Tracing the rise of GCCs in India as cybersecurity powerhouses

pwc

Global capability centres (GCCs) in India are increasingly transforming into cybersecurity centres of excellence (CoEs). **Manu Dwivedi** outlines strategies that could help augment their cybersecurity offerings.

In the next four years, the global cost of cybercrime is expected to rise substantially – from USD 9.22 trillion in 2024 to USD 13.82 trillion by 2028.[1] India, despite being the most targeted country for cyberattacks and facing 13.7% of all such attacks, is emerging as a key player in the global cybersecurity landscape.[2] The country's thriving technology industry, proliferation of innovative startups, and skilled talent pool have ensured that it holds centre stage when it comes to cybersecurity. Around 28% of global organisations have more than half of their cybersecurity teams in India, and 17% of them have over 75% of their teams in India.[3]

From conventional GCCs to cybersecurity CoEs

Bolstering India's prowess in cybersecurity are GCCs that are fast transitioning from conventional centres of operational support to bastions of cybersecurity excellence for their parent organisations. This evolution is not only reshaping the GCC landscape but also underscoring India's growing presence in cybersecurity on the global stage. Availability of IT talent, cost efficiency and proximity to key markets have made GCCs in India the top choice for multinational companies to set up their cyber CoEs. Operating across all service lines – IT services, BPO, engineering services and software product development – GCCs in India have gone up the value chain by delivering complex work.[4] In the last couple of years, more than 150 multinationals have set up their GCCs in India.[5]

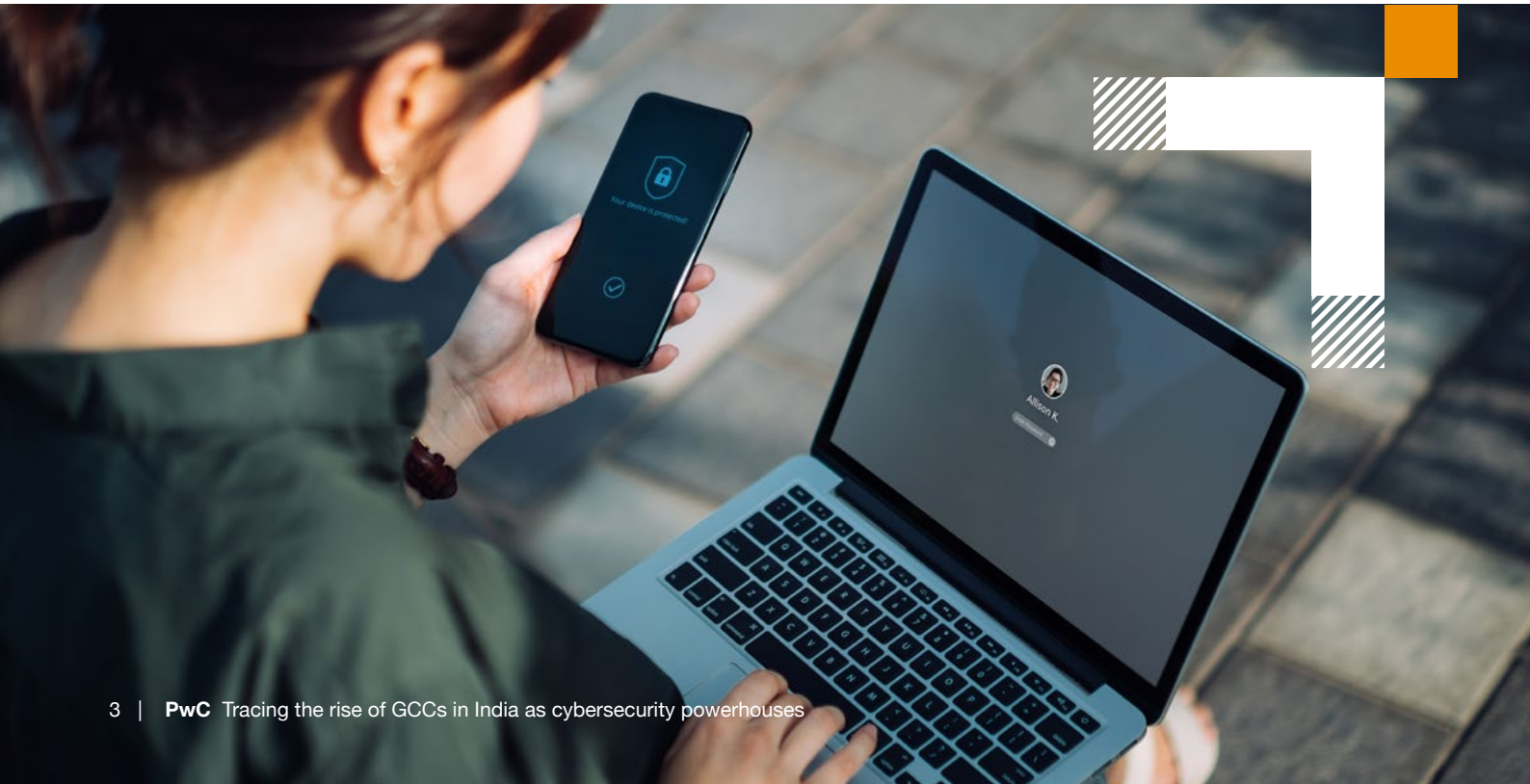
Of these, several have emerged as trailblazers in the realm of cybersecurity, offering a diverse array of services tailored to the needs of their parent organisations. These services encompass threat detection and response, vulnerability assessment, penetration testing, security operations centre (SOC) management, risk assessments and incident response. These GCCs collaborate closely with their parent companies and stakeholders to devise bespoke cybersecurity solutions, leveraging their deep domain expertise and technological prowess. At the forefront of technological innovation, they harness emerging technologies such as artificial intelligence (AI), machine learning (ML), blockchain, and quantum computing to bolster their cybersecurity capabilities, protect against digital threats, and help proactively identify and neutralise evolving cyberthreats, thereby safeguarding critical assets and ensuring business continuity for their parent organisations and clients.

