



Secure in India 2023

GCC empowered global cybersecurity
and digital risk management

nasscom



December 2023

kpmg.com/in

Contents

1

GCC cybersecurity organisation

12

- Why global organisations invest in cyber GCCs¹?
- Why cyber GCC leaders are key for global cybersecurity?
- What functions cyber GCCs deliver?

2

Cybersecurity talent, Diversity, Equity, and Inclusion (DE&I)

20

- Do cyber GCCs continue to have required depth and breadth of cyber skills?
- Do cyber GCCs continue to acquire and retain talent?
- Do cyber GCCs contribute to DE&I agenda?

3

Securing digital transformation

26

- How cyber GCCs foster innovation culture?
- Do cyber GCCs leverage emerging technologies?
- Key use cases for innovation and leveraging emerging technologies

4

Cyber risk culture

38

- Cyber GCCs identify, manage and report risks
- What keeps cyber GCC leaders awake?
- Key initiatives cyber GCCs undertake to promote risk culture

GCC – Global Capability Centre

1. 'Cyber GCC' refers to teams focused on global cybersecurity delivery, located within respective GCCs in India

5**Together for better****46**

- Why and how cyber GCCs collaborate with their ecosystem?

6**Cyber GCCs in a Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) World****52**

- 'Defense in depth' through 'Cyber Fusion Centres'
- 'Cyber insurance' enabled cyber GCCs
- Are cyber GCCs privacy ready?

7**Methodology****60****8****Acknowledgements****61**

Foreword

Today, we are in a world dealing with geopolitical conflicts, supply chain disruptions, economic uncertainties, continued emergence of digital, operational, and advanced technologies, especially with the rise of Artificial Intelligence (AI). These global events continue to have a ripple effect on the global business ecosystem, pose unforeseen challenges and provide opportunities to transform.

'Trust' in business is a key 'asset' for organisations and is vital to build and protect trust in the world challenged with above events. With rampant digitisation, data is a foundational block for competitive advantage and global organisations are tapping the data to provide transformative experience to their customers. However, cyber criminals are ahead of the curve in proactively leveraging advanced technologies, including AI, in exploiting weaknesses of global organisations impacting the 'trust', 'data' and other valuable assets. Within this ecosystem, where digitisation meets the challenge of safeguarding business assets, global organisations continue to embrace and expand cyber GCCs in managing cybersecurity and digital risks.

Today, cyber GCCs are seen as value generating entities and hubs of cyber leadership, diverse cybersecurity talent, and excellence. They drive global cybersecurity and digital risk management employing innovation, resilience, adaptability, DE&I and business growth agenda propelling these as cyber-Centres of Excellence (CoE). Cyber GCCs are not only about 'protection' but also focus on 'anticipation', 'collaboration', 'unlocking horizontal value' and 'enabling business growth'.

The 'Secure in India' report, in its previous editions, provided global leadership with a viewpoint on cyber GCCs capabilities, leading practices, innovation, talent, and ecosystem. This edition of 'Secure in India' focuses on how cyber GCCs are empowering their global organisations deal with cybersecurity and digital risks, including new business and digital technology models.

The insights detailed in this report have been prepared based on an extensive study and in consultation with global cyber leaders, cyber GCC leaders, cybersecurity Subject Matter Experts (SMEs) and reputed industry bodies. It provides key recommendations for cyber GCCs to help them sustain competitive advantage, transform into global 'centres of expertise' and enable global organisations to 'Secure in India'.



Atul Gupta

Partner and Head
Digital Trust, KPMG in India



KS Viswanathan

Vice President, Industry
Initiatives, nasscom



Vinayak Godse

CEO, Data Security
Council of India (DSCI)

Industry view

GCCs have emerged as transformation partners for their global organizations by 'building trust', 'strengthening resilience' and 'exceeding outcomes' across key business growth drivers. GCCs continue to strive for excellence by not only improving in existing business services and technologies but also deliver on innovation and growth agenda.

Cyber GCCs are a source of strategic advantage to global organizations, as they enable various businesses to 'protect, adapt, scale and innovate'. Cyber GCCs continue to expand their contribution across cybersecurity and digital risk functions, proactively their global organizations deal with uncertainties across geopolitical, regulatory, dynamic business, technology, and social landscape.

Cyber GCCs help in nurturing talent, sustain, and develop skills, contribute to improved business practices including DE&I agenda. It's heartening to experience new generations of talent learn, integrate and contribute to the global business ecosystem through cyber GCC platform.

As cyber GCCs gather momentum in dealing with new business models powered by technology advancements (e.g., AI, crypto, operational technology etc.), global organizations have both accountability as well as significant opportunity in contributing to the entire world through empowering Cyber GCCs and helping them reach their fullest potential.



Ramachandra Kulkarni

Managing Director, Technology Risk,
Goldman Sachs

Global view

Organisations across industries and geographies are increasingly relying on digital technologies. With this reliance comes the challenge of protecting networks and data from cyber threats, thus highlighting the critical need for skilled cybersecurity professionals.

Despite the global cybersecurity workforce growing by an estimated 10 per cent between 2022 and 2023, a deficit of almost four million cybersecurity professionals remains. India is no exception to this trend. In May 2023, there were an estimated 40,000 job openings for cybersecurity professionals, yet due to talent shortages, 30 per cent of these vacancies could not be filled.

To tackle the workforce gap, organisations must proactively invest in attracting, training, and retaining cybersecurity workers. Failure to do so can have far-reaching consequences with organisations finding themselves understaffed in the face of emerging threats. In fact, today, 64 per cent of cyber leaders rank talent-related challenges, such as recruitment and retention, as key obstacles to managing organisational cyber resilience. The deficit of cybersecurity professionals not only hampers an

organisation's ability to anticipate and respond to cyberattacks – including 1.3 million attacks reported across India in 2022 – but also poses serious implications for the economy and national security.

With one of the world's largest youth populations and boasting 31.7 per cent of Science, Technology, Engineering and Mathematics (STEM) graduates worldwide, India has the opportunity to position itself as a fertile ground for cultivating cyber talent. Ultimately, such assets coupled with India's emerging cybersecurity market, which is expected to reach a value of US\$13.6 billion by 2025, can help ensure a continuous pipeline of skilled professionals and position the country as a global leader in cybersecurity for years to come. In this pursuit, GCCs in India have a key role to play as they provide organisations across the world with a platform to access talent, skills and innovation. In the coming years, these GCCs have the potential to grow up the value chain and strengthen resilience across the global business ecosystem.



Akshay Joshi

Head of Industry and Partnerships, Centre for Cybersecurity, World Economic Forum

Government view

Securing Digital India

“

Cybersecurity is no longer confined to the digital world only. It has become a subject of national security – global security.

”

एस. कृष्णन, आई.ए.एस.
सचिव
S. Krishnan, I.A.S.
Secretary



इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार
Ministry of Electronics &
Information Technology (MeitY)
Government of India

MESSAGE

Cyber security has emerged as a key pillar of business growth, innovation, and advanced technology adoption, globally. We are in an era where digital advancements are transforming the landscape across sectors and especially within global organisations who has their capability centers operating out of India. There is an immediate need to move at a faster pace in this area to ensure security considerations are embedded in the emerging areas such as but not limited to 5G, Artificial Intelligence, Machine Learning, Non-Fungible Tokens (NFT), Metaverse, Blockchain, Internet of Things, Drone technology, Virtual Reality, Augmented Reality, Robotics and Automation and 3D Printing. These tech trends are expected to have a significant impact on various industries and daily life which have the potential to revolutionize the way we work, communicate, and interact.

The Government of India and Ministry of Electronics and Information Technology (MeitY) are committed to make India a global hub and preferred destination for Cyber GCCs. Cyber GCCs are at cusp of a very interesting phase of digital transformation. Over the period, Cyber GCCs have moved from cost arbitrage to value arbitrage.

A collaborative approach involving Cyber GCCs, industry bodies (nasscom, DSCI), Government, startups, Academia, and Law enforcement to share and adopt leading best practices is imperative for the nation. GCCs in India are set to grow manifold and it's an opportunity for all of us to join hands and 'Secure in India'.


(S. Krishnan)

Dated: 15.12.2023
Place: New Delhi



इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्प्लेक्स, नई दिल्ली-110003 / Electronics Niketan, 6, C.G.O. Complex, New Delhi-110003
Tel. : 011-24364041 • email : secretary@meity.gov.in



Key Takeaways

01



Global organisations continue to invest in cyber GCCs to manage cybersecurity and digital risks

- Top five drivers to establish cyber GCCs include - availability of cybersecurity skills (86 per cent), cost arbitrage (75 per cent), round the clock delivery (75 per cent), cyber innovation, research and development (58 per cent) and proximity with other business functions (53 per cent)
- About 28 per cent of global organisations surveyed have more than half of their global cybersecurity teams in cyber GCCs. This has doubled since 2020. About 70 per cent of respondents have cybersecurity teams with over 25 resources in India
- About 89 per cent of cyber GCC CISOs participate in global committees governing cybersecurity. 67 per cent of the organisations surveyed have cybersecurity team members across global locations reporting to cyber GCC leadership.

02



Cyber GCCs emerge as global cybersecurity skills hub

- Maximum increase in cyber skill demand is noted for cloud security (81 per cent), followed by third party risk management (78 per cent), cybersecurity risk assessments (75 per cent), technology regulatory compliance and standards management (75 per cent) and secure development (69 per cent)
- Cyber GCC attrition challenges continue, with compensation, market demand for similar skillsets and locational preferences reported as top three challenges in retention of cyber talent. Remote working, since covid, continues to play a role in locational preference shifting to hometown
- Most cyber GCCs have DE&I agenda focused on cybersecurity with top three initiatives as targeted recruitment (22 per cent), DE&I training and awareness (22 per cent) and inclusion and sustenance at various leadership levels (20 per cent).

03



Cyber GCCs focus on culture of innovation to manage risks effectively

- Most of the organisations surveyed are leveraging emerging technologies for cybersecurity, including cloud (81 per cent), Robotic Process Automation (RPA) (56 per cent), AI and Machine Learning (ML) (39 per cent) and low code and no code (33 per cent)
- Significant interest has been noted in Generative AI for cybersecurity, across various functions including security operations, third party risk management, vulnerability management, risk and control assessments etc.
- The top three innovation programs leveraged by cyber GCCs include incubation events, hackathons, bug bounty programs, implementation of focused innovation programs and idea-based investments.

04



Cyber GCCs foster risk culture and risk transparency

- Most cyber GCCs are helping their global organisations identify, assess, remediate, track and report cybersecurity risks to their global boards. The top five cybersecurity risks reported to the global boards include third party cybersecurity risk, software supply chain security risk, cyber regulatory risk, endpoint security risk and cloud security risk
- Preferred methods of cybersecurity risk reporting include cybersecurity dashboards, periodic cybersecurity governance meetings, periodic cybersecurity posture reporting and cyber risk quantification. About 44 per cent still utilise manual Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) reporting
- Key programs to promote cybersecurity risk culture in cyber GCCs include cybersecurity training and awareness, recognition/incentivisation and gamification/simulation/bug bounties.

05



Global organisations trust cyber GCCs across three lines of defense

- About 78 per cent of cyber GCCs are unlocking horizontal value as teams across their three Lines of Defense (3LoD) actively collaborate for managing cybersecurity and digital risks
- Cyber GCCs belonging to sectors such as technology, telecom, energy etc., have established 3LoD approach to cybersecurity and digital risk management, as well, beyond financial services
- Top five cybersecurity functions based on budget prioritisation include-cybersecurity risk assessments, technology regulatory audit and standards compliance management, cybersecurity engineering, product management and automation, third party risk management and secure development.



GCC cybersecurity organisation



Global organisations have been focusing on managing cybersecurity and digital risks. They continue to invest in and expand cyber GCCs, elevate cyber GCC leadership and talent, harness innovation and scale offered by the cyber GCCs.

As cyber GCC organisations mature, expectations are not only to manage risks effectively but also to enable global organisations innovate, grow and sustain their businesses through continued, proactive and

scalable cybersecurity and digital risk management capabilities.

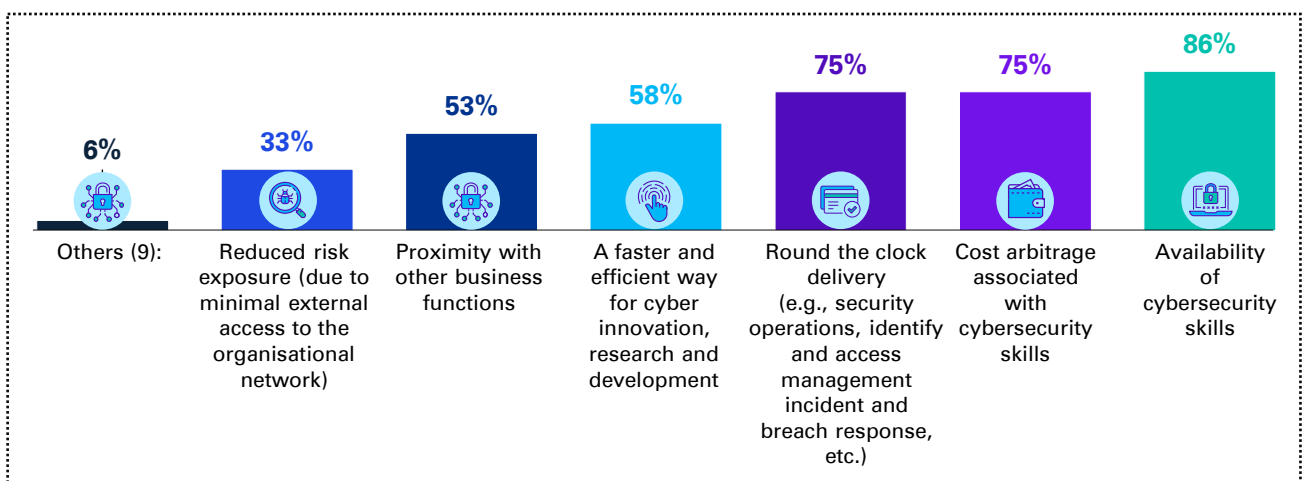
As global leaders seek agile and affordable cybersecurity strategies that integrate seamlessly, cyber GCCs are helping their global organisations meet their key business objectives. By spearheading the delivery of diverse portfolios, cyber GCC organisations are playing a vital role in empowering global cybersecurity and digital risk management.

#1 Cyber GCCs empower global cybersecurity and digital risk management



While these continue to be key drivers in setting up and expanding cyber GCCs, faster and efficient cyber innovation, Research and Development (R&D), proximity with other business functions and reduced risk exposure (due to minimal access to the organisational network) are emerging as significant factors for leveraging the GCC model.

