17
Nauru	0.0000	0.1667	0.0000	0.0000	0.0000	0.0294	18
Palau	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	18
Solomon Islands	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	18
Democratic People's Republic of Korea	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19
Marshall Islands	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19
Timor-Leste	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19

Americas	Legal	Technical	Organizational	Capacity	Cooperation	Index	Regional Rank
United States of America	1.0000	0.8333	0.8750	1.0000	0.5000	0.8235	1
Canada	0.7500	1.0000	0.8750	0.8750	0.5000	0.7941	2
Brazil	0.7500	0.6667	0.8750	0.7500	0.5000	0.7059	3
Uruguay	1.0000	0.6667	0.6250	0.5000	0.5000	0.6176	4
Colombia	0.7500	0.5000	0.7500	0.7500	0.2500	0.5882	5
Argentina	1.0000	0.3333	0.3750	0.5000	0.1250	0.4118	6
Chile	0.7500	0.5000	0.2500	0.3750	0.2500	0.3824	7
Costa Rica	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	8
Ecuador	0.2500	0.6667	0.1250	0.5000	0.2500	0.3529	8
Mexico	0.2500	0.5000	0.1250	0.3750	0.3750	0.3235	9
Peru	0.7500	0.3333	0.2500	0.1250	0.3750	0.3235	9
Panama	0.2500	0.5000	0.3750	0.2500	0.1250	0.2941	10
Jamaica	0.7500	0.0000	0.1250	0.1250	0.3750	0.2353	11
El Salvador	0.0000	0.3333	0.2500	0.1250	0.2500	0.2059	12
Guatemala	0.0000	0.3333	0.1250	0.3750	0.1250	0.2059	12
Paraguay	0.0000	0.3333	0.1250	0.2500	0.2500	0.2059	12
Trinidad and Tobago	0.2500	0.0000	0.5000	0.1250	0.1250	0.2059	12
Venezuela	0.5000	0.3333	0.0000	0.2500	0.1250	0.2059	12
Barbados	0.5000	0.0000	0.1250	0.2500	0.1250	0.1765	13
Belize	0.2500	0.0000	0.2500	0.1250	0.2500	0.1765	13
Bahamas	0.7500	0.0000	0.0000	0.1250	0.1250	0.1471	14
Nicaragua	0.5000	0.0000	0.2500	0.1250	0.0000	0.1471	14
Saint Kitts and Nevis	0.7500	0.0000	0.1250	0.0000	0.1250	0.1471	14
Antigua and Barbuda	0.7500	0.0000	0.0000	0.1250	0.0000	0.1176	15
Bolivia	0.0000	0.0000	0.2500	0.1250	0.1250	0.1176	15
Dominican Republic	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	15
Grenada	0.7500	0.0000	0.0000	0.1250	0.0000	0.1176	15
Guyana	0.0000	0.3333	0.1250	0.0000	0.1250	0.1176	15
Saint Lucia	0.7500	0.0000	0.0000	0.0000	0.1250	0.1176	15
Suriname	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	15
Haiti	0.0000	0.0000	0.0000	0.1250	0.1250	0.0588	16
Dominica	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	16
Cuba	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Honduras	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
Saint Vincent and the Grenadines	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

Commonwealth of Independent States	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Azerbaijan	0.7500	0.5000	0.5000	0.5000	0.5000	0.5294	1
Georgia	0.7500	0.6667	0.7500	0.2500	0.2500	0.5000	2
Russia	1.0000	0.3333	0.5000	0.3750	0.5000	0.5000	2
Moldova	0.7500	0.5000	0.2500	0.2500	0.3750	0.3824	3
Ukraine	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	4
Armenia	0.5000	0.5000	0.0000	0.0000	0.1250	0.1765	5
Belarus	0.7500	0.3333	0.0000	0.0000	0.1250	0.1765	5
Kazakhstan	0.7500	0.3333	0.0000	0.0000	0.1250	0.1765	5
Tajikistan	0.7500	0.0000	0.0000	0.0000	0.2500	0.1471	6
Uzbekistan	0.7500	0.1667	0.0000	0.0000	0.1250	0.1471	6
Kyrgyzstan	0.5000	0.0000	0.0000	0.0000	0.2500	0.1176	7
Turkmenistan	0.7500	0.0000	0.0000	0.0000	0.0000	0.0882	8