1. Statista, Cybercrime to skyrocket
2. State-sponsored cyberattacks against India up 278% in three years
3. 70% GCCs have large security teams in India
4. PwC, Six imperatives to scale up the GCC market in India
5. Nasscom and Zinnov. India-redefining-globalization-blueprint

By 2025, the country is poised to have 1,900 GCCs with the market size touching USD 60 billion.[6] Many of these offshore centres are likely to emerge as hubs for cyber leadership, resilience and innovation. Existing GCCs, too, are diversifying their portfolio to include cybersecurity services. The key factors driving the rise of GCCs in India as cybersecurity nodes include:

- **Government policies promoting cybersecurity:** India has established robust regulatory frameworks governing data protection – such as the recent Digital Personal Data Protection (DPDP) Act, 2023 – and cybersecurity, providing GCCs with a secure operating environment. Compliance with international standards and regulations is facilitated by India's adherence to best practices in cybersecurity governance. Based on global best practices, the Government has drawn up a framework that sets the cybersecurity standards in India. The National Cybersecurity Reference Framework (NCRF) aims to provide clear guidelines on roles and responsibilities for cybersecurity based on existing rules and regulations.[7] It also recommends that enterprises allocate at least 10% of the total IT budget to cybersecurity.[8] Besides, there are several other initiatives that aim to promote cybersecurity awareness in the country. For instance, the Ministry of Electronics and Information Technology (MeitY) has joined hands with technology players to focus on cybersecurity training and skill development among government officials.[9]
- **Cost efficiency:** Establishing a GCC in India offers significant cost advantages compared to setting up similar operations in developed countries. Lower labour costs, favourable exchange rates and government incentives make India an attractive destination for companies seeking to optimise their cybersecurity investments.
- **Enhanced infrastructure:** Metropolises such as Bengaluru, Hyderabad and Pune are renowned for their world-class technology parks and infrastructure facilities. GCCs leverage this infrastructure to establish secure data centres, testing labs, and innovation hubs dedicated to cybersecurity research and development.
- **Availability of talent:** India boasts a large pool of highly skilled professionals in cybersecurity, owing to its robust education system and emphasis on science, technology, engineering and math (STEM) disciplines. At 25–27%, the demand and supply gap in India's technology talent is the lowest among the global technology leaders, including the US, Australia and the UK.[10] GCCs are leveraging this talent pool to build world-class cybersecurity teams capable of addressing complex threats.

