Under High-profile global cyber attacks, Global Cybersecurity Index 2017 measures the commitment of the ITU Member States to cybersecurity

Singapore has topped a global cyber security index released by the United Nations, followed by other UN member states such as the United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France and Canada, the other top 10 countries. The Index has been released by the UN telecommunications agency International Telecommunication Union (ITU). The moves come against the backdrop of a series of high-profile global cyber attacks over the past two months, such as the WannaCry ransomware attack in May and NotPetya in June.

UN survey shows big gaps in the level of cybersecurity across 193 countries in the world. As per the findings of the Global Cybersecurity Index 2017 (GCI), India ranks 23 out of the 193 member countries when it comes to commitment to cybersecurity. India has been listed in the "maturing category" of the index with a score of 0.683. Around 77 countries have been placed in the maturing category as they have developed complex commitments to cyber security and engage in cybersecurity programmes and initiatives.

The global community is increasingly embracing ICTs as key enabler for social and economic development. The information and communication technologies (ICT) networks, devices and services are increasingly critical for day-to-day life. In

2016, almost half the world used the Internet (3.5 billion users) and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020.

Yet, just as in the real world, the cyber world is exposed to a variety of security threats that can cause immense damage. In 2016, nearly one percent of all emails sent were essentially malicious attacks, the highest rate in recent years. Ransomware attacks increasingly affected businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. Attackers are demanding more and more from victims, with the average ransom demand rising to over 1,000 USD in 2016, up from approximately 300 USD a year earlier. In May 2017, a massive cyberattack caused major disruptions to companies and hospitals in over 150 countries, prompting a call for greater cooperation around the world.

The scale of cybercrime makes it critical for governments to have a robust cybersecurity ecosystem in place to reduce threats and enhance confidence in using electronic communications and services. First launched in 2014, the goal of the Global Cybersecurity Index (GCI) is to help foster a global culture of cybersecurity and its integration at the core of ICTs. The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

Important features of the report:

- One of the strongest commitments is to outline a cybersecurity strategy describing how the country will prepare and respond to attacks against its digital networks. According to the report Only 38% countries have a published cybersecurity strategy and only 11% have a dedicated standalone strategy; another 12% have a cybersecurity strategy under development.
- Despite half of the Member States not having a

cybersecurity strategy, 61% do have an emergency response team (i.e., CIRT, CSRIT, and CERT) with national responsibility. However, just over a fifth (21%) publish metrics on cybersecurity incidents This makes it difficult in most countries to objectively assess incidents based on the evidence and determine if protection measures are working.

- "Cybersecurity is an ecosystem where laws, organisations, skills, cooperation and technical implementation need to be in harmony to be most effective," stated the report, adding that cybersecurity is "becoming more and more relevant in the minds of the decision makers."
- In addition to showing the overall cyber security commitment of ITUs 193 member-states, the Index also shows the improvement and strengthening of the five pillars of the ITU Global Cybersecurity Agenda: legal, technical, organisational, capacity building and international cooperation.

Some of the interesting comparisons

- Australia is third ranked in the region and home to AusCERT, one of oldest CERTs in the region formed in 1993. The highest scoring pillar is technical where there is a certification programme for information security skills provided by the Council of Registered Ethical Security Testers (CREST). Modelled after CREST, the council offers assessment, accreditation, certification, education and training in cyber and information security for individuals and corporate entities in both Australia and New Zealand.
- The Russian Federation ranked second in the region, scores best in capacity building. Its commitments range

from developing cybersecurity standards to R&D and from public awareness to a home-grown cybersecurity industry. An example of the latter is Kaspersky Labs, founded in 1997 and whose software protects over 400 million users and some 270 000 organizations.

- Estonia is the highest-ranking nation in the Europe region. Like Georgia, Estonia enhanced its cybersecurity commitment after a 2007 attack. This included the introduction of an organizational structure that can respond quickly to attacks as well as a legal act that requires all vital services to maintain a minimal level of operation if they are cut off from the Internet. The country also hosts the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence.

Conceptual framework

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation).

The five pillars of the GCI are briefly explained below:

1. Legal: Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. Technical: Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.
3. Organizational: Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
4. Capacity Building: Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.
5. Cooperation: Measured based on the existence of

partnerships, cooperative frameworks and information sharing networks.

The GCI 2017 edition measured the commitment of the ITU Member States to cybersecurity and highlighted a number of illustrative practices from around the world. As a logical continuation of the first iteration of the GCI issued in 2014, this version has motivated countries to improve their work related to cybersecurity, raised awareness in countries for the need to start bilateral, multilateral and international cooperation, and increased the visibility of what countries are doing to improve cybersecurity.

References and Resources also include:

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

http://indiatoday.intoday.in/education/story/india-global-cybersecurity-index/1/996589.html