Africa	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Mauritius	0.7500	0.6667	0.6250	0.5000	0.5000	0.5882	1
Uganda	0.7500	0.5000	0.8750	0.2500	0.5000	0.5588	2
Rwanda	1.0000	0.5000	0.5000	0.3750	0.5000	0.5294	3
Nigeria	0.2500	0.3333	0.5000	0.5000	0.5000	0.4412	4
Cameroon	0.7500	0.5000	0.3750	0.5000	0.1250	0.4118	5
Kenya	1.0000	0.3333	0.2500	0.2500	0.5000	0.4118	5
South Africa	0.2500	0.5000	0.6250	0.2500	0.2500	0.3824	6
Burkina Faso	0.0000	0.5000	0.7500	0.0000	0.2500	0.3235	7
Ghana	0.7500	0.3333	0.2500	0.2500	0.1250	0.2941	8
Togo	0.0000	0.3333	0.3750	0.2500	0.2500	0.2647	9
Cote d'Ivoire	0.7500	0.3333	0.1250	0.1250	0.1250	0.2353	10
Liberia	0.0000	0.0000	0.2500	0.3750	0.2500	0.2059	11
Tanzania	0.5000	0.3333	0.0000	0.1250	0.2500	0.2059	11
Benin	0.5000	0.0000	0.2500	0.1250	0.1250	0.1765	12
Botswana	0.7500	0.1667	0.2500	0.0000	0.0000	0.1765	12
Malawi	0.0000	0.0000	0.1250	0.3750	0.2500	0.1765	12
Senegal	1.0000	0.0000	0.1250	0.0000	0.1250	0.1765	12
Zambia	0.2500	0.3333	0.1250	0.1250	0.0000	0.1471	13
Burundi	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	14
Seychelles	0.7500	0.0000	0.0000	0.0000	0.1250	0.1176	14
Angola	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
Gambia	0.5000	0.0000	0.1250	0.0000	0.0000	0.0882	15
Madagascar	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
Mali	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
Niger	0.2500	0.0000	0.0000	0.1250	0.1250	0.0882	15
South Sudan	0.5000	0.0000	0.0000	0.0000	0.1250	0.0882	15
Zimbabwe	0.2500	0.0000	0.1250	0.0000	0.1250	0.0882	15
Congo	0.0000	0.0000	0.1250	0.0000	0.1250	0.0588	16
Mozambique	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	16
Sao Tome and Principe	0.0000	0.0000	0.1250	0.0000	0.1250	0.0588	16
Sierra Leone	0.0000	0.0000	0.2500	0.0000	0.0000	0.0588	16
Swaziland	0.2500	0.0000	0.1250	0.0000	0.0000	0.0588	16
Cape Verde	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Chad	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Democratic Republic of the Congo	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Eritrea	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Ethiopia	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Gabon	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Guinea	0.0000	0.0000	0.1250	0.0000	0.0000	0.0294	17
Guinea-Bissau	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Central African Republic	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
Equatorial Guinea	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
Lesotho	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18
Namibia	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18

(Source: ABI Research)

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

Categories and Performance Indicators

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

1. Legal Measures

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

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

A. Criminal Legislation

Cybercrime legislation designates laws on the unauthorized (without right) access, interference, and interception of computers, systems, and data. The laws can be ranked by level: none, partial, comprehensive. “Partial” legislation refers to the simple insertion of computer-related wording in an existing criminal law or code, with language limited to extending, for example, fraud, forgery, surveillance, or theft to cyberspace. “Comprehensive” legislation refers to the enactment of a dedicated law or act dealing with the specifics of computer crime (e.g., the U.K. Computer Misuse Act 1990). This category can include partial legislation wherein the case law or jurisprudence is extensively developed.

B. Regulation and Compliance

Cybersecurity regulation designates laws dealing with data protection, breach notification, and certification/ standardization requirements. The laws can be ranked by level: none, partial, comprehensive. “Partial” regulation refers to the insertion of computer-related wording in existing or new criminal or civil law so the law extends applicability to cyberspace in regulation not specifically or uniquely related to cybersecurity (e.g., the E.U. Directive 95/46/EC on the “protection of individuals with regard to the processing of personal data and on the free movement of such data”). “Comprehensive” regulation refers to the enactment of a d edicated law, act, or directive requiring cybersecurity compliance (e.g., the U.S. Federal Information Security Management Act of 2002).

2. Technical Measures

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

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

A. CERT/CIRT/CSIRT

The establishment of a national computer incident response team (CIRT), computer emergency response team (CERT), or computer security incident response team (CSIRT) provides the capabilities to identify, defend, respond, and manage cyber threats and enhance cybersecurity in the nation state. This ability needs to be coupled with the gathering of the nation state’s own intelligence instead of relying on secondary reporting of security incidents, whether from a CIRT’s constituencies or other sources.

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

B. Standards

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within 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.

C. Certification

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of national (governmental) agencies and public-sector professionals by internationally recognized cybersecurity standards. These certifications, accreditations, and standards include but are not limited to the following agencies: 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.

3. Organizational Measures

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

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

A. Policy

The development of a policy to promote cybersecurity is recognized as a top priority. A national strategy for the security of network and information systems should maintain resilient and reliable information infrastructure and aim to ensure the safety of citizens; protect the material and intellectual assets of citizens, organizations, and the nation state; prevent cyberattacks against critical infrastructure; and minimize damage and recovery times from cyberattacks . Policies on national cybersecurity strategies or national plans for the protection of information infrastructures are those officially defined and endorsed by a nation sate and can include the following commitments: establishing clear responsibility for cybersecurity at all levels of government (local, regional, and federal or national), with clearly defined roles and responsibilities; making a clear commitment to cybersecurity, which is public and transparent; and encouraging private-sector involvement and partnership in government-led initiatives to promote cybersecurity.