Figure 1: Key drivers to leverage GCC model for cybersecurity



#2 The growth trajectory of cyber GCCs

The surge in cyber GCCs over the last seven years can be attributed to a combination of factors including significant rise in cybersecurity and digital risks associated with continued digitisation, new business models, rise in advanced technologies and increasing expansion of talent pool in the cybersecurity domain. This has led to about 23 per cent increase in cyber GCCs since 2020, with global organisations strategically choosing to establish their presence in cyber GCCs, capitalising on its ecosystem for technological innovation and cybersecurity talent.



Figure 2: Year of inception of cybersecurity functions in India GCCs

Year of establishing Cyber GCC in India		
Before 2008	2008-2015	2016-2023
13%	32%	55%
% of Cyber GCCs established in India		

#3 Cyber GCCs in India emerge as a global cybersecurity hub

Cyber GCCs witness a significant increase in team size. About 28 per cent of global organisations have more than half of their global cybersecurity team strength in India. This growth reflects cyber GCCs prominence as a strategic hub for cybersecurity and digital risk management.

Figure 3: Per centage of global cybersecurity team strength in cyber GCC

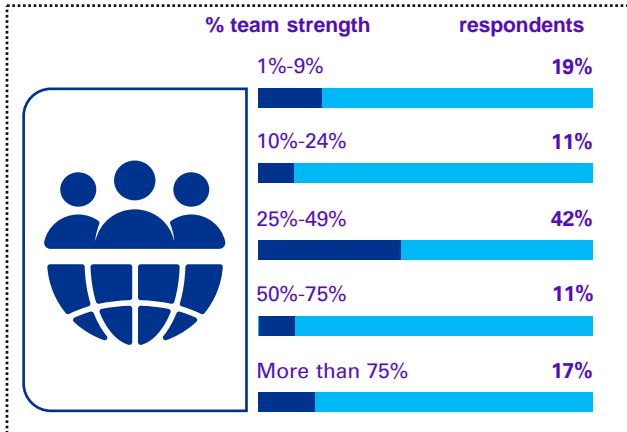
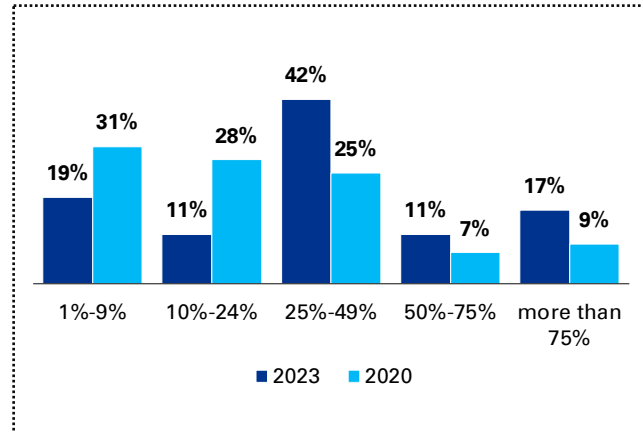


Figure 4: Growth in Cybersecurity team strength



With increased digitisation, the need for managing cybersecurity and digital risks is on the rise. GCCs in India have gained the confidence of their global parent organisations based on cyber GCCs focus on nurturing niche and specialised cybersecurity talent and developing digital risk skillsets.

Pranav Kathale, Partner, Digital Risk and Cloud Security, KPMG in India



#4 Cyber GCC leadership accountability is on the rise

As cybersecurity and digital risk functions are increasingly delivered from cyber GCCs, accountability and influence of cyber GCC leadership has risen significantly. About 89 per cent of survey respondents highlighted cyber GCC leadership is part of the global committees managing cybersecurity and digital risks. About 67 per cent also highlighted that global teams are reporting into the cyber GCC leadership, signifying growing stature and importance of cyber GCCs to their global organisations.

Figure 5: Cyber GCC leadership participation in global committees

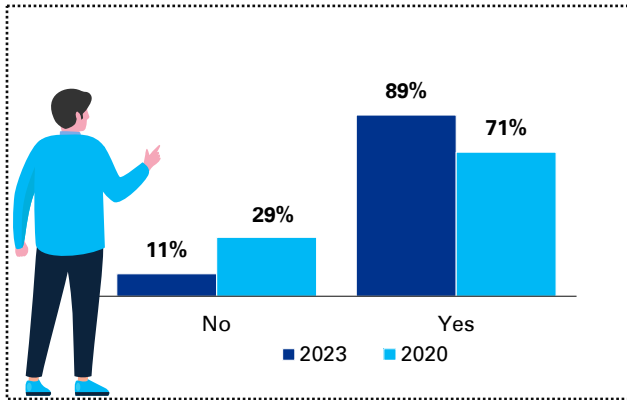
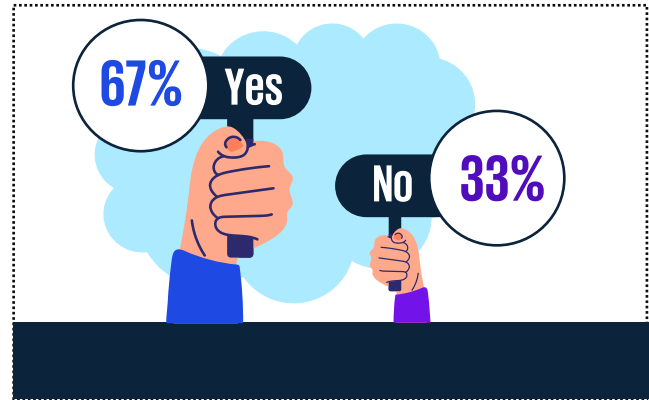


Figure 6: Global team reporting into cyber GCC leadership



Cyber GCC leadership has risen to the global challenge of growing cybersecurity and digital risks. They contribute to build and sustain a cyber risk culture, develop cybersecurity teams of scale and upgrade their skillsets on a continuous basis, and help advise global leadership on cybersecurity matters. They have become key for effective global cybersecurity and digital risk management.



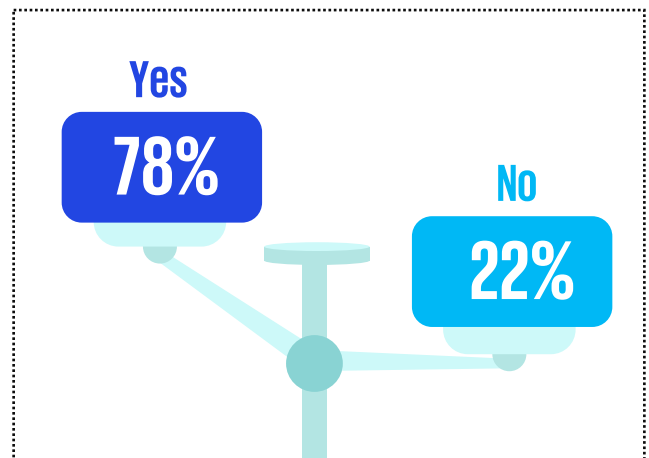
Srinivas Potharaju, Partner, Digital Risk and Cyber, KPMG in India



#5 Cyber GCCs fortify the three lines of defense

Majority of cyber GCCs follow three Lines of Defense (3LoD) approach to identify, manage, and monitor cybersecurity risks effectively and efficiently. More importantly, cyber GCCs are unlocking horizontal value, as teams across 3LoD are actively engaging and collaborating for managing cybersecurity and digital risks.

Figure 7: Adoption of 3LoD by GCCs



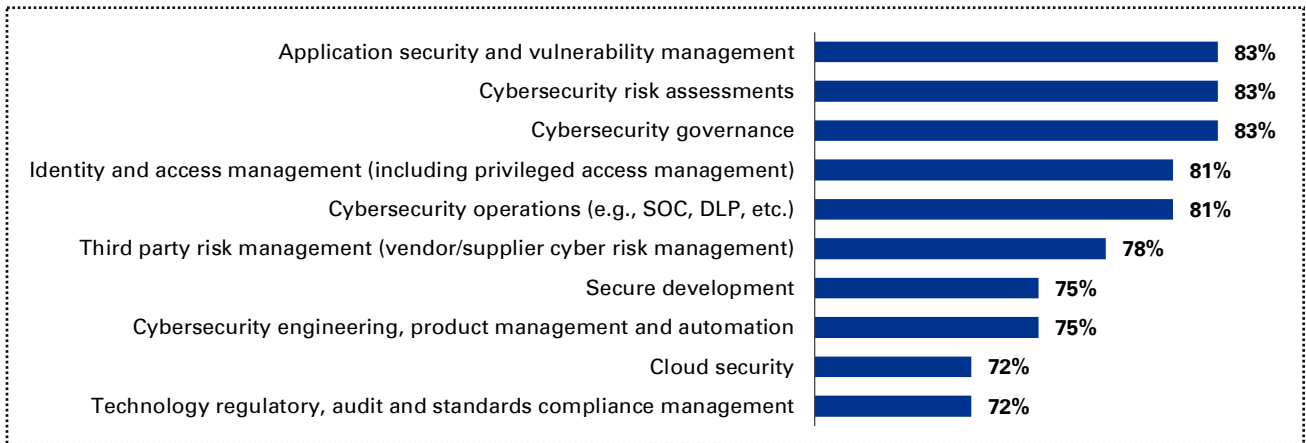
Cyber GCCs are playing an important role in modernising various cybersecurity activities and functions across the 3LoD, as they continue to operate with clear understanding of issues and changes needed.

#6 Core¹ grows further and 'emerging' functions surge

Top five cyber GCC functions include 'application security and vulnerability management', 'cybersecurity risk assessments', 'cybersecurity governance', 'Identity and Access Management (IAM)' and 'cybersecurity operations.' These form core of the cyber GCC contribution to managing cybersecurity risks and continue to grow significantly.

Cyber GCCs have experienced a significant increase in emerging functions such as cybersecurity engineering, product management and automation, secure development, cloud security and third party risk management including software supply chain security risk management.

Figure 8: Top 10 cybersecurity functions being delivered from cyber GCCs



Cyber GCC Case Studies



Risk assessment of emerging technologies: A leading energy GCC has developed a focused team to perform risk assessment of various emerging technologies such as drones, Distributed Ledger Technology/Blockchain (DLT), Low Code and No Code Platforms, RPA, Operations and Technology (OT) based applications, Internet of Things (IoT) based applications, AI based applications etc. This has resulted in greater understanding and appreciation of emerging technology risk, identification of suitable controls to manage the risk and enhanced awareness amongst user communities of corresponding emerging technology risk.

Third party risk signals: A leading telecom GCC developed a custom solution to monitor security risks from their third parties, through available risk intelligence platforms. Also, a leading pharma GCC has developed a Natural Language Processing (NLP) based solution to sift through third party data and identify risk signals, correlating with insights from their internal and external data sources.

GenAI risk and control framework: A leading energy major GCC has developed a GenAI risk and control framework and applied the same for all GenAI use cases. This has resulted in risk managing the innovative use cases, identifying new risks and helping develop suitable controls.

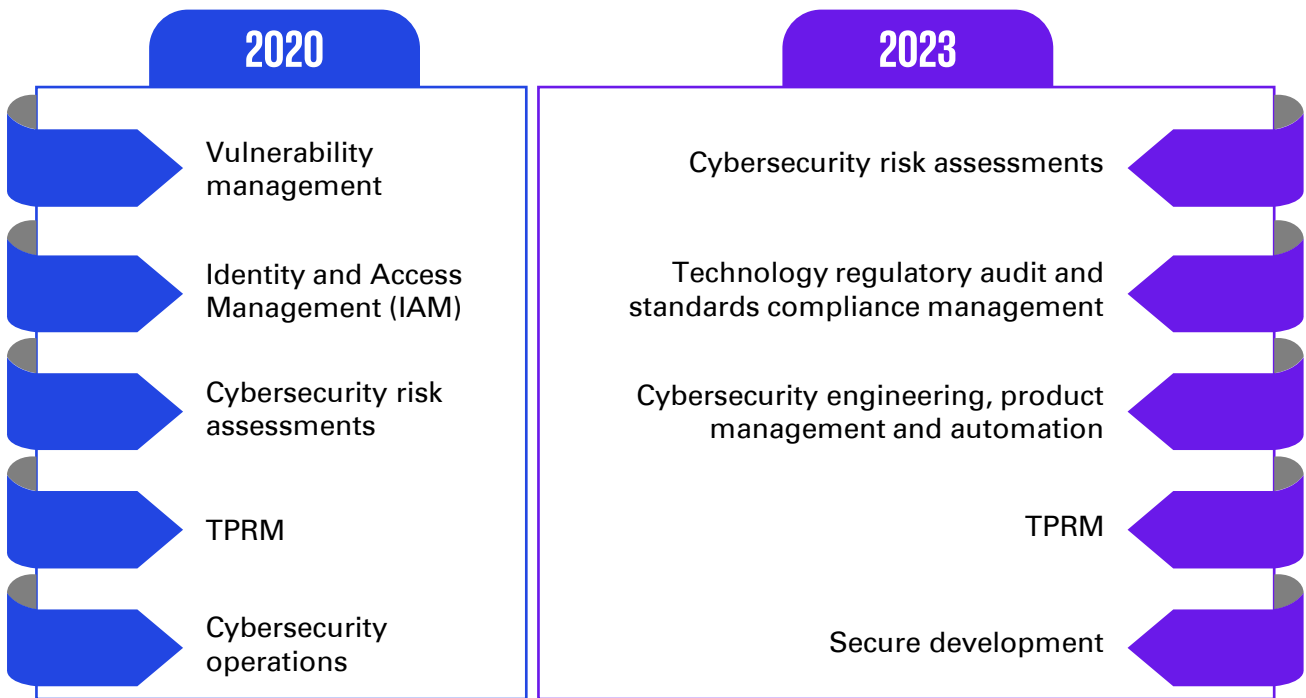
1. 'Core' functions refer to cybersecurity and digital risk functions which are on the rise and are being prioritised based on budget, compliance and necessity.