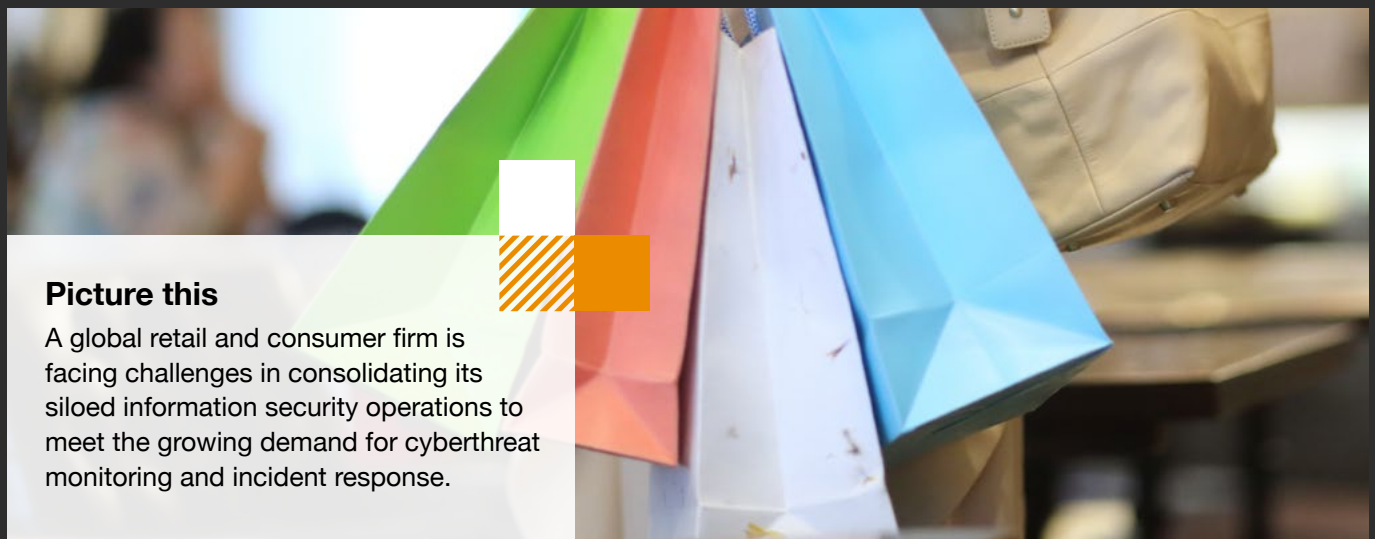
6. Nasscom and Zinnov. GCC 4.0 | India redefining the globalization blueprint
7. Overhaul of cybersecurity framework
8. Centre may push enterprises to use security products developed in India
9. Cybersecurity workforce in India
10. Nasscom, India tech industry digital talent demand and supply 2023



Setting up guardrails

The following use cases demonstrate how GCCs can fulfil their parent organisation's cybersecurity requirements. They showcase the value of global collaboration and of leveraging India's talent pool and resources to drive innovation, enhance security capabilities, and deliver cost-effective solutions.

Establishing an SOC



Picture this

A global retail and consumer firm is facing challenges in consolidating its siloed information security operations to meet the growing demand for cyberthreat monitoring and incident response.

Proposed solution

The firm could tap its India-based GCC to establish a dedicated SOC to support the following cybersecurity requirements of its parent company.

- **Talent acquisition:** The GCC could tap into India's vast talent pool by recruiting cybersecurity professionals with expertise in threat intelligence, network security and incident response.
- **Infrastructure development:** The SOC could be equipped with advanced monitoring tools, threat detection software, and a secure communication network to enable real-time monitoring and response to security incidents.
- **24/7 monitoring:** The SOC could operate round-the-clock, continuously monitoring the parent company's systems and networks for suspicious activities or potential threats.
- **Incident response:** In the event of a security incident, the India-based SOC could collaborate closely with the parent company's IT security team to investigate, contain and remediate the threat promptly.

