Securing the new normal: GCCs at the forefront of managing global digital risks

January 2021

By Srinivas Potharaju, Risk Transformation Leader and Partner, Digital, KPMG in India; Pranav Kathale, Emerging Technology Risks Leader and Director, Digital, KPMG in India; Srijit Menon, Third Party Risk Management Leader and Director, Digital, KPMG in India

(4 min read)

COVID-19-led disruption has fuelled sharp acceleration in digitisation. This, combined with increasing cybersecurity threats, has put the spotlight on an organisation's ability to manage digital risks. Global organisations face the twin challenge of protecting business and ensuring growth, while riding the digital wave.

The rapid adoption of digital technology has also increased the focus on managing digital risks. This 'digital risk debt' (DREBT) is represented by the growing divide between the need for digitisation and capability to deal with the concomitant risks. Cyber Global Capability Centres (GCCs) have presented a reliable, cost effective, secure and resilient operating model for organisations that are seeking a commercial and scalable solution to plug their DREBT.

Secure in India 2020, published by KPMG in India in collaboration with NASSCOM and DSCI, charts the growth of cyber GCCs in India and presents key insights on business case, organisation model, innovation, leadership, workforce and risk culture. Global chief information security officers, GCC leaders, GCC cybersecurity leaders and cyber subject matter experts participated in the Secure in India 2020 survey, sharing key insights and perspectives on how global organisations are leveraging cyber GCCs in managing global cybersecurity and digital risks.

Cyber GCCs have proactively embraced Work from Home (WFH) and are now adjusting to long-term remote work. Cyber GCCs are updating their policies, procedures, tools and strategies to ensure they remain resilient and continue to securely enable their global organisations.
While the pandemic has caused a great deal of disruption and hardships for businesses around the world, it has also opened up a plethora of opportunities for cyber GCC stakeholders.

1. **Global organisations:**

    - There is immense potential to harness cyber GCCs for leadership of global functions. A significant proportion of cyber GCC leaders serve on global cybersecurity committees and have global teams reporting into them. Cyber GCC leaders could be leveraged for additional roles in the functioning of the global organisation

- Cyber GCCs can be leveraged in the adoption of emerging technologies and to manage digital risks. In recent years, innovation, research and development have emerged as key drivers for the establishment of cyber GCCs. The innovation potential of cyber GCCs can be leveraged for product development and managing risks related to emerging technologies

- Cybersecurity innovation is another area in which cyber GCCs can be leveraged and recognised for their contributions. Cyber GCCs have deployed various use cases of process and platform innovation. They have focused their innovation strategies on several domains including Robotic Process Automation (RPA), Artificial Intelligence (AI), Machine Learning (ML), Security Orchestration, Automation and Response (SOAR) for Security Operations Centre (SOC) and Cloud Security, among others.

2. GCC cyber leaders:

- There is an opportunity to increase collaboration with the wider ecosystem and deepen the relationship with academic institutions, other GCCs and government bodies. This would help facilitate co-creation, investment opportunities, leadership development and joint representation in regulatory bodies

- There is also scope for conceptualisation and participation in industry wide crisis simulation exercises. Given the increase in concentration of global functions, cyber GCCs have become vital to an organisation's resilience. Participation in industry-wide crisis simulation exercises will increase readiness to respond to emerging and sophisticated cyber threats and signal maturity to the wider ecosystem

- Cyber GCC digitisation efforts have received a boost. They are embracing technologies including AI, ML, RPA and Cloud to increase the efficiency and effectiveness of the cybersecurity functions delivered.

3. Cyber GCC team members:

- There are a growing number of training opportunities to upskill and meet the demand for future oriented skills. This is an important focus area as cyber GCCs step up adoption of digital and emerging technologies for cybersecurity functions and addressing the related risks

- In the last few years, the GCC cybersecurity and digital risk leadership has broken through the glass ceiling, spearheading global cybersecurity functions for their organisations. This has opened up a number of cyber leadership opportunities within the GCC for the team members.

4. Policy makers:

- A conducive policy environment to support cyber GCC growth and realise the potential of 'Secure in India' is crucial. Policymakers are, therefore, working towards enhancing policies

to make India an attractive destination for global organisations and GCCs. Similar to the recently announced relaxation in Department of Technology (DoT) – Other Service Providers (OSP) guidelines, other policy areas which may be relevant to cyber GCCs include Software Technology Parks of India (STPI) and Special Economic Zone (SEZ) related acts, cybersecurity policy, data privacy and data localisation regulatory requirements

- The academic and start-up ecosystems are key drivers for the establishment and expansion of cyber GCCs. Recent initiatives for government backed start-up accelerator programs as well as focus on cybersecurity courses in institutions will go a long way in attracting cyber GCCs

- There is also an opportunity to give greater recognition to cyber GCCs. This can be achieved by strengthening the Cyber GCC brand in India and highlighting both national and global efforts. Major summits such as the World Economic Forum (WEF), and other such platforms/events may be explored.

5. Start-ups:

- Start-ups can partner with cyber GCCs to solve specific problems which are a priority for global organisations. This would not only increase start-ups' reach but also help them tap into the global market.

6. Academia:

Cyber GCCs and the world of academia have the chance to cultivate a strong symbiotic relationship.

- There is an opportunity for academic institutions to align their course curriculum with industry practices

- There are also myriad opportunities for joint research, virtual internships and co-development of products

- Academic institutions can encourage participation from cyber GCCs in leadership development programmes. They can also help cultivate a robust talent pipeline. This would help address in-demand and future oriented cybersecurity and digital risk skills.

As the dust settles on a turbulent year for businesses around the world, cyber GCCs have helped effectively navigate the fallout from this crisis, playing a key role in enabling their parent organisations. It is, however, essential that cyber GCCs continue to evolve as this new normal emerges. And this will depend on how effectively stakeholders across the business, policy and academic ecosystems capitalise on the opportunities that will arise as the risk landscape changes.
(*Manoj Kumar, Sanjana Poddar, Sangram Keshari Rout, Divya Mishra, Sushmita Karmakar and Karanveer Singh Chawla have contributed to this article*)