#7 Cyber GCCs continue to spend on 'core' and invest on 'emerging'

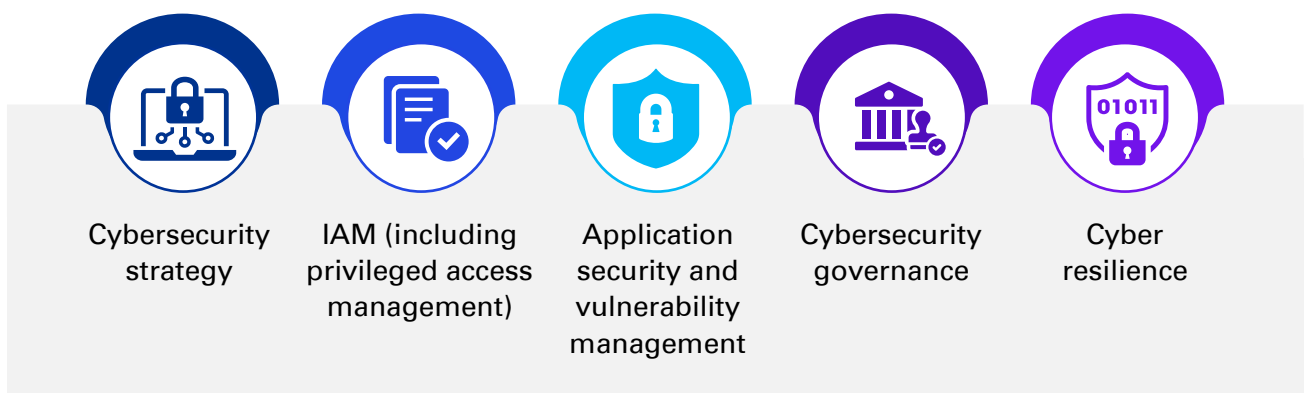
As digitisation footprint grows, proactive risk management caused by adoption of digital solutions, has resulted in, cybersecurity risk assessments, Third Party Risk Management (TPRM) and Technology, regulatory, audit and compliance management functions gaining substantial budgetary allocation.

'Shift left', 'digitisation of cybersecurity functions', 'tech for cyber' and 'continuous risk management' approaches have shaped greater focus on these functions, especially secure development and cybersecurity engineering product management and automation.

Top functions based on cybersecurity and digital risk budget prioritisation



In addition to the above mentioned, following are next five functions, basis budget prioritisation





Cyber GCC Case Studies

Automated Continuous Controls Monitoring (CCM) platform: A leading financial services GCC has built a CCM platform

- a. Which measures control effectiveness for entire population of control transactions, for each control, on a continuous basis
- b. Reports control effectiveness gaps, as and when they occur, through automated dashboard
- c. Auto assigns remediation actions to respective role-based action owners

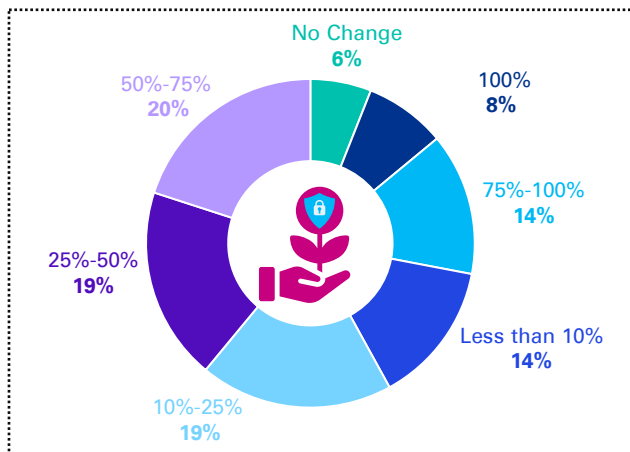
Controls across various control programs such as Sarbanes Oxley (SOX), International Standard on Assurance Engagements (ISAE), Risk and Control Self-Assessment (RCSA) etc. have been onboarded to the CCM platform

- d. Providing continuous coverage of control effectiveness measurement
- e. Reducing manual efforts involved in control testing
- f. Covering entire control transactions on an occurrence basis as against a sample on a periodic basis.

#8 Cyber GCCs reported exponential growth in cybersecurity delivery



Figure 9: Growth in cybersecurity services



About **94 per cent** of respondents have reported an increase in services delivered by cybersecurity functions, with more than **42 per cent** reporting about **50 per cent** increase.

No cyber GCC reported de-growth, highlighting continued expansion of cybersecurity functions across cyber GCCs, including a significant rise in emerging functions to manage digital risks.



Cybersecurity and digital risk functions growth in cyber GCCs reflects both the talent and initiative of cyber GCCs in delivering consistently and exceeding outcomes to their global organisations. Whether it's existing cybersecurity or emerging digital risks, cyber GCCs are working in tandem with their global counterparts to proactively manage the risks.



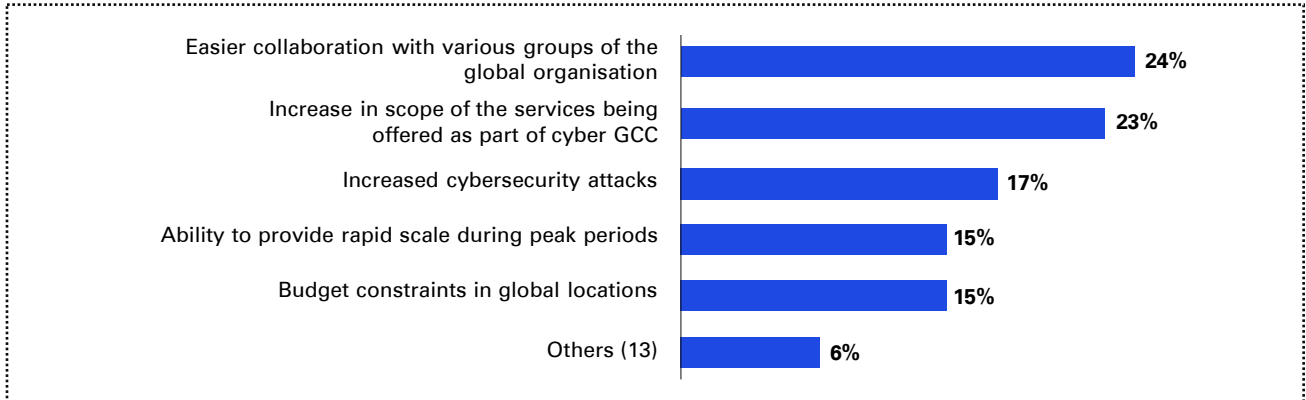
Akhilesh Tuteja, Head of Clients and Markets and Global Cybersecurity Leader, KPMG in India



#9 Cyber GCCs playing catalyst in managing cybersecurity debt

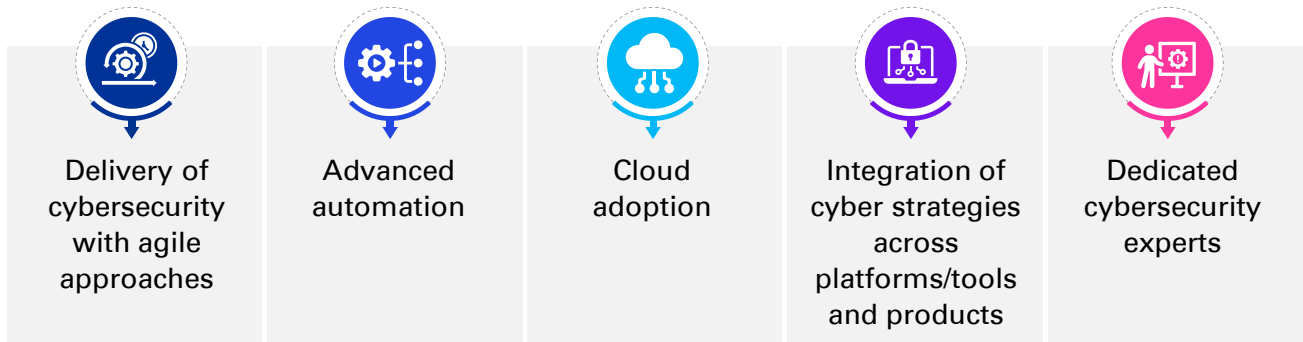
Cyber GCCs have become trusted advisors and partners for global organisations, helping them with the challenges and opportunities created by geopolitical tensions, supply chain disruptions, economic uncertainties, and the ongoing rise of digital, operational, and advanced technologies, especially AI. Their commitment to collaboration, innovation, and value delivery approach makes them an asset to the global organisations.

Figure 10: Growth factors of cyber GCCs



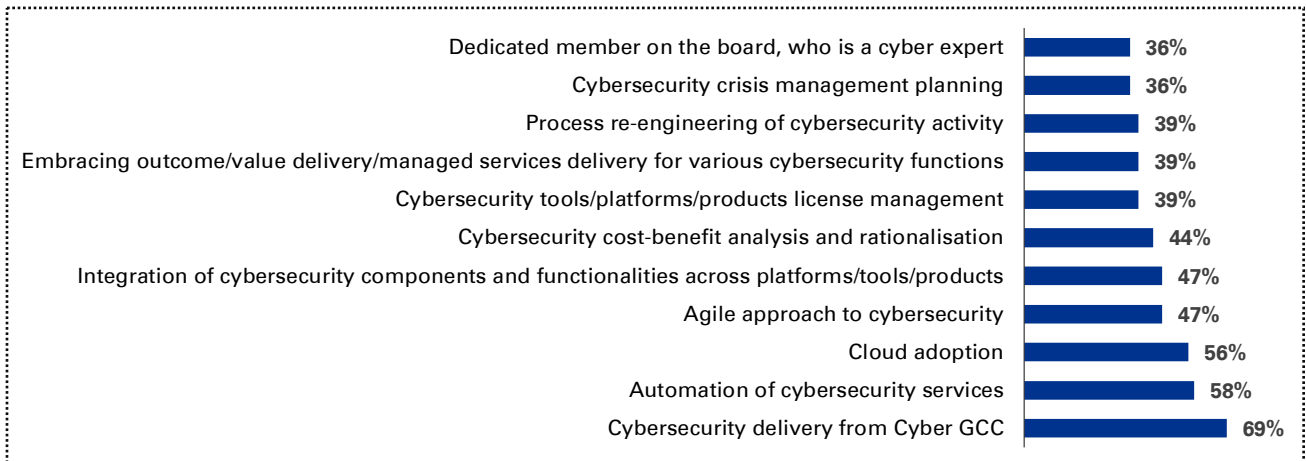
#10 Cyber GCCs deliver significant value

In the wake of economic challenges and uncertainties, global organisations are faced with growing cybersecurity and digital risks. Cyber GCCs come to the rescue, implementing various strategies including:



Cyber GCCs help global organisations optimise cybersecurity spend, allowing them “to do more with less”

Figure 11: Strategies for delivering value to GCCs





Cybersecurity talent, Diversity, Equity, and Inclusion (DE&I)



Amidst the surge in demand for cybersecurity skills, cyber GCCs are constantly evolving their talent acquisition and development strategies. While cyber GCCs are looking to implement automation-based strategies to bring in efficiencies of scale in BAU operations, they are also looking to upskill and attract talent in emerging technologies and initiatives to meet business imperatives. The rise in demand for cyber skills, combined with shortage of specific cybersecurity skills, makes talent retention a key area of focus for cyber GCC leaders. Cyber GCCs have also embraced the DE&I agenda, focusing on inclusivity and empowerment as core values.

#1 Significant rise in demand for cybersecurity and digital risk management skills

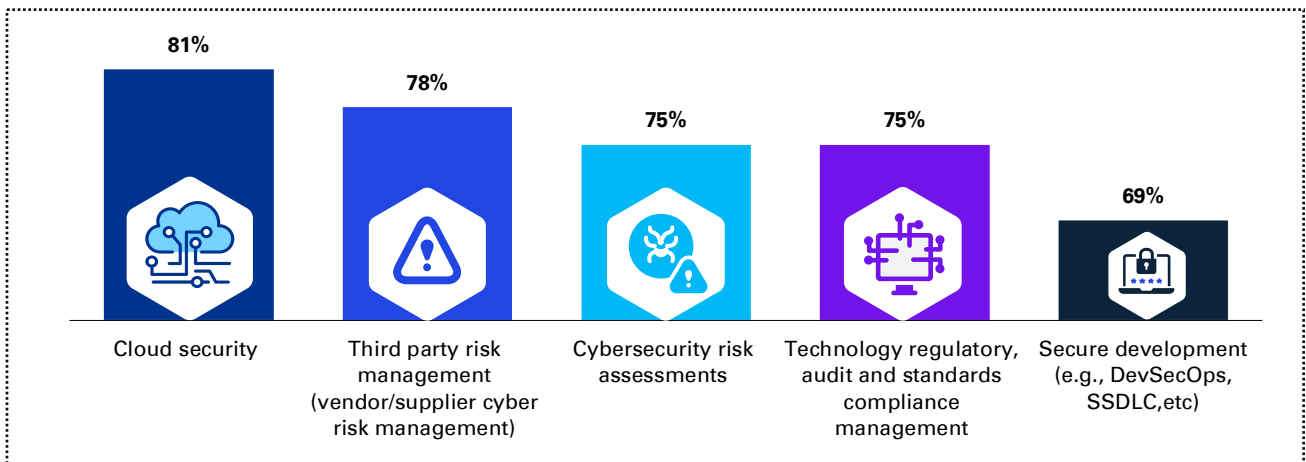
The global cybersecurity landscape is influenced by various events including digitisation, rapid evolution of AI technology, increased reliance on third party ecosystem and supply chain, emerging business and technology models (including Web 3.0, crypto, DLT etc.).

Cyber GCCs have been focusing on cybersecurity and digital risk functions, helping their global organisations deal with the

cybersecurity challenges resulting from these global events.

In line with the global demand, cyber GCCs have experienced a significant rise in demand for various cybersecurity skills. These include cloud security, Third party risk management, cyber risk assessment, secure development and technology, regulatory, audit and standards management.

Figure 12: Cybersecurity skills in demand



#2 Cybersecurity skills acquisition requires a balanced approach

Growing demand for cybersecurity skills requires cyber GCCs to implement various strategies including external hire, using service providers, internal training and leveraging the gig workforce. Cyber GCCs are exploring gig model for certain skill requirements such as

technology, regulatory, audit and standards management and cyber forensics. Certain cyber GCCs have reported leverage of Hire-Train-Deploy (HTD) model for training and acquiring talent for various cybersecurity skills.

#3 Advancing cyber GCC expertise through upskilling

In line with rising cybersecurity talent demand, cyber GCCs are actively leveraging interactive and collaborative methods for cybersecurity and digital risk learning. By embracing methods such as gamification, bug bounties, cyber war games and hackathons, cyber GCCs are enabling their talent with experiential learning techniques. Certain cyber GCCs have signed up focused programs with universities and finishing schools, especially for emerging technology, cybersecurity and digital risk skills.

Training and awareness programs, certification programs, professional examinations and

workshops through both classroom and digital learning continue to be the most preferred methods for upskilling and cross skilling cyber talent. GCCs encourage cross-functional experience or job-rotation, for deeper understanding of business environment beyond the cyber function. Almost 69 per cent of respondents acknowledge the value of active engagement with industry forums and special interest groups. This supports active learning and sharing intelligence with the wider cyber ecosystem beyond the GCC, facing similar challenges and benefit from community-based initiatives.