Possible benefits

- **Enhanced threat detection:** The establishment of the global SOC in India and centralised cyberthreat monitoring and incident response services could significantly improve the parent company's ability to detect and respond to cybersecurity threats in real time.
- **Cost savings:** By leveraging India's cost-efficient resources, the GCC could achieve operational efficiency and cost savings in managing the SOC operations.
- **Improved security posture:** The proactive monitoring and incident response capabilities of the SOC could strengthen the overall security posture of the parent company, reducing the risk of data breaches and downtime.

Collaborating around cybersecurity research and development

Picture this

The India GCC of an automotive company would like its India R&D team and the parent company's cybersecurity experts to strengthen collaboration to drive innovation and product development.

Proposed action

- **Cross-team collaboration:** The GCC's India R&D team could work closely with the parent company's cybersecurity experts to identify emerging threats, assess security vulnerabilities and develop proactive defence strategies.
- **Innovation workshops:** Regular innovation workshops and brainstorming sessions could be conducted to bring together engineers and cybersecurity professionals from both teams to exchange ideas and explore new approaches to cybersecurity challenges.
- **Prototype development:** The collaborative effort could result in the development of prototype solutions for threat detection, malware analysis, and security automation, leveraging India's expertise in software development and the parent company's domain knowledge in cybersecurity.

Possible benefits

- **Accelerated product development:** The collaboration between the GCC's India R&D team and the parent company's cybersecurity experts could accelerate the development of innovative cybersecurity solutions, bringing new products to market faster.
- **Competitive advantage:** By leveraging India's talent pool and R&D capabilities, the GCC could gain a competitive advantage in offering cutting-edge cybersecurity solutions tailored to the evolving threat landscape.
- **Knowledge sharing:** The collaboration could foster knowledge sharing and skill development among team members, enhancing the collective expertise of both India and parent company teams in cybersecurity R&D.

Setting up unified threat and vulnerability management (TVM) operations

Picture this

The GCC of a multinational technology company based in India needs to improve the efficiency and effectiveness of its TVM services for its parent organisation. The parent organisation previously operated TVM services in silos across different regions, leading to inefficiencies and gaps in coverage.

Proposed action

The GCC could establish unified TVM services for the parent organisation, consolidating fragmented operations into a centralised and coordinated approach that includes:

- **Comprehensive assessment:** The GCC could conduct a thorough assessment of the parent organisation's existing TVM processes, tools and resources across different regions to identify gaps and opportunities for improvement.
- **Standardisation of processes:** Based on the assessment findings, the GCC could develop standardised TVM processes, procedures and workflows to ensure consistency and efficiency across all regions. This would include defining clear roles and responsibilities, establishing escalation procedures and implementing standardised reporting mechanisms.
- **Centralised tools and platforms:** The GCC could implement centralised TVM tools and platforms to enable real-time visibility into the organisation's entire IT infrastructure, including on-premises, cloud and hybrid environments. This can allow for centralised vulnerability scanning, assessment and reporting capabilities.
- **Skill development and training:** The GCC could provide training and skill development programmes for TVM personnel across different regions to ensure that they are equipped with the necessary knowledge and expertise to perform their roles effectively. This could include training on the latest threat intelligence, vulnerability assessment techniques and remediation strategies.
- **Continuous monitoring and reporting:** The GCC could establish a centralised monitoring and reporting framework to track vulnerabilities, prioritise remediation efforts, and provide regular updates to senior management and stakeholders. This could include the implementation of key performance indicators (KPIs) and metrics to measure the effectiveness of TVM activities.

Possible benefits

- **Improved visibility and control:** The establishment of unified TVM services could provide the parent organisation with comprehensive visibility into its entire IT infrastructure, enabling better prioritisation of vulnerabilities and more effective risk management.
- **Streamlined operations:** Standardised processes and centralised tools could streamline TVM operations, reducing duplication of efforts, eliminating silos and improving overall operational efficiency.
- **Enhanced security posture:** The GCC's proactive approach to vulnerability management and continuous monitoring could help the parent organisation identify and remediate vulnerabilities more effectively, reducing the risk of cyberthreats and data breaches.
- **Cost savings:** By consolidating TVM operations and leveraging centralised resources, the parent organisation can achieve cost savings through utilisation of improved resources and reduced overheads.

