Global Cybersecurity Index (GCI) 2020

In June 2021, the International Telecommunication Union (ITU) released the Global Cybersecurity Index 2020, a trusted reference that measures the commitment of countries to cybersecurity and promotes action towards secure digital ecosystems needed for recovery and growth.

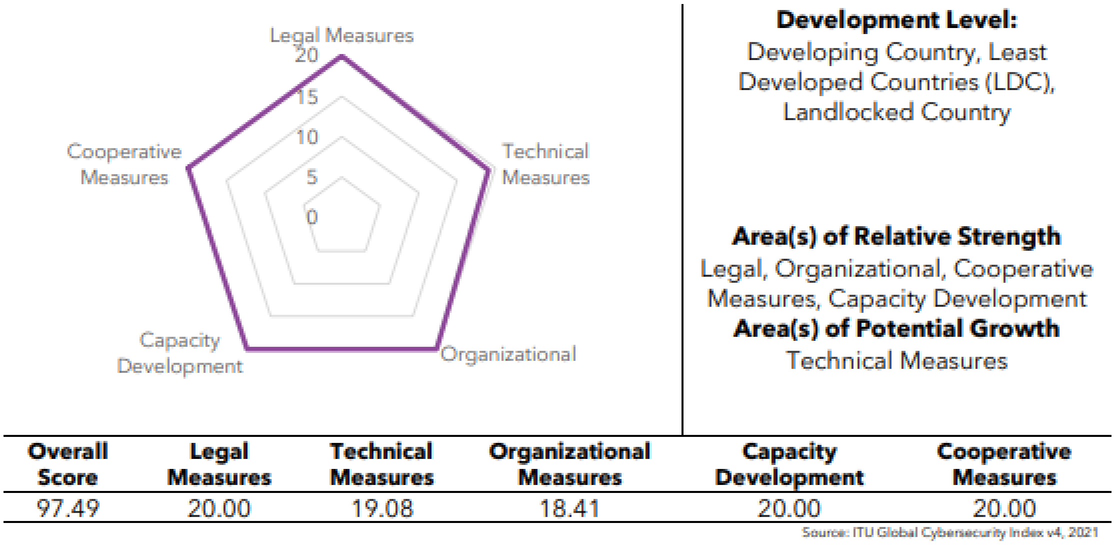
GCI 2020 - Key Findings, Scores & Rankings

- Overall, the United States of America ranked at the first position in GCI 2020 with a score of 100
- The Democratic People's Republic of Korea ranked at the last position with a score of 1.35
- In 2020, India ranked at the 10th position, in comparison to its 47th position in the last GCI
- In the Asia-Pacific region, India ranked at the 4th position
- The table given below mentions the region-wise toppers along with their scores:

GCI Results - Regional scores and ranking of countries		
Region	**Country**	**Score**
Africa	Mauritius	96.89
America	United States of America	100
Arab States	Saudi Arabia	99.54
Asia-Pacific	Korea (Rep. of)	98.52
Commonwealth of Independent States (CIS)	Russian Federation	98.06
Europe	United Kingdom	99.54

- The image given below shows India’s status and scores based on the different parameters on which the Global Cybersecurity Index is analysed:

India (Republic of)



Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.49	20.00	19.08	18.41	20.00	20.00

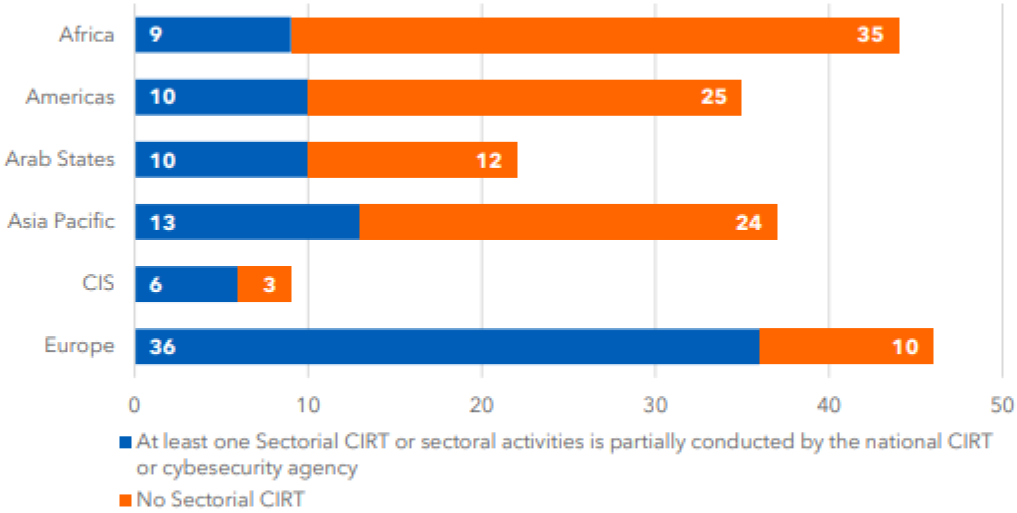
Source: ITU Global Cybersecurity Index v4, 2021