Upskilling and Cross-skilling cybersecurity talent across cybersecurity and digital risk functions is not just about creating technically well-rounded professionals but also, about fostering a culture of understanding the impact and collaborating with various teams to protect against cyber threats. In addition to technical skills, understanding of specific business priorities and challenges are required for cyber GCCs to deliver strategic value.



Vijay Kumar Puttaswamy, Director, Information Security Compliance & GRC Transformation for VMWare

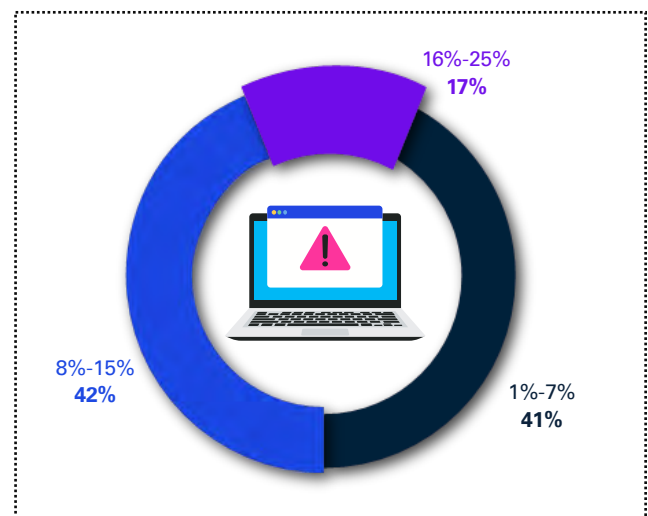


#4 Annual attrition rate of cyber GCCs has increased over the last three years

Demand for cybersecurity and digital risk talent continues to highlight the reliance of global organisations on cyber GCCs. In the current survey, almost 83 per cent of cyber GCCs reported an average attrition rate ranging from 1-15 per cent.

About 17 per cent of the survey respondents reported a higher annual attrition rate falling between 16-25 per cent range. The growth in cyber GCCs in India is consistently fueling the demand for cyber talent and talent retention is a key priority for cyber leaders.

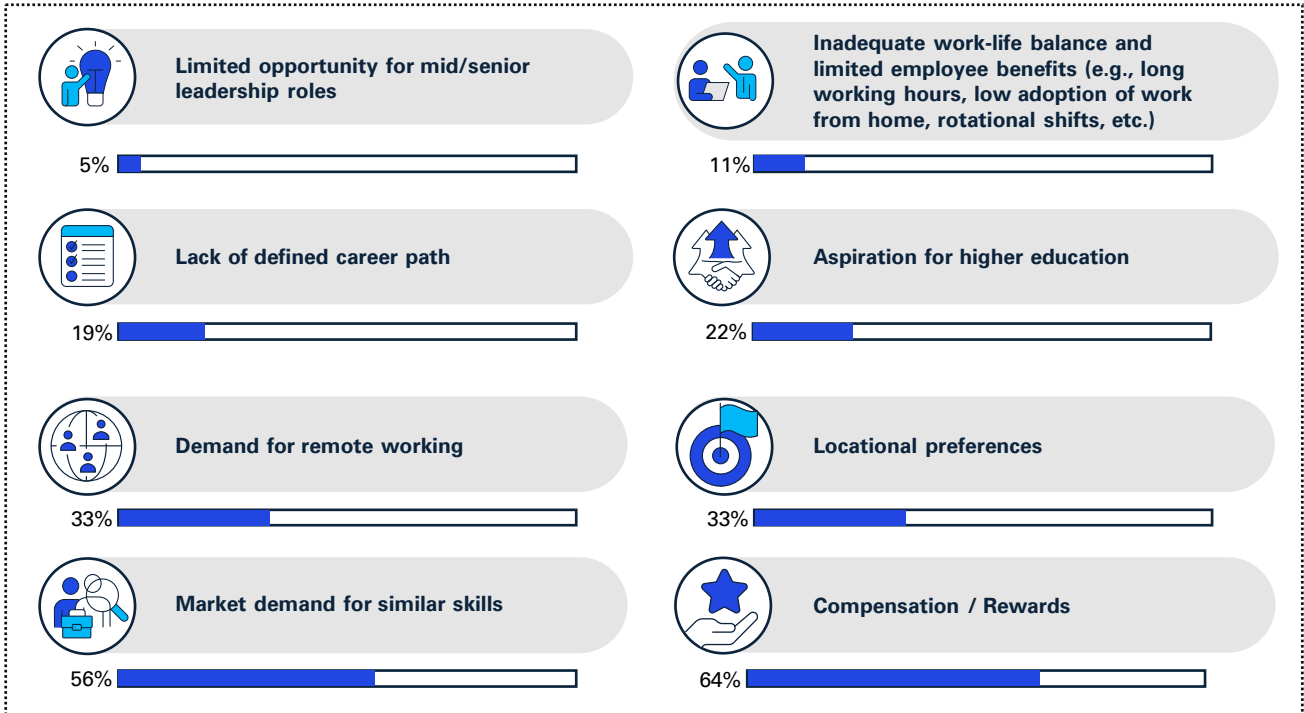
Figure 13: Annual attrition rate of GCC cybersecurity team



#5 Demand for remote working poses a challenge

Key challenges highlighted by cyber GCCs in attracting or retaining cybersecurity talent include growing market demand for similar skillsets, compensation and rewards and locational preferences.

Figure 14: Key challenges towards attracting/retaining cyber talent



Post covid, demand for remote work has presented both opportunities and complexities for cyber GCCs. While remote working provides access to a larger and more diverse talent pool beyond traditional work locations, it has become a significant challenge in attracting cybersecurity professionals required to be based in office locations. There is an increase in demand for remote work from cyber GCC professionals.

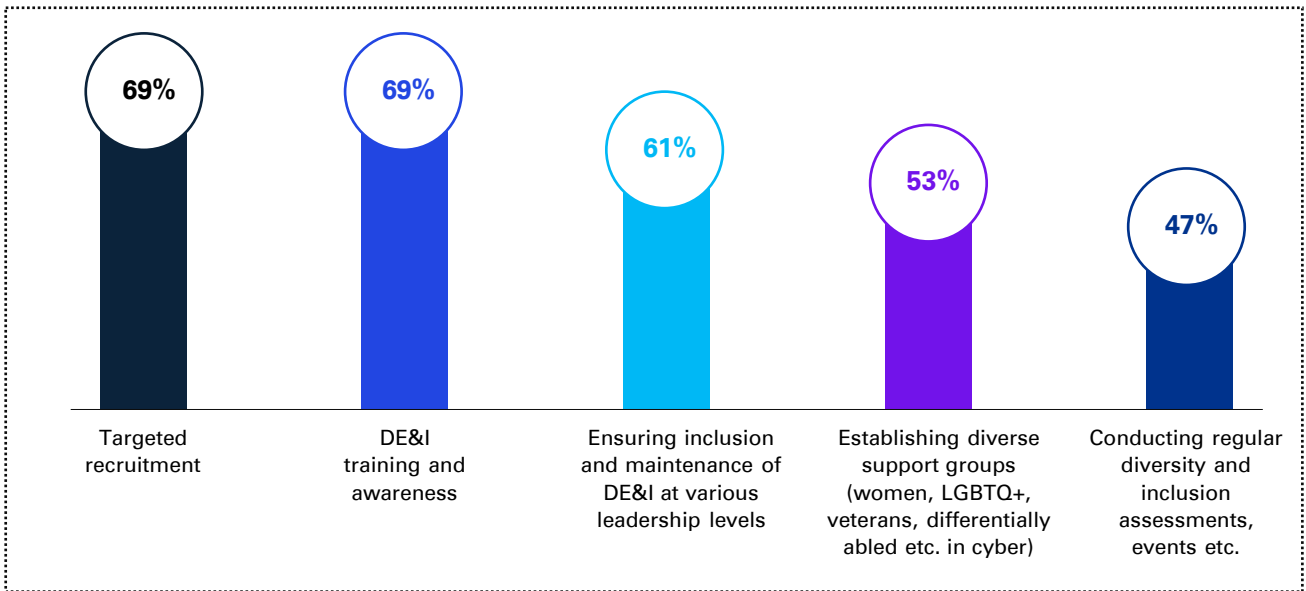


#6 DE&I empowers cybersecurity

To improve the pipeline of diversity in talent, cyber GCCs are actively hiring across levels, from diverse groups including differently-abled, veterans, women in cyber, LGBTQ+, millennials and new age talent etc. Cyber GCCs continue to run training and awareness programs to uplift the awareness and sensitivity of the teams to the challenges faced

by these groups. Many organisations leverage formal and informal mechanisms for teams to discuss and share experiences to enhance the DE&I quotient. These forums may extend to the wider community as well. Organisations also conduct regular events including discussion forums, networking events etc. celebrating their contributions.

Figure 15: Top five initiatives to promote DE&I



#7 New age cybersecurity challenges require fresh thinking

Cyber GCCs are refreshing their approaches to deal with new age cybersecurity and digital risk challenges. With most cyber GCCs experimenting with emerging technologies for competitive advantage, the gap in knowledge and experience between a fresher and an experienced cyber professional is closing in rapidly. Freshers have the advantage of rigorous training in new technologies, come with fresh thinking and approaches vital for the cybersecurity teams. Cyber GCCs are adopting various methods, specific to business

environment, to attract new age cyber talent including – mentorship, internship, defining structured cybersecurity curriculum, focused cybersecurity programs, pre-campus engagement for specific cybersecurity problems, conducting Catch-The-Flag (CTF) contests, cybersecurity hackathons and bug bounties etc.

Cyber GCCs execute four key strategies for enhancing the skills of entry-level professionals:

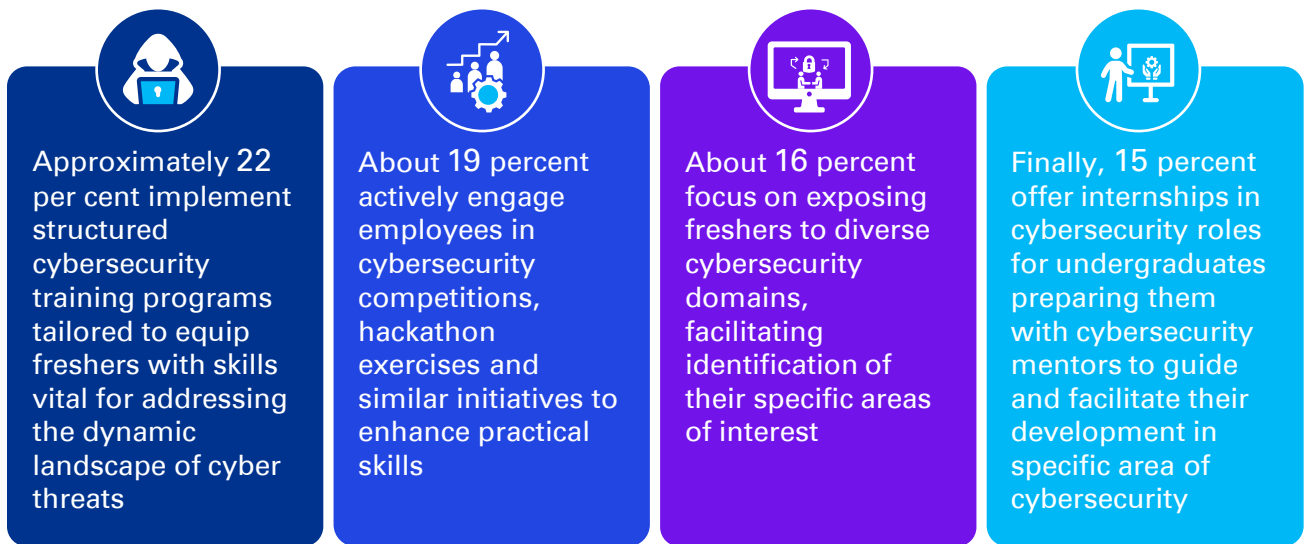
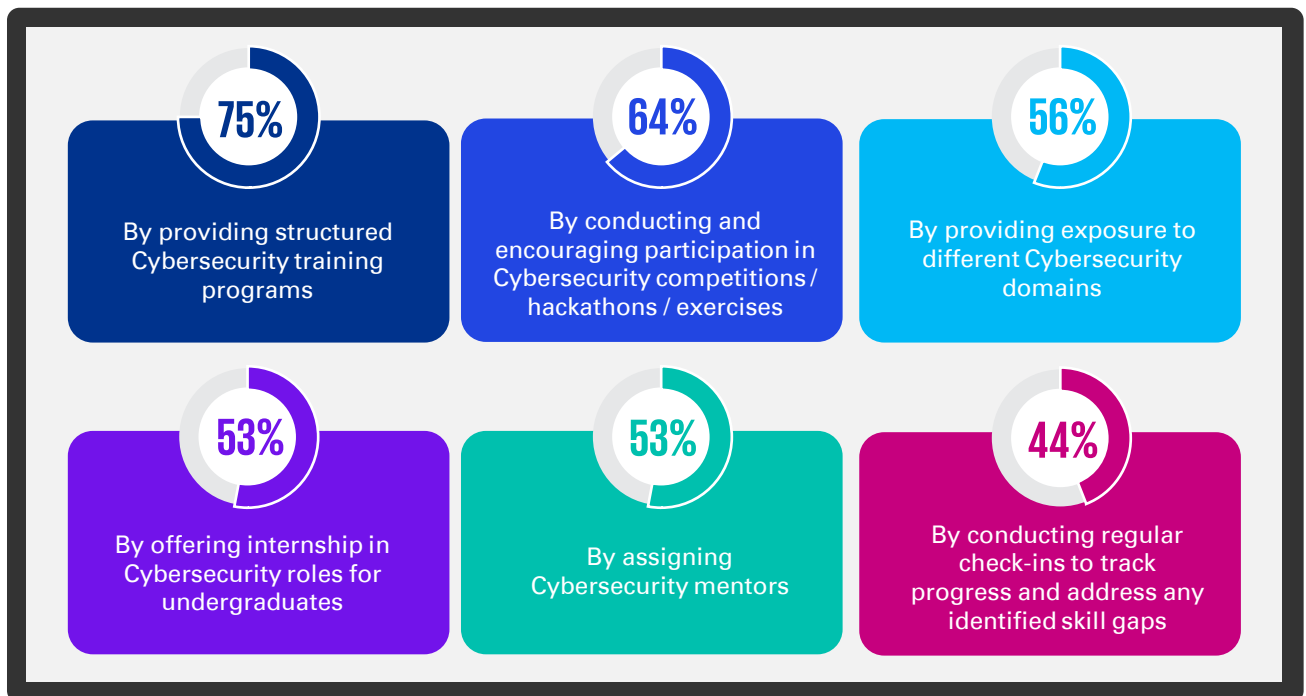