These use cases show how GCCs may effectively utilise their India operations to mitigate cyber risks for their parent companies while tapping into India's talent pool and resources to drive innovation.

Enabling GCCs to expand their cybersecurity offerings

While GCCs in India have long been recognised for their contributions to various business functions, including IT, finance, research and development, and customer support, many are considering expanding their offerings to include cybersecurity services. The following are select strategies a GCC may consider prior to providing cybersecurity services:

Assess the parent organisation's cybersecurity requirements: The first step to be taken by a GCC that considers venturing into cybersecurity services is to conduct a comprehensive analysis of its organisation's global demand. The GCC should understand the cybersecurity challenges faced by the parent organisation and target clients, and identify emerging trends, regulatory requirements, and customer preferences to gauge the demand for cybersecurity services in their target markets.

Focus on a strategic roadmap: Once the market demand is assessed, the GCC could develop a strategic roadmap outlining the steps needed to establish cybersecurity services within the centre and leverage the benefits offered by the Indian ecosystem. It should define clear objectives, timelines, and resource requirements for the initiative as well as identify key stakeholders and secure buy-in from senior management to ensure alignment with organisational goals. Starting small with proofs of concept (PoCs) could be a better idea for fostering confidence in the parent organisation.

Develop skilled talent: GCCs looking to provide cybersecurity offerings would require a competent cybersecurity workforce. Currently, India has a shortage of 8 lakh cybersecurity professionals against a global shortage of four million.[11] Redirecting India's digitally skilled workforce to cybersecurity through training programmes, certifications, and career development opportunities can help plug this gap.

Establish strategic partnerships: GCCs that want to enhance their cybersecurity offerings should forge strategic partnerships with cybersecurity vendors, technology providers, academia, and industry associations so that they can capitalise on innovative solutions, share best practices, and stay up-to-date with the latest trends in the cybersecurity domain.

Invest in infrastructure and technology: The cybersecurity landscape demands rapid innovation and adaptation to outpace threats such as ransomware and malware. Therefore, GCCs should invest in developing the right infrastructure by establishing secure data centres, testing labs, and innovation hubs dedicated to cybersecurity research and development.

Prioritise regulatory compliance: GCCs planning to venture into cybersecurity offerings need to stay abreast of evolving regulatory requirements and compliance standards. For instance, GCCs often handle sensitive data and need to prioritise data protection to stay compliant with the DPDP Act which is in line with global cybersecurity and data protection standards.

Emphasise the value proposition: GCCs should develop case studies, success stories, and industry certifications to showcase their cybersecurity capabilities and expertise to parent organisations and stakeholders.

Customer centricity: While GCCs work for their parent organisations, they must adopt a customer-centric mindset, viewing their parent organisation as clients and customise cybersecurity offerings to meet their unique requirements. GCCs should proactively engage with clients, conduct regular assessments and offer tailored solutions to tackle their cybersecurity challenges.