Parameters for GCI 2020 Assessment

There are five key parameters and themes of cybersecurity based on which the performance of the countries are analysed. Discussed below are the same.

- **Legal Measures**
    - Legal and regulatory frameworks include the establishment of legislation for illicit activities in cyberspace, along with the tools to investigate, prosecute and enforce such legislation
    - Data theft legislation must be passed by the countries
    - Online harassment and online racism and xenophobia have also been a great cause of concern as per the statistics from GCI
    - **Online data privacy & protection -** 133 countries have signed protection and privacy regulations into law, 15 are in the drafting process, and 46 have no regulation in place
    - **Legislation on the theft of personal information -** This is important due to the increase in usage of social media platforms and online transactions. Of the 194 countries, 97 have passed a law, 17 have drafted and the remaining 80 countries have taken no action
    - **Online harassment legislation -** Globally, 100 countries have adopted legislation criminalizing instances of online harassment and abuse, 17 are in the process of drafting and implementing these measures and 77 have no legislation on the subject
- **Technical Measures**
    - Increased deployment of Computer Incident Response Teams (CIRTs) or Computer Emergency Response Teams (CERTs) enable countries to respond to incidents at the national level. At the end of 2020, 131 countries had established national CIRTs

- While national CIRTs address issues on the national level, sector-specific CIRTs address the cybersecurity needs of a specific sector such as health, transport, telecommunication, utilities. The image given below shows the number of sector-specific CIRTs:



- **Organizational Measures**
  - Organizational measures examine the governance and coordination mechanisms within countries that address cybersecurity
  - This year, more focus has been placed on countries engaging in a regular update of **National Cybersecurity Strategies (NCS)**. This ensures that countries are adapting to the evolving realities
  - 127 countries having a national cybersecurity strategy; 60 countries have demonstrated progress in establishing NCS
- **Capacity Development Measures**
  - Digital technology brings immense economic and societal benefits, cyber risks can offset the benefits of digitalization. Securing the cyber domain through cybersecurity capacity building activities is key as it contributes to reducing issues such as the Digital Divide and cyber risks.
  - Promoting three of the Sustainable Development Goals, SDG 8 (Decent Work and Economic Growth), SDG 9 (Industry, Innovation and Infrastructure), and SDG 10 (Reduced Inequalities) are important from the cybersecurity capacity development
  - Public awareness of cybersecurity is also of utmost importance. Results from the GCI show that about **60 percent of countries** are, or have been during the past two years, **engaged in improving cyber awareness, against 38 per cent that did not report any cybersecurity campaigns**
- **Cooperative Measures**
  - Cybersecurity risks are increasingly borderless and collaboration remains an essential tool to tackle cybersecurity challenges

  - **Bilateral and multilateral agreements are crucial** in codifying norms and behaviours and enhancing international cooperation on cybersecurity. GCI reports suggest that 90 countries out of 194 have a bilateral agreement in cybersecurity
  - Public-private partnerships (PPP) are critical to cybersecurity efforts, from sharing actionable intelligence, exchanging good practice, and communicating R&D needs and priorities

COVID-19 Pandemic and its Impact on Cybersecurity - GCI Analysis

The report released by ITU mentions that since April 2020, when the COVID pandemic began to widespread across the world, internet usage increased by 30 percent.

This pandemic made digital tools and technology an integral part of everyone's life and in such circumstances, cyber safety is of high importance. The ongoing pandemic has created distrust, especially online and there is increased recognition of cybersecurity risk.