Figure 16: Strategies for training freshers on cybersecurity





Securing digital transformation



#1 Cyber GCCs cultivating an innovation culture

GCCs have been at the forefront of innovation in cybersecurity for their global organisations, failing fast, failing cheaper and innovating with experiential learning. Cyber GCC talent has been tapped beyond day-to-day operations through various structured interventions including the following:




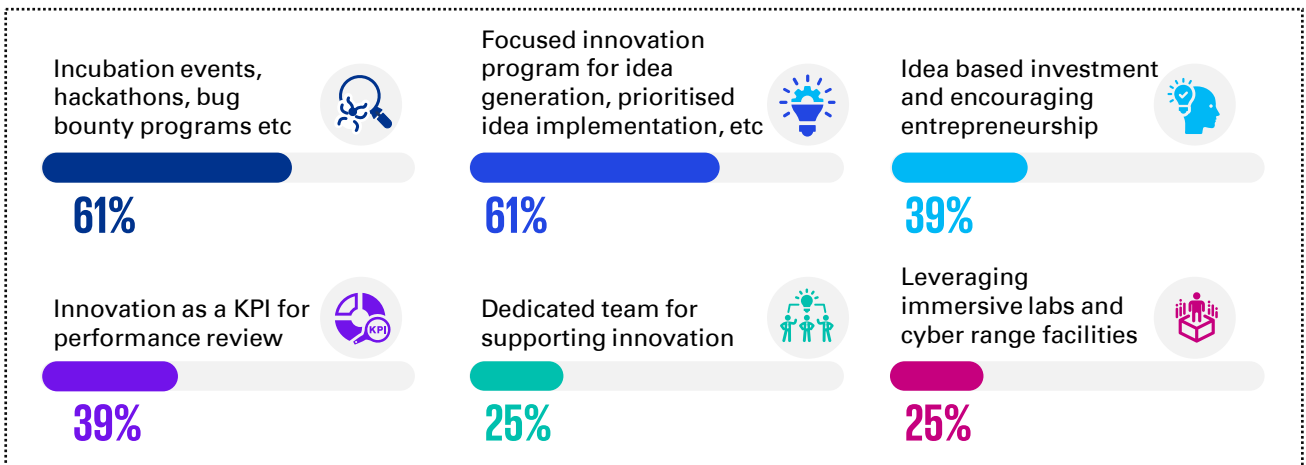
 Hackathon/bug bounty/incubation events	 Focused programs	 Idea based investments
<p>Involving wider organisation (e.g., developer community) to ideate, report, recognise, encourage and solve known and unknown cybersecurity challenges and problems. Developing a trusted, engaging and collaborative cybersecurity ecosystem within the organisation and across the industry.</p>	<p>Global organisations have dedicated investments and charter to identify and solve short-term (tactical and ad-hoc solutions such as access recertification program), medium-term (cybersecurity engineering, automation and implementation programs) and long-term (minimising heavy investments with alternate and advanced techniques, solutions and technologies) cybersecurity challenges.</p>	<p>Following the success of start-up ecosystem globally and in India, specific carveouts/focused groups/tiger teams have been created in cyber GCCs to conceptualise, experiment, contextualise, harden and adopt latest/advanced technology empowered cybersecurity solutions. Many GCCs encourage an engineering approach of developing Minimum Viable Products (MVPs) to demonstrate quick results to help assess go/no-go decision and secure further investments.</p>

Figure 17: Key initiatives taken to promote a culture of innovation



“

In the age of artificial intelligence, cyber GCCs must embrace digital transformation as a strategic enabler, integrating cutting-edge technologies to elevate their cybersecurity capabilities and safeguard global cybersecurity.

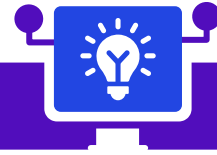
Annapurna Alladi, Partner, Cyber Assurance, KPMG in India



”

Other measures adopted by GCCs to enhance innovation quotient include 1) innovation as a Key Performance Indicator (KPI) , making the cyber GCC leadership accountable for defining and implementing the innovation agenda 2) leveraging cyber immersive labs, providing a gamified environment for experiential learning

3) setting up Centers of excellence/dedicated teams for innovation in cyber, with clearly established outcomes including new products, integration features for existing products, curated solutions for specific cybersecurity functions.



Key Cyber Innovation use cases

Vulnerability rewards programs, secure tools and platforms programs, risk and control automation programs including packaged software implementation, bespoke cyber software implementation, Artificial Intelligence (AI) and Machine Learning (ML) empowered cybersecurity and digital risk platforms etc. are some of the key initiatives, programs that cyber GCCs are involved with and driving along with their global counterparts.

Many of the cyber GCCs surveyed have initiated innovation programs, with some providing specific examples in their survey response, including:



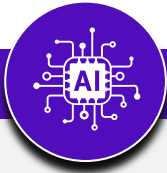
Cyber innovation through Service/Process/Program improvement

- Cyber fusion centres
- Integrated audit and risk framework
- End User Computing Applications (EUCA), End User Developed Applications (EUDA) reduction and risk management framework
- AI and ML risk management
- RPA and low code and no code platform risk management
- DLT risk management.



Platform/Technology based cyber innovation

- Development and maintenance of automated risk and control measurement engines (e.g., automated CCM)
- Development of TPRM platform
- Development and maintenance of global cybersecurity reporting and dashboarding
- Implementation of Security Orchestration, Automation and Response (SOAR) for Security Operations Centre (SOC)
- AI empowered assessment platforms to process third party submitted compliance evidence reports
- Cloud security posture management
- Development of in-house, 24/7 Capture-the-Flag (CTF) platform in both tech and non-tech roles
- Use of RPA for seamless service account password changes
- Cloud security automation (including compliance as a code)
- Data Loss Prevention (DLP) monitoring and automation
- Improvement in security monitoring and incident response by leveraging Robotics Process Automation (RPA)
- Application security management.



GenAI powered cybersecurity use cases

Cyber Fusion Centre

- a) Pattern recognition and rule-based flagging of Suspicious Activity Reporting (SAR)
- b) Transaction fraud prevention, potentially associated with money laundering

Security Operations/Incident Response/Threat Management

- a) Incident Response (analysis for pattern recognition and response definition)
- b) Incident dashboard creation. Near zero manual intervention except for last minute fine tuning
- c) Refining some of the UEBA rule sets to reduce false positives
- d) Reverse engineer the payloads
- e) Use plain English for threat hunting, without need to learn multiple Query Languages

Technology Risk Management and Governance

- a) Create effective controls, policies, and risk statements for rules/requirements
- b) Enhanced obligation summary generation - Generate a plain simple language summary of rules/requirements, maintaining their original content and intent, allowing users for the creation of summaries that are easy to comprehend for a wide audience, while still conveying the necessary information and nuances of the original rules/requirements
- c) Merge similar obligations - streamline and consolidate obligations to enhance efficiency, reduce duplication, and improve overall compliance management.

- d) Harmonisation of controls - eliminate unnecessary duplicates and streamline the compliance efforts
- e) Control validation - enable users to assess the quality of controls based on standard attributes
- f) Creating audit scope (requires sanity checks and to further refine the results)
- g) Confirming classification of document to ensure sensitive and confidential are rightly classified

Vulnerability Management

- a) Auto fix code vulnerabilities from SAST
- b) Consolidation of vulnerabilities and baseline configuration issues
- c) Predictive vulnerability detection

Third Party Risk Management (TPRM)

- a) Analyse patterns/themes from third party risk data
- b) Track the flow of data across the lifecycle, including when it leaves an organisation to boundary third or fourth party etc.

Relevant across cybersecurity domains

- a) Aggregation, normalisation, first level of analysis to identify anomalies
- b) Assessment reporting (initial draft)
- c) Analysis of collected data; and identification of issues/items
- d) Reporting and dashboarding



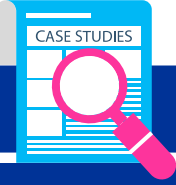
Innovation has been cornerstone in addressing the fast evolving and ever-growing cybersecurity and digital risks. Cyber functions in GCCs have emerged as leaders in addressing these requirements through working on complex use cases, establishing labs to explore synergies across tools and platforms, reengineering of processes and innovating the risk solutions. GCCs have an advantage of establishing the right balance across business risk and cyber risk to create a Trusted environment.



Atul Gupta, Partner and Head, Digital Trust, KPMG in India



Cyber GCC Case Studies



Vulnerability rewards program: A leading financial services GCC has put in place a program for their developer community, to encourage them self-report their application vulnerabilities, incentivising and gamifying vulnerability reporting through organisation wide recognition and assignment of specific rewards, including monetary and leadership engagement. This has resulted in identification of vulnerabilities across various production systems, reducing efforts involved in ethical hacking and penetration testing and more importantly made the developer community more security conscious, and in some cases involved them more in faster remediation.

Customer GRC platform: A leading financial services GCC has built custom applications replacing a commercial eGRC platform. These include a risk and control catalog system, risk assessment platform, vulnerability management platform, security incident management platform, continuous controls monitoring platform and a threat work bench.

Third Party continuous cyber risk monitoring: A leading telecommunications GCC has developed a solution for continuous monitoring of cyber risks associated with its identified portfolio of third parties, which helps in responding to or managing potential cyber risks arising from the third parties on a daily basis.

Risk Intel collected from subscribed and other publicly available sources is leveraged to monitor the vulnerabilities in systems/applications/networks, security incidents and significant changes in risk score. This intel is further contextualised to the arrangement/service provided by each third party within the portfolio. The output of this effort is identification of third parties of interest and controls relevant to the identified vulnerabilities. This solution focuses on mitigating the impact of these vulnerabilities, by focusing on effectiveness of relevant controls.



#3. Cyber GCCs foster open-source technologies adoption

About **58 per cent** of cyber GCCs surveyed are either actively using or planning to consider using open-source technologies for cybersecurity. Cyber GCCs are leveraging open-source technologies for cybersecurity, as they help tap into the innovation through wider developer community, open-source components and standards (e.g. leveraging Open Security Controls Assessment Language (OSCAL) by National Institute of Standards and Technology (NIST), facilitating standardised and machine readable formats for automated control assessments).



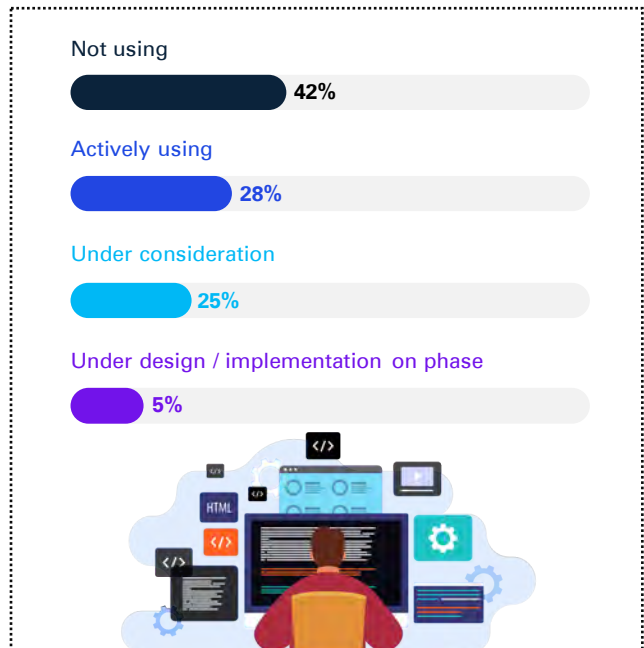
In this ever-evolving landscape fueled by technological advancements, visibility of assets and observability of events are pivotal to managing risk across technology assets. By integrating comprehensive monitoring and real-time analysis, organizations can anticipate and mitigate potential threats, ensuring a robust cybersecurity posture in a connected world.



Hariharan Dharmarajan
Vice President, Cyber Security,
Global Services, Fiserv



Figure 18: Adoption of open-source technologies



Cyber GCC Case Studies



Zed Attack Proxy (ZAP) based solution for security scanning: A leading financial services GCC built a custom solution leveraging open-source security scanning platform (ZAP - ZED Attack Proxy), which scans entire application portfolio. This solution is implemented on their infrastructure, integrated with Continuous Integration/Continuous Delivery (CI/CD) pipeline and ticketing tools, along with automation for running the solution in headless mode and for multiple authentication mechanisms. Also, they have created custom scan policy to tackle our changing cybersecurity threats and created a framework to send scanned reports to the respective stakeholders directly.

This resulted in a reduction in time and manual effort to run scans on application ecosystem, leading to 1) cost-savings vis-a-vis licensing cost and resource time, and 2) greater flexibility in customising the platform as per requirement.

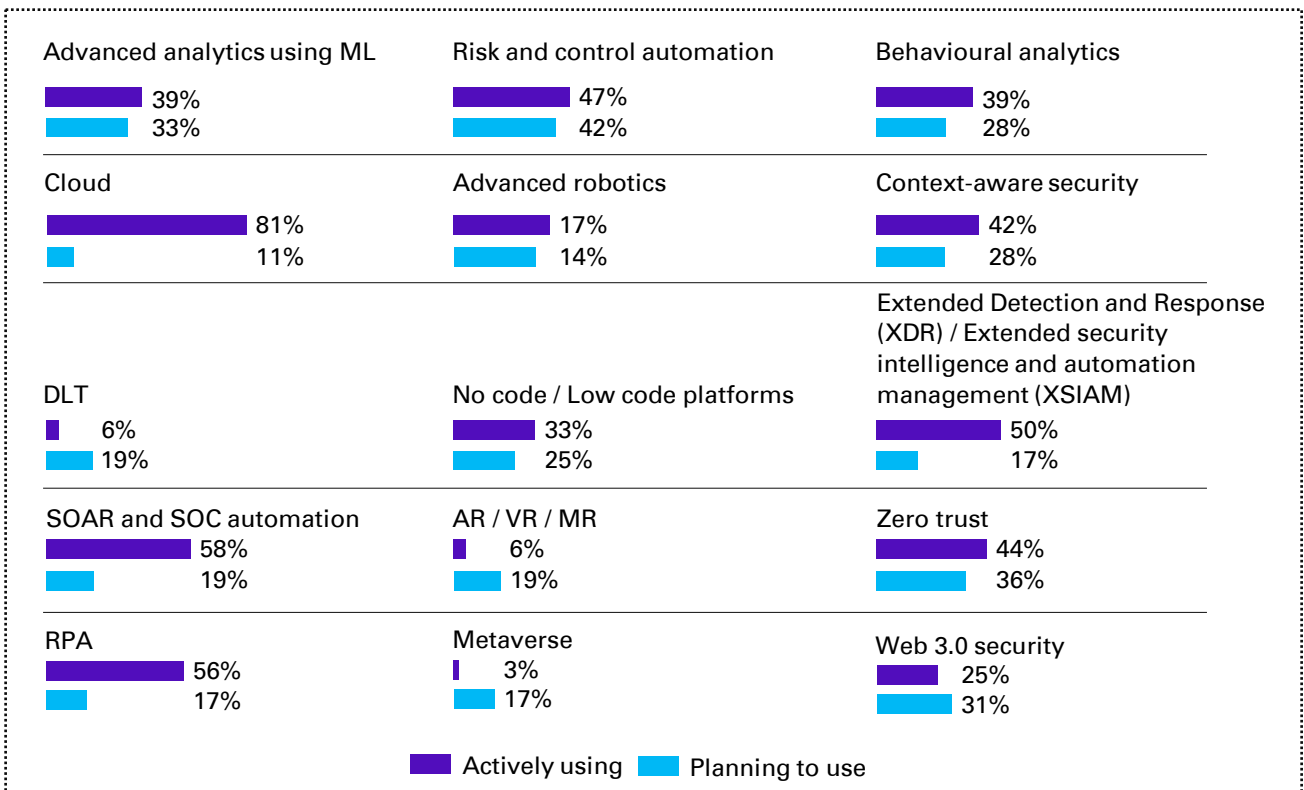
Key cybersecurity areas where cyber GCCs leverage open-source Technologies



Cyber GCCs, on the other hand, continue to manage potential risks and vulnerabilities associated with adoption of open-source technologies. Various programs including third-party application risk management, open-source software security management and software supply chain security management are playing a key role in securing adoption of open-source technologies.