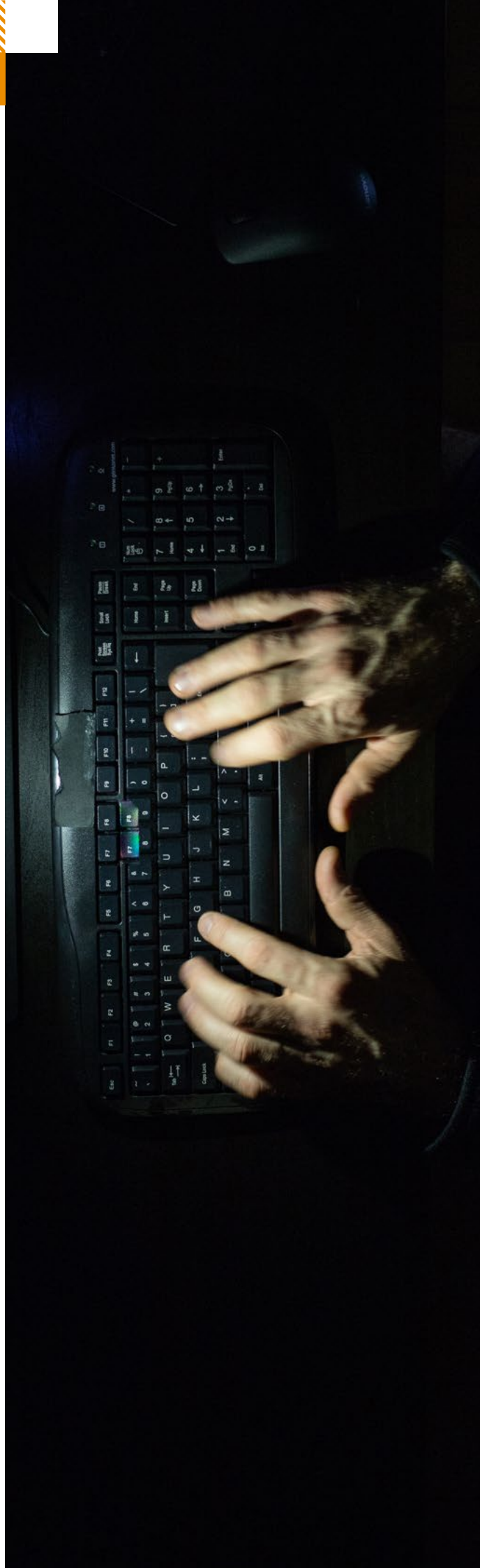
11. India has a shortage of cybersecurity professionals

Looking ahead

As the demand for cybersecurity solutions grows, exciting opportunities will be unlocked for GCCs exploring cybersecurity services. By adopting a customer-centric approach that also includes market evaluation, strategic alliances, robust training and upskilling programmes, infrastructure development investment, and regulatory conformity, GCCs can establish themselves as top cybersecurity providers. Below are some key trends that will define the journey of GCCs to cyber leadership in the country:

- **Increasing demand:** The demand for cybersecurity services is rising globally as well as in India, with the country reporting at least 40,000 job vacancies in the cybersecurity domain in May 2023.[12] GCCs that are able to tap into the rise in demand by offering a range of cybersecurity solutions will sprint ahead of the competition.
- **Expansion of cybersecurity services:** Service offerings by GCCs are likely to expand to include not just traditional functions such as threat detection and incident response, but also specialised services such as security analytics and compliance management.
- **Adoption of new technologies:** GCCs will harness AI, generative AI, ML and blockchain to drive innovation. Some GCCs have already established AI centres of excellence to design and implement AI solutions.[13]
- **Innovation hubs:** GCCs in India will drive cybersecurity innovation within their parent organisations. Knowledge exchange through collaborations with R&D teams, academia and industry partners will put GCCs at the forefront of technological innovation.
- **Upskilling and talent development:** GCCs will invest in upskilling and talent development programmes to groom the next generation of cybersecurity talent. They are likely to offer cybersecurity training programmes, certifications, and internship opportunities in collaboration with industry partners and academia.

By leveraging a favourable business environment, technology prowess and a skilled talent pool, GCCs in India are poised to emerge as global leaders in cybersecurity. Offshore centres will continue to shape the future of cybersecurity with a laser focus on collaboration, innovation and continuous improvement that will enable businesses to navigate the complex cybersecurity landscape with confidence and resilience.



12. India witnesses demand for cybersecurity jobs
13. When GCCs and AI merge

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Manu Dwivedi
Partner and Leader - Cybersecurity and Risk Consulting, GCC
PwC India
manu.dwivedi@pwc.com

Rajesh Ojha
Partner and Leader - GCC Market Segment
PwC India
rajesh.ojha@pwc.com

Editorial team:

Vishnupriya Sengupta, Dion D'Souza and Ruchika Uniyal

pwc.in

Data Classification: DC0 (Public)

HS/May 2024 - M&C 37311