GLOBAL CYBERSECURITY OUTLOOK 2025 - REPORTS

NEWS: *The World Economic Forum (WEF) recently released* ***Global Cybersecurity Outlook 2025.***

WHAT'S IN THE NEWS?

About Global Cybersecurity Outlook 2025

- It is produced in collaboration with Accenture and it examines the cybersecurity trends that will affect economies and societies in the year to come.
- It explores major findings and puts a spotlight on the complexity of the cybersecurity landscape, which is intensified by geopolitical tensions, emerging technologies, supply chain interdependencies and cybercrime sophistication.

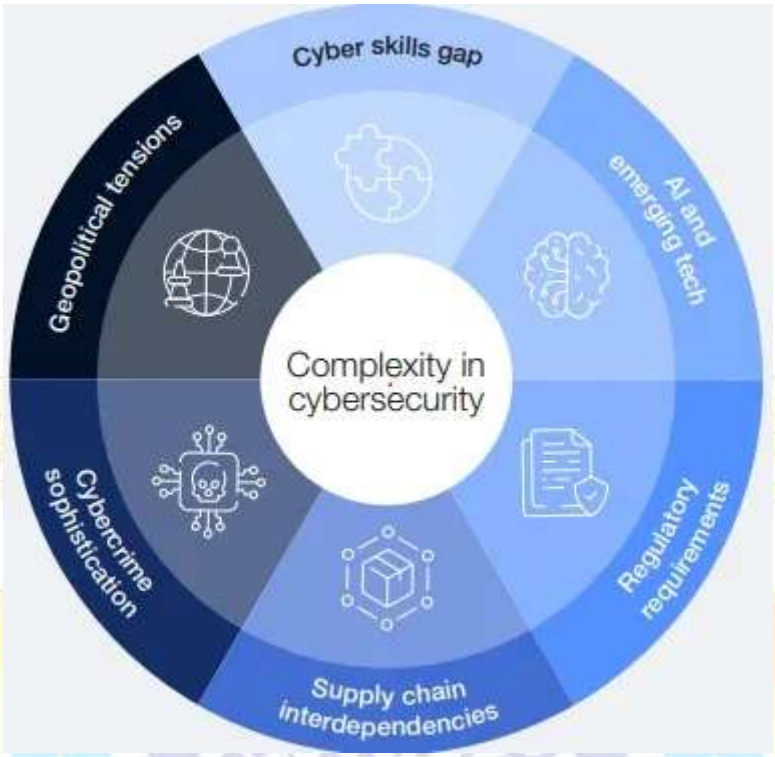
Key issues Highlighted

- **Geopolitical Conflicts:** Ongoing conflicts, such as the war in Ukraine, have increased cyber vulnerabilities in critical sectors like energy, telecommunications, and nuclear power.
- **Cybersecurity Readiness:** Two-thirds of organizations anticipate AI impacting cybersecurity, but only one-third have requisite tools to assess AI-related risks, with smaller organizations facing significant challenges.
- **Cyber Skills Gap:** As of 2024, there is a shortage of 4.8 million cybersecurity professionals.
    - Only 14% of organizations have a skilled workforce to address current cybersecurity challenges. Public-sector organizations are particularly impacted.
- **Supply Chain Interdependencies:** Over 50% of large organizations identify supply chain complexity as a barrier to cyber resilience.
    - Concerns include vulnerabilities in third-party software, cyberattacks, and challenges in enforcing security standards.
- **Cybercrime Sophistication:** Cybercriminals are leveraging generative AI tools for more personalized and automated attacks, including phishing and social engineering.
    - In 2024, 42% of organizations experienced phishing and deepfake attacks.
- **Regulatory Challenges:** 70% of organizations find cybersecurity regulations too complex, causing compliance issues.

Impacts

- **Critical Infrastructure:** Cyberattacks on water utilities, satellites, and power grids can disrupt essential services and public safety.
    - An example of this is the October 2024 attack on a U.S. water utility.
- **Biosecurity Risks:** Advancements in AI, cyberattacks, and genetic engineering pose threats to laboratories and public safety.
    - Incidents in South Africa and the UK highlight the risks.
- **Economic Disparity:** A divide in cyber resilience exists, with developed regions (e.g., Europe and North America) better prepared than emerging economies (e.g., Africa and Latin America).

- **Transition Issues to RE:** The shift to renewable energy systems introduces new vulnerabilities, making power grids attractive targets for cybercriminals.



What is the Global Cybersecurity Index (GCI)?

- **About:**
  - GCI, **launched in 2015** by ITU **measures the** comprehensive development and **commitment** to **cybersecurity at a global level.**
  - The GCI utilises a **multi-stakeholder approach** and leverages the capacity and expertise of **different organisations**.
- **Aim:**
  - It aims to **improve the quality of the survey,** foster international cooperation, promote knowledge exchange and **raise awareness** of the importance and different dimensions of **cybersecurity.**
- **Pillars of Assessment:**
  - The assessment is based on **5 pillars: Legal Measures, Technical Measures, Organisational Measures, Capacity Development**, and **Cooperation**.
  - The index aggregates the assessment into an **overall score** for each country.
- **5- Tier Analysis:** Countries are categorised into five tiers based on their cybersecurity efforts, with Tier 1 representing the highest level.
  - Tier 1- Role-modelling (score of 95–100)
  - Tier 2- Advancing (score of 85–95)
  - Tier 3- Establishing (score of 55–85)

- Tier 4- Evolving (score of 20–55)
- Tier 5- Building (score of 0–20).

What is ITU?

- It is the **United Nations (UN)** specialised agency for **Information and Communication Technologies (ICT)s**.
- It was **founded in 1865 t**o **facilitate international connectivity in communications** networks.
- It is headquartered in **Geneva, Switzerland.**
- It allocates **global radio spectrum and satellite orbits**, develops the **technical standards** that ensure networks and technologies seamlessly interconnect, and strives to improve access to ICTs to underserved communities worldwide.
- ITU currently has a membership of **193 countries** and over 900 private-sector entities and academic institutions.
    - India has been a member of ITU since 1869 and has been a member of the **ITU Governing Council** since its inception in 1952.

Suggestions and Way Forward

- **Strategic Investment:** Cybersecurity should be treated as a strategic investment rather than a technical issue, with leadership focusing on technical and economic dimensions.
- **Collaboration:** Stronger collaboration between business and cybersecurity leaders is essential to manage growing threats and risks.
- **Simplify Regulations:** Streamline and harmonize global cybersecurity regulations to enhance compliance and resilience.
- **Skills Development:** Address the global cyber skills gap through targeted training and upskilling programs.
- **Focus on Emerging Technologies:** Organizations must develop tools to assess and mitigate risks associated with AI adoption.