#4. Navigating the future: A deep dive into the adoption of emerging technologies by cyber GCCs

Figure 19: Usage of emerging technology for cybersecurity activity



With the changing cybersecurity landscape, cyber GCCs have actively deployed existing and emerging technologies for effective cybersecurity and digital risk management. Of the survey respondents, top five technologies being leveraged for cybersecurity include

Cloud



The widespread adoption of cloud technologies is rooted in the pursuit of scalability, flexibility, cost competitiveness and collaboration solutions.

Cloud technologies empower cyber GCCs to adapt swiftly to evolving threats and provide a robust foundation for secure and scalable cybersecurity operations. Some use cases for adopting cloud-based solutions for cybersecurity include:

Cloud based SIEM

Cloud based Identity and Access Management

Cloud based end point solutions

Security Orchestration, Automation and Response (SOAR) and Security Operations Centre (SOC) Automation



Cyber GCCs adopt various technologies for their SOC automation with the aim of achieving efficiencies of scale and reducing manual workloads in their security orchestration processes. SOAR and SOC automation empower cyber GCCs to respond promptly to security incidents, minimising response time, and allowing for a more proactive, resilient and robust cybersecurity posture. The following instances are some of the notable use cases:

Automating response to threats detected

Integration with GRC for issue management

Phishing mail analysis for pattern recognition

Reducing time to respond and SOC analyst fatigue

Robotic Process Automation (RPA)



RPA serves as a transformer in enhancing the capabilities of cyber GCCs. RPA makes it easier to automate routine and repetitive tasks and is preferred choice for cyber process automation. This allows the analyst to focusing resources on assessing root cause of issues and their impact. Use cases developed by cyber GCCs include

Access reviews and access certification

Automated ticket handling

Automated evidence gathering

Automated reporting in incident analysis

Cyber GCC Case Studies



AUDIBOTs: A leading manufacturing GCC has developed Robotics Processing Automation (RPA) bots for performing specific audit activities of various business, IT and security controls. This has led to reduced manual efforts, faster identification of audit issues and reduced audit risks.

Vendor BOTs: A leading global bank GCC, has developed bots for assisting their vendors perform desktop checks, which are part of their ODC third party risk management framework. This has helped vendors reduce their manual efforts, enhance their compliance levels and made the third party risk management more collaborative and partnership oriented.

Extended Detection and Response (XDR) and Extended Security Intelligence on Automation Management (XSIAM)



Cyber GCCs leverage XDR and XSIAM solutions for enhanced threat visibility, streamlined response capabilities, and automation in cybersecurity operations which use stand-alone security solutions. The unified approach of XDR and XSIAM enables quicker response towards security incidents reducing risk exposure. Use cases developed by cyber GCCs include

Threat management



End point and network security management

Risk and Control Automation



Cyber GCCs leverage risk and controls automation to enhance and streamline risk management process and internal controls. Cyber GCCs have moved on from leveraging automation only for risk and control reporting to automation in risk and control assessments, control testing, controls monitoring and issue management, contributing to enhanced risk visibility. The adoption of risk and control automation is grounded in the global trend towards proactive risk management. Some specific areas where risk and controls automation are being leveraged include

Automated CCM



Audit workflow management



Compliance workflow automation and centralising artefact collection and archival

Leveraging emerging technologies for cyber GCCs (Technology for cyber)



Cyber GCCs are actively exploring the use of AI/ML including GenAI in enhancing productivity and improving accuracy of outcome. Some specific use cases for AI/ML include

AI (generative, predictive, conversational)



- Threat vector analysis
- AI for risk identification
- AI models integration with Integrated Development Environments (IDE) for vulnerability identification
- Intelligent threat detection, case content summarisation, incident response recommendation, error detection.

Advanced cybersecurity analytics using ML



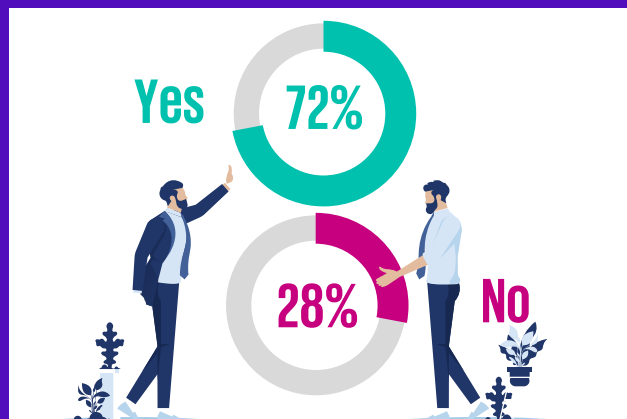
- User Entity Behavioural Analytics (UEBA)
- Risk profiling of end users and end points
- Correlation of logs for Incident Response (IR)
- SOC and incident prioritisation
- Event management
- Secure SDLC fraud and abuse detection
- Data protection
- Controls review.

#5. Cyber GCCs playing a crucial role in tracking End-of-Life and End-of-Support components

Figure 20: End-of-Life (EOL)/End-of-Support (EOS) tracking

Cyber GCCs are proactively tracking and managing risks from End-of-Life (EoL) or End-of-Support (EoS) software, hardware, and other technology components to protect business functions dependent on such assets.

Global organisations continue to report EOL/EoS to their global boards and associated committees and secure investments to plan and implement upgrades or alternates.



#6 Cyber GCCs optimise software asset management

Figure 21: Mode of cybersecurity software procurement

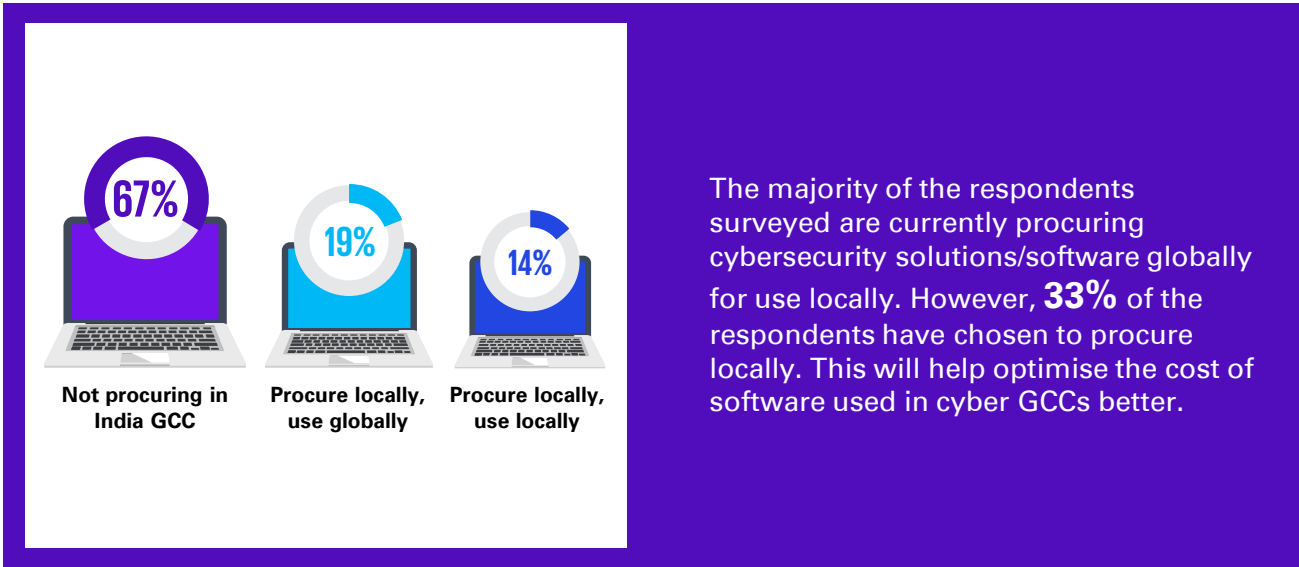


Figure 22: Cybersecurity software publisher customer adoption teams helping cyber GCC teams to get maximum value

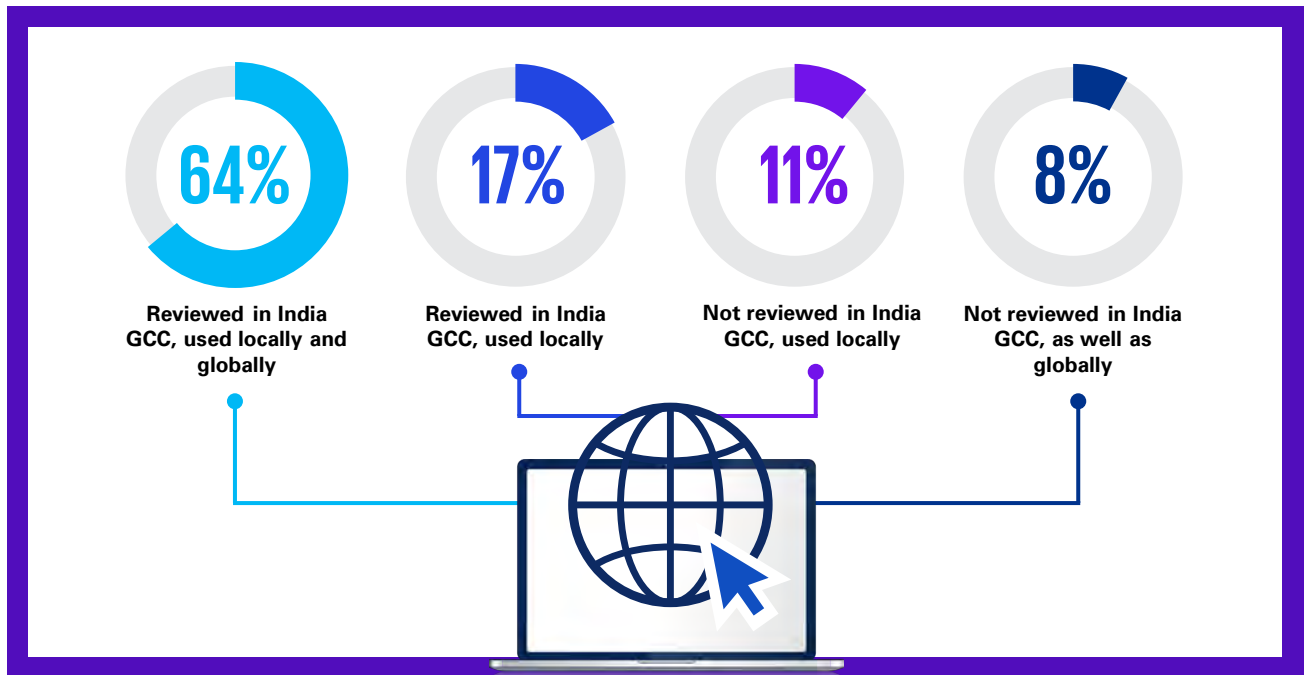


Key objectives of this engagement include enhancement of solution understanding, implementation capability and optimisation of usage of cybersecurity solutions. Organisations seem to prioritise building a collaborative relationship with customer success teams to address potential challenges, receive tailored and seamless support, and ensure a smoother integration of the acquired software into their cybersecurity systems landscape.

#7. Cyber GCCs securing software throughout the lifecycle

Software acquisition and development is one of the major functions delivered by most GCCs in India. Due to functional adjacency, cyber GCC teams are working closely with teams involved in software acquisition and software development to manage risks associated with the software. About 81 per cent of survey respondents highlighted cyber GCCs are reviewing the security of software acquired or developed across their global organisations.

Figure 23: Security review of software





Cyber risk culture



#1: Cyber GCCs manage top risks tracked by their global boards

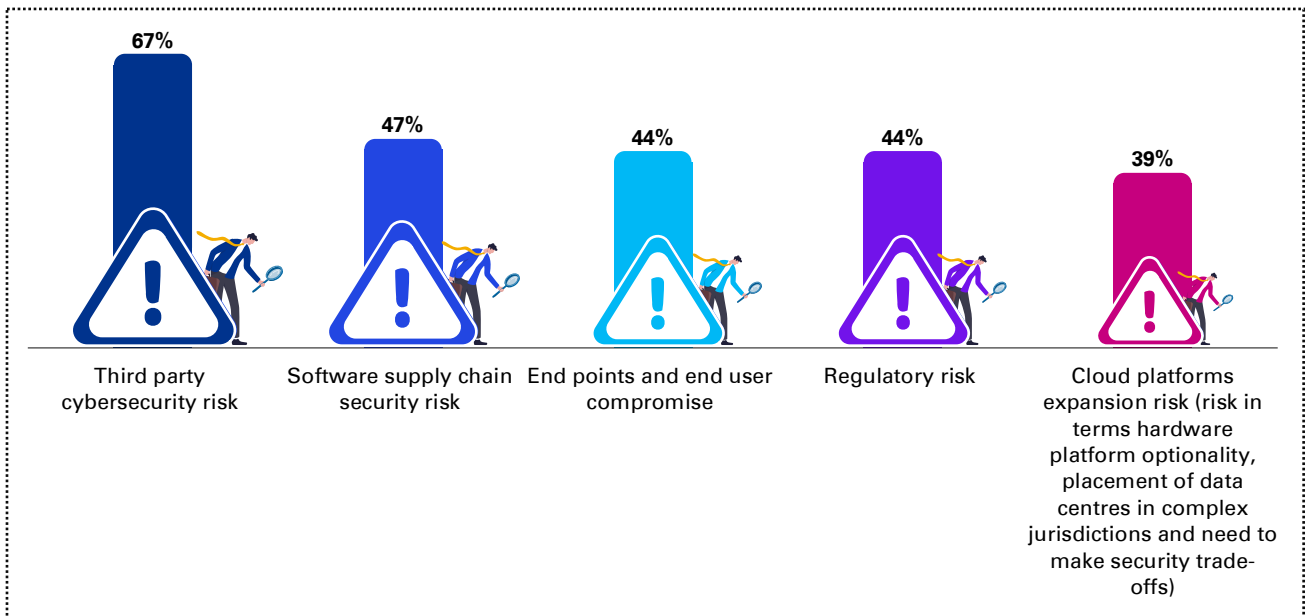
The top five cybersecurity risks reported to the global boards include third party cybersecurity risk, software supply chain security risk, cyber regulatory risk, endpoint security risk and cloud security risk.