B. Roadmap for Governance

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

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

C. Responsible Agency

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

D. National Benchmarking

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

4. Capacity Building

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

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

A. Standardization Development

Standardization is a good indicator of the level of maturity of a technology, and the emergence of new standards in key areas underlines the vital importance of standards. Although cybersecurity has always been an issue in national security, and treated differently in various countries, uniform approaches are supported by commonly recognized standards. These standards include but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.

B. Manpower Development

Manpower development should include efforts by nation states to promote widespread publicity campaigns to reach as many people as possible, as well as make use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centers, computer stores, community colleges and adult education programs, and schools and parent/teacher organizations to get the message across about safe cyberbehavior online. This includes actions such as setting up portals and websites to promote awareness, disseminating support material for educators, and establishing (or incentivizing) professional training courses and education programs.

C. Professional Certification

This performance indicator can be measured by the number of public-sector professionals certified under internationally recognized certification program standards, including but not being limited to the following agencies : 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.

D. Agency Certification

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

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

5. Cooperation

Cybersecurity requires input from all sectors and disciplines, and, for this reason, needs to be tackled from a multi-stakeholder approach. Cooperation enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application. Information sharing is difficult at best between different disciplines and within private-sector operators. It becomes increasingly so at the international level. However, the cybercrime problem is one of a global nature, and is blind to national borders or sectoral distinctions. Cooperation enables sharing of threat information, attack scenarios, and best practices in response and defense. Greater cooperative initiatives can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats and enable better investigation, apprehension, and prosecution of malicious agents.

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

A. Intra-state Cooperation

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

B. Intra-agency Cooperation

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

C. Public-Private Partnerships

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

D. International Cooperation

This performance indicator refers to any officially recognized participation in international cybersecurity platforms and forums. Such cooperative initiatives include those undertaken by but not limited to the United Nations General Assembly, the International Telecommunication Union (ITU), Interpol/Europol, the Organisation for Economic Co-operation and Development (OECD), the United Nations Office on Drugs and Crime (UNODC), the United Nations Interregional Crime and Justice Research Institute (UNICRI), the Internet Corporation for Assigned Names and Numbers (ICANN), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Internet Engineering Task Force, and the Forum of Incident Response and Security Teams (FIRST).

Methodology

The statistical model used will be based on a Multi-Criteria Analysis (MCA). The MCA establishes preferences between options by reference to an explicit set of identified objectives and for which there are established measurable criteria to assess the extent to which the objectives have been achieved. A simple linear additive evaluation model will be applied. The MCA performance matrix describes the options, and each column describes the performance of the options against each criterion. The individual performance assessment is numerical.

The benchmark scoring will be based on the indicators below, each of which is weighted equally (although the weighting for the subcategories will be slightly higher than others since some contain more sub-groups). “0” points are allocated when there are no activities, “1” point is allocated for partial action, and “2” points for more comprehensive action. Total points allocated for each category are:

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

1. LEGAL MEASURES	4
A. Criminal Legislation	2
B. Regulation & Compliance.	2

2. TECHNICAL MEASURES	6
A. CERT/CIRT/CSIRT	2
B. Standards	2
C. Certification	2

3. ORGANIZATIONAL MEASURES	8
A. Policy	2
B. Roadmap for Governance	2
C. Responsible Agency	2
D. National Benchmarking	2

4. CAPACITY BUILDING	8
A. Standardization Development	2
B. Manpower Development	2
C. Professional Certification	2
D. Agency Certification	2

5. COOPERATION	8
A. Intra-state Cooperation	2
B. Intra-agency Cooperation	2
C. Public-Private Partnerships	2
D. International Cooperation	2

Notation:

x_{qc} Value of the individual indicator q for country c, with q=1,...,Q and c=1,...,M.

I_{qc} Normalized value of individual indicator q for country c

CI_c Value of the composite indicator for country c

The benchmark used will be the score of the hypothetical country that maximizes the overall readiness (34) points. The resulting composite index will range between 0 (worst possible readiness) and 1 (the benchmark).

$$CI_c = \frac{I_{qc}}{34}$$

The normalization technique will be based on a ranking method:

$$I_{qc} = Rank\ (x_{qc})$$

Impact

The long-term aim of the GCI is to drive further efforts in the adoption and integration of cybersecurity on a global scale. A comparison of national cybersecurity strategies will reveal those states with high rankings in specific areas, and consequently expose lesser-known yet successful cybersecurity strategies. This can prompt increased information sharing on deploying cybersecurity for those states at different levels of development, as well. By measuring the level of cybersecurity preparedness in various areas, the index will allow states to assess where they are on a scale of development, where they need to make further improvements, and how far they are from implementing an acceptable level of cybersecurity. All states are moving toward a more digitized and connected environment, and adopting cybersecurity early on can enable the deployment of more secure and resilient infrastructure.

© 2014 ABI Research. Distributed with permission of ABI Research. *Global Cybersecurity Index*: December 9, 2014

ABIresearch

Global Cybersecurity Index

Michela Menting: Practice Director

Published December 9, 2014

Post Office Box 452 • 249 South Street
Oyster Bay, New York 11771 USA
Tel: +1 516-624-2500 | Fax: +1 516-624-2501

www.abiresearch.com