These risks highlight growing reliance on third party ecosystems, heightened scrutiny by regulators on existing and emerging technologies, continued end-point and end-

user exposure and accelerated cloud expansion across sectors.

Other key risks being tracked include insider risk, production integrity risk, product user security risk, operational technology security risk, reputational risk, identity risk, IT governance risk, critical infrastructure and system risk, cloud migration risk and technology obsolescence.

Figure 24: Top five cybersecurity risks tracked by global boards



#2: Cyber GCCs play an active role in managing top risks

Many cyber GCCs are helping their global organisations identify, assess, remediate, track and report cybersecurity risks.

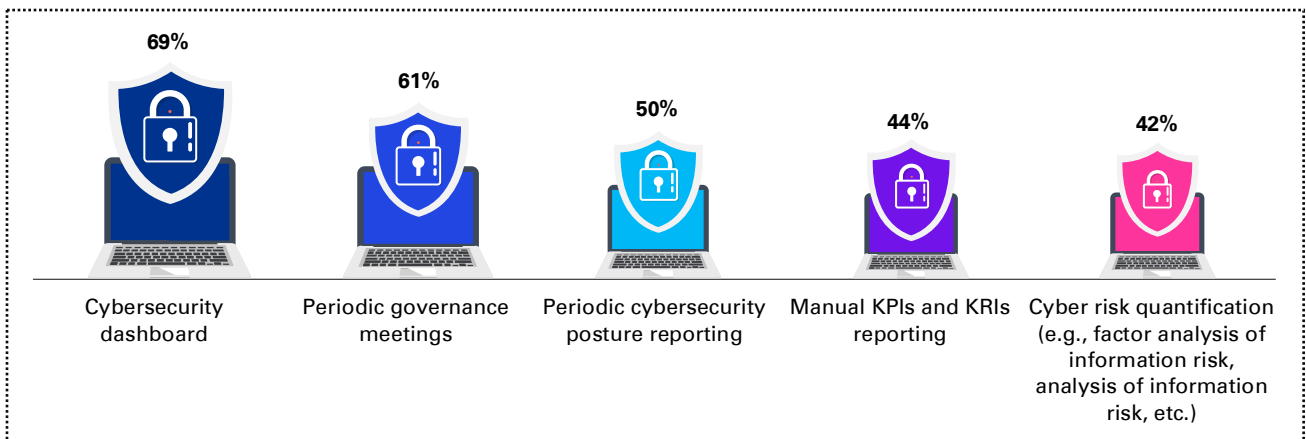
Across the 3LoD, cyber GCCs are focused on identifying and assessing cybersecurity and digital risks, including emerging technologies such as, GenAI, DLT, cryptocurrency, payments, OT, low code and no code etc.

Beyond risk assessments, cyber GCCs are helping identify and design suitable controls to mitigate cybersecurity and digital risks working closely with relevant business, technology and other functional stakeholders in GCCs and across the locations of respective global organisations.

#3: Data driven cybersecurity risk reporting mechanism is growing

The evolution of cybersecurity risk reporting within cyber GCCs is marked by the increased adoption of cybersecurity risk quantification and automated reporting through cybersecurity dashboards. This strategic shift empowers decision-making processes, fostering transparency, with timely insights.

Figure 25: Cyber GCC – risk reporting models



Preferred methods of cybersecurity risk reporting include cybersecurity dashboards, periodic cybersecurity governance meetings, periodic cybersecurity posture reporting and cybersecurity risk quantification. About 44 per cent still utilise manual KPIs and KRIs for reporting.

Cyber GCC Case Studies



Cybersecurity reporting: A leading technology GCC and a leading investment bank GCC have developed an automated cybersecurity reporting system, based on metrics associated with key cybersecurity functions. A cybersecurity risk dashboard has been built on top of the system, providing enhanced risk visibility, tracking top risks identified by their global boards and appointed committees.

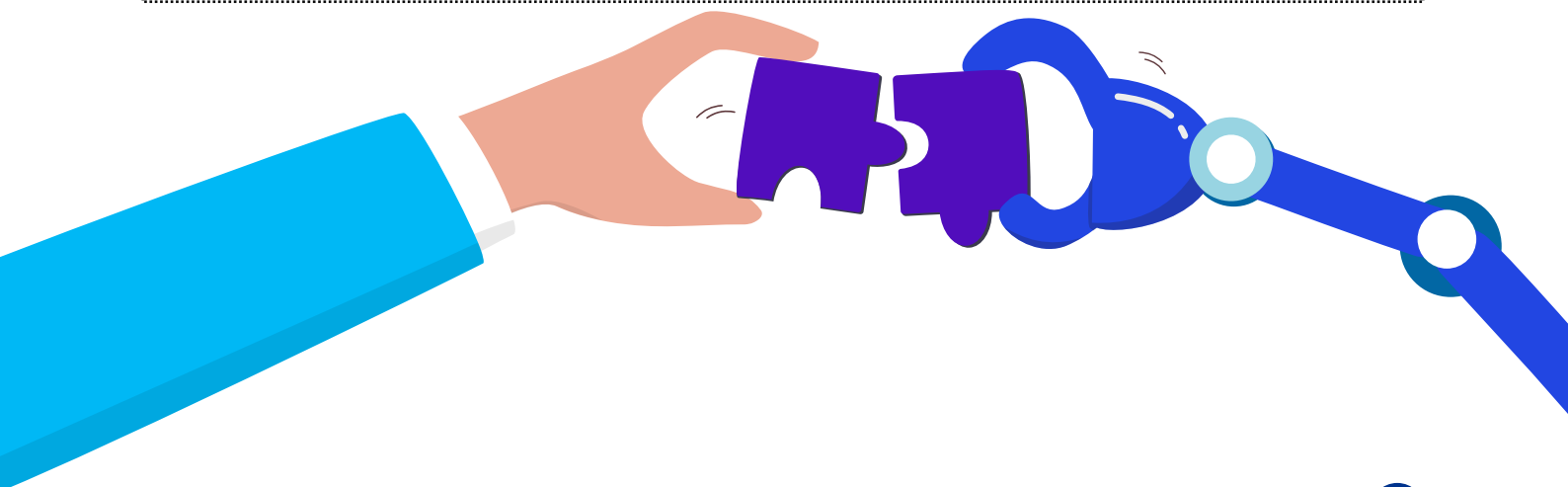
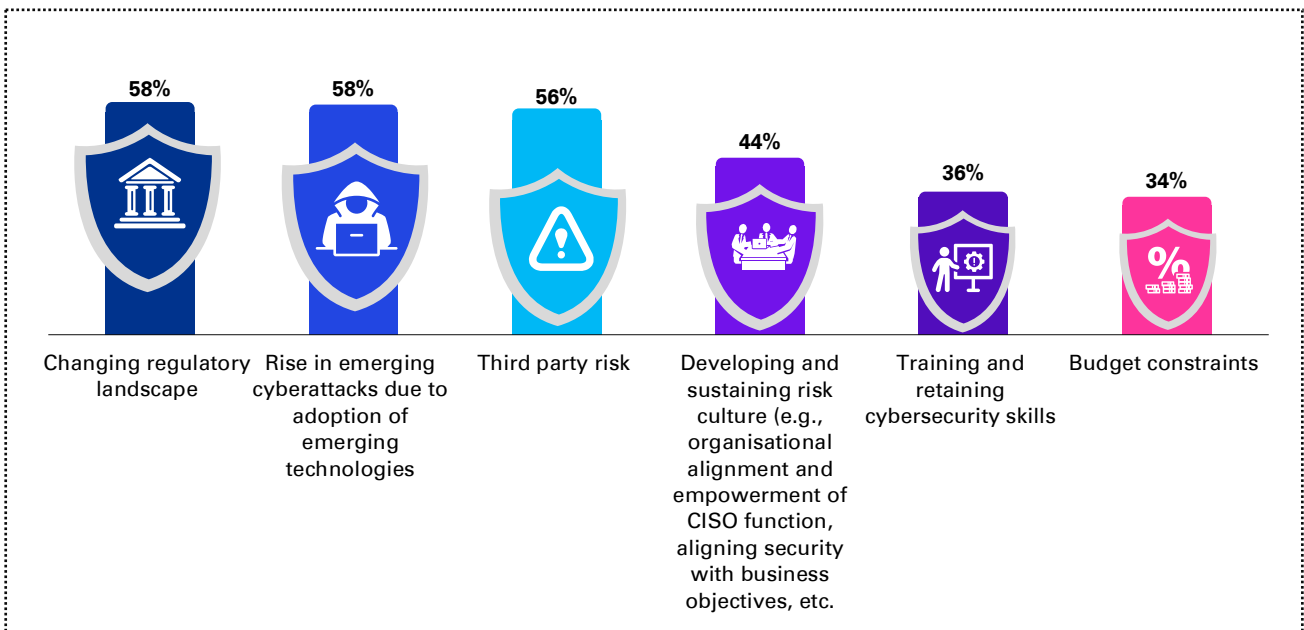
#4: Cyber GCCs navigate existing cybersecurity and emerging digital risk challenges

Top challenges faced by cyber GCCs continue to be the same since 2020, these include:



Adding to this, CISOs are faced with challenges emerging from expanding digital footprint, evolving risks from emerging technologies usage and challenges in identifying advanced technologies empowered cybersecurity and digital risk management solutions to deal with new age technology risks (e.g., AI for AI - AI powered solution for AI risk management, as against a manual or tactical automation-based solution).

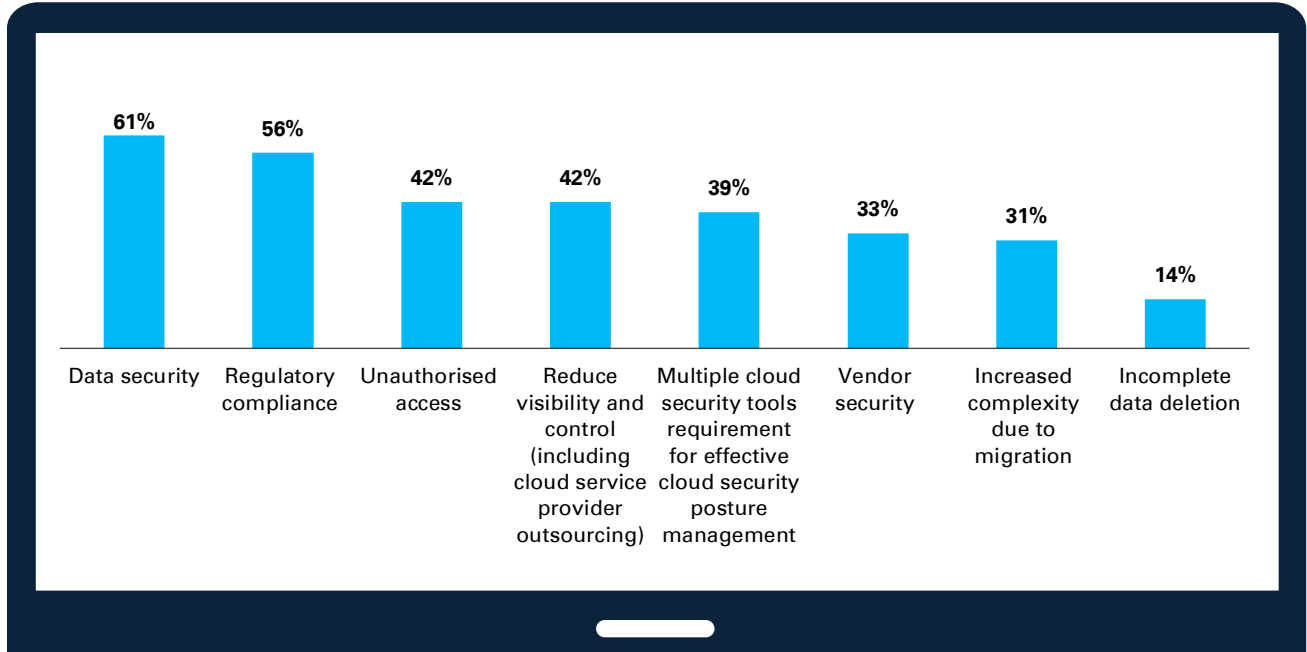
Figure 26: Top Challenges for cyber GCC leadership



#5: Key cloud security challenges faced by cyber GCCs

Cloud adoption has seen a significant increase across global organisations and GCCs help drive this as a key business initiative. Top security challenges reported by the GCCs in cloud adoption include the following:

Figure 27: Key cybersecurity challenges faced by Cyber GCCs during cloud adoption



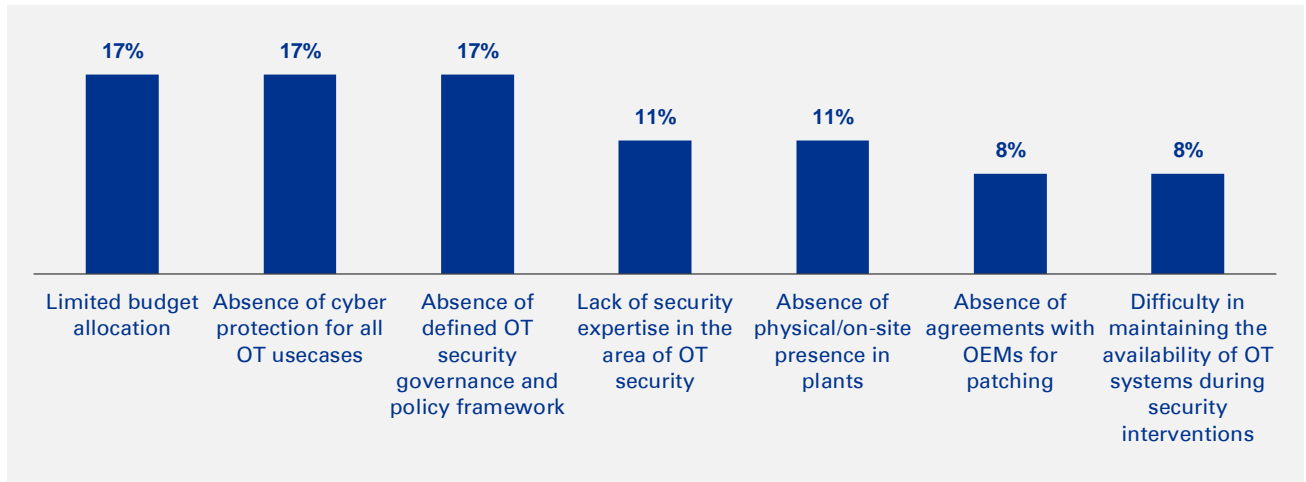
However, cyber GCCs reported that risk managed cloud adoption has distinct advantages, including:



#6: Key operational technology and network challenges faced by cyber GCCs

Global organisations continue to deploy OT systems and leverage cyber GCCs to manage various applications and solutions powered by OT systems and networks. Cyber GCCs not only help in identifying risks but also are focused on implementing controls suitable to manage these risks. It is observed that maturity of handling OT security in cyber GCCs is evolving, however, the survey unveils a diverse set of challenges faced by cyber GCCs in managing OT systems and networks, including:

Figure 28: Challenges faced by Cyber GCCs in securing OT systems and networks



#7: Cyber GCCs key to manage Software Supply Chain Security Risk Management (SSCSR)

Cyber GCCs are playing a pivotal role in orchestrating and fortifying software supply chain security, safeguarding the integrity and resilience of global organisations and their corresponding software supply chains. They actively engage in critical functions including Software Bill of Materials (SBOM) and Software Supply Chain Security Risk Management (SSCSR) lifecycle activities.

Cyber GCC Case Studies



Software Supply Chain Security (SSCS) Risk Management: A Swedish telecommunication GCC developed a framework to manage and mitigate SSCS. Also, they perform SSCS risk assessment for third party software products covering risk areas such as Software Development Lifecycle, Software Development Infrastructure Security, SSCS program Governance, Software Product Security Capability, SBOM, and Third Party/Partners Risk Management.

#8: Top 10 cyber threats

Many cyber GCCs consider themselves at “adaptive” maturity level i.e., continually improved, when it comes to dealing with cybersecurity threats.



Notably, in 2023, cyber GCCs reported a substantial increase in readiness level for dealing with rogue software attacks.

#9: Cyber GCCs imbibing cyber risk culture

As cyber GCCs continue to deal with evolving cybersecurity threats, and challenges including emerging technologies risk management, cybersecurity and digital risk management requires, more important than ever, a cultural shift.

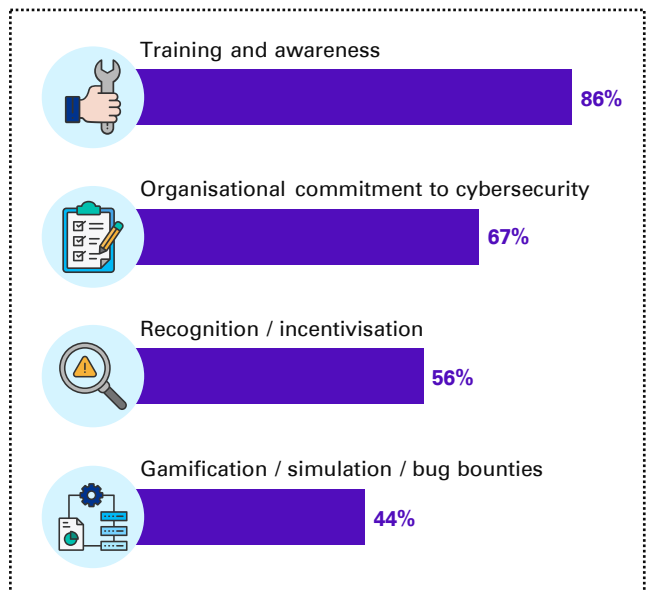
Cyber GCCs continue to work with internal and external stakeholders to bring in and manage a change, which empowers their organisations to better understand and appreciate the cybersecurity and digital risks and associated impact on their business.

Key programs taken up by cyber GCCs to promote cybersecurity risk culture include cybersecurity training and awareness, recognition/incentivisation and gamification/simulation/bug bounties.

There is an increase in gamification, simulation, and bug bounty programs (increased by about 30 per cent compared to 2020), while training and awareness continues to be a preferred approach, followed by

organisations commitment to promote cybersecurity risk culture and implementation of recognition and incentivisation measures.

Figure 29: Key initiatives taken to promote risk culture in cyber GCCs







Together for better



In the post-pandemic landscape, the imperative for collaboration within the cybersecurity ecosystem has grown exponentially, consistent with the rapid pace of digital transformation and advancements in emerging technologies. Central to this industry-wide collaboration driven by cyber GCCs is sharing of key challenges, benchmarks and leading practices in dealing with cybersecurity and digital risks.

Cyber GCC forums are on the rise, showcasing innovation across key cybersecurity and digital risk domains and leveraging collective intelligence to provide counsel to government, regulators and industry bodies on cybersecurity matters impacting GCCs.

Cyber GCCs collaboration with various industry stakeholders including start-ups, other GCCs, academia and law enforcement, regulatory and industry bodies is driven by multifaceted strategy aimed at fostering innovation, knowledge exchange and industry resilience.

Engagement with startups and academia offers cyber GCC access to diverse, accelerated and commercial models of innovation, leveraging the agility and creativity inherent to them.

Learning from other GCCs becomes a key motivator, creating a dynamic environment where shared experiences and insights contribute to collective growth and adaptability.

Cyber GCCs interact and engage with the regulators not only focused on achieving regulatory compliance but also help appreciate global and cyber GCC challenges in meeting the regulatory requirements.

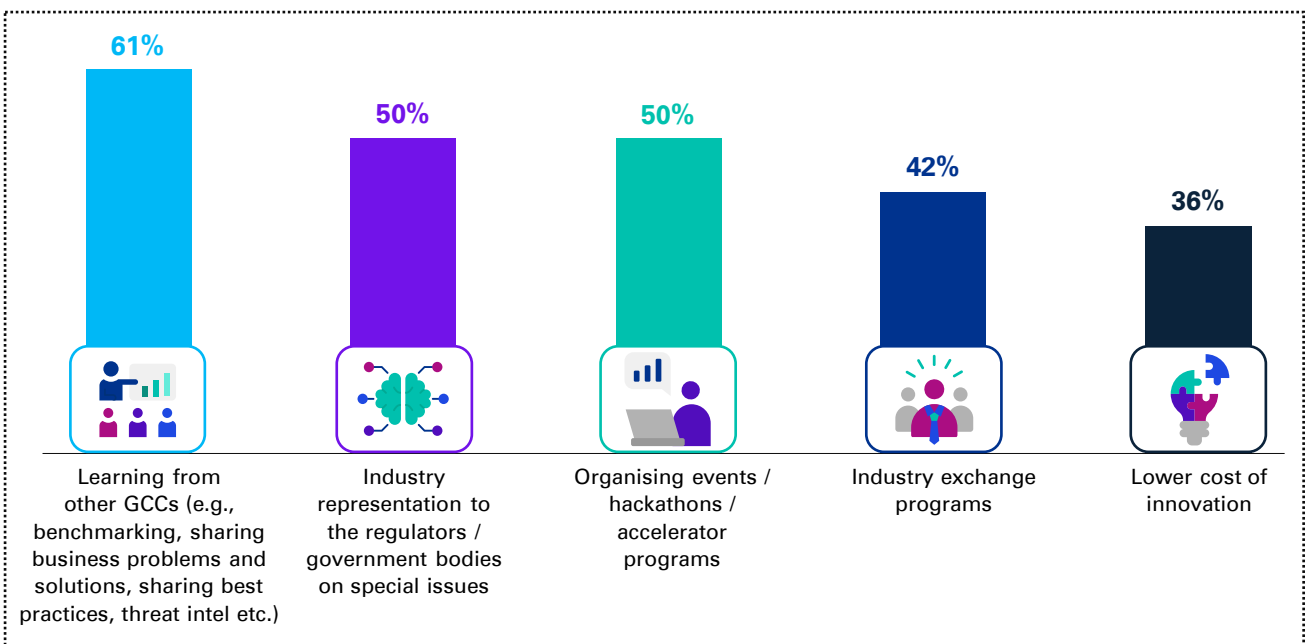
In essence, 'Together for Better' epitomises cyber GCCs commitment to increasing industry-wide cyber resilience and fostering a secure digital future for all.

#1 Cyber GCCs collaborate for better

Global organisations have been collaborating through various platforms including industry associations, information sharing and analysis groups, enabling their leaders and talent through industry events, hackathons and focus groups such as Special Interest Groups (SIGs) creating standards and industry-wide frameworks focused on cybersecurity and digital risk management.

Cyber GCCs have imbibed this culture of industry-wide collaboration and have empowered their global organisations to innovate faster, strengthen organisational and industry-wide resilience efforts and most importantly sustain and develop new generation talent, tools, platforms and new-age practices required to deal with cybersecurity and digital risks.

Figure 30: Top five drivers for cyber GCC collaboration



Key drivers for cyber GCC collaboration include:



a. Learning from other GCCs

As cyber GCCs expand across various cybersecurity and digital risk management functions, it is imperative for them to learn from peers through:

- Benchmarking of cybersecurity practices, sharing of cybersecurity challenges, problems and solutions, leading practices, threat intelligence etc.
- Participating in cyber GCC forums and events, to discuss emerging technologies and cybersecurity considerations and collaborate in improving industry standards and frameworks
- Conducting industry-wide joint simulation exercises to address common cybersecurity challenges.



b. Industry representation to the regulators/government bodies on specific issues and matters related to cybersecurity

Cyber GCCs collaborate with government bodies and regulators to ensure industry representation on specific issues due to the critical intersection between digital empowered economy and cybersecurity and digital risk management.

By engaging with government and regulatory entities, cyber GCCs actively

participate in shaping policies and regulations that directly affect the industry, ensuring that the rules are both effective and practical. This collaboration also facilitates information sharing, enabling timely response to emerging cybersecurity and digital risks and aligning industry practices with national security priorities.

Additionally, cyber GCCs bring global experience to the table, helping regulators better appreciate challenges and leading practices of global organisations. Some of the key government initiatives including National cybersecurity strategy, DPDP Act, G20 summit declaration of cybersecurity as a global problem, Honourable Prime Minister of India call for crypto regulation, cybersecurity and

human-centric AI governance have found resonance with cyber GCCs and their global counterparts. As India emerges stronger as a global economy, it continues to attract global organisations, the role of cyber GCCs will evolve further with active participation, consultation, compliance and formulation of various security strategies.



c. Cyber GCCs partner with start-ups for innovation

Many Cyber GCCs are leveraging start-ups to augment their capabilities and propel innovation by encouraging accelerator programme as well as exploring tie-ups with the start-up community for:

- Co-creation of cybersecurity products, especially involving AI, Machine Learning and other advanced technologies
- Niche product line, including Web 3.0 security, privacy technology, crypto security etc.
- Access to cybersecurity talent with niche skills in aforementioned areas.

Start-ups are gaining access to global cybersecurity challenges, problems and sponsorship through cyber GCC platform. This will not only increase start-ups' reach but also help them tap into the global market.



d. Cyber GCCs and academia unite: crafting a cybersecurity career value proposition

Availability of talent is a key factor in the growth of cyber GCCs in India. To attract and retain the right talent, cyber GCCs are working with academic institutions and schools in bringing practical experience to the curriculum. This is done through internships, mentorship programs, guest

lectures, hackathons and industry specific programs. By actively engaging with educational institutions, these centres not only attract top-tier talent but also create a conducive environment for knowledge exchange and innovation.

Collaboration with	2023	2020
other GCCs for benchmarking, sharing business problems and solutions, sharing leading practices and threat intel	55%	29%
regulators and government bodies for Industry representation on specific issues	47%	23%
branding for talent acquisition	39%	32%
sharing information with the wider ecosystem	33%	NA
focus on leadership development	31%	NA



Collaboration between a Cyber GCC and the broader ecosystem will foster the speed and enhance the impact from the work that they doing . Collaboration with the ecosystem – peers, partners, startups and academia is a force multiplier having the potential of creating industry-wide collective cybersecurity shield, safeguarding the health of global space, while fostering cybersecurity innovation.



Sukanya Roy, Head, BPM and GCC Initiatives









Cyber GCCs in a Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) World



Post covid, digital technology advancements including Gen-AI adoption, geopolitical uncertainties, rising cyber warfare and increased demand for cyber skillsets and talent, have led to significant increase in the role of cyber GCCs supporting their global organisations.

Amidst changing regulatory landscape, global organisations are dealing with a dynamic and

challenging environment. Cyber GCCs are working with their global organisations in managing these, in addition to sustaining BAU and organisational priorities. Cyber GCCs are adopting innovative, collaborative and scalable approaches to cybersecurity and digital risk management.



Cyber Fusion Centers are next generation Security Operation Centres (SOCs), acting as nerve centers, integrating deep functional and technical capabilities across Cyber GCCs and their global organisations. In this ever-evolving global cybersecurity and digital risk landscape, these centers of cyber excellence are at the forefront of navigating uncertainties

Shalini Pillay, Partner and GCC Leader, KPMG in India



#1 Cyber GCCs tap into advanced and latest technologies

As the digital landscape continues to evolve, cyber GCCs recognise the importance of harnessing capabilities of advanced, latest, and fit-for-purpose cybersecurity instrumentation to identify, detect, protect, respond, and recover from growing and active cybersecurity threats.

Top five cybersecurity tools leveraged by cyber GCCs include Intrusion Detection Systems/Intrusion Prevention Systems

(IDS/IPS), Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), Threat Intelligence Platforms (TIP) and Network Traffic Analysis (NTA).

Also, use cases are being developed with advanced technologies such as AI, ML, and behavioural analytics to identify anomalies and to proactively defend against emerging threats.



#2 Elevating the defense by leveraging Cyber Fusion Centers (CFCs)

CFCs are central for cross-functional collaboration and innovation to manage cybersecurity with agility and comprehensive response capabilities. They bring stand-alone cyber functions together to respond to various cyber crisis situations. CFCs leverage emerging technologies, data driven strategies and threat

intelligence in identifying and managing cybersecurity and digital risks on a real time basis.

About 56 per cent of cyber GCCs support their global organisations in either setting up or operating existing CFCs.

The top three CFC benefits reported by cyber GCCs include:

Faster Incident Response timeframe:

CFCs are leveraged in building use cases through seamless integration of threat intelligence, advanced analytics, and automated workflows across various functions and processes, instrumental in achieving faster incident resolution and building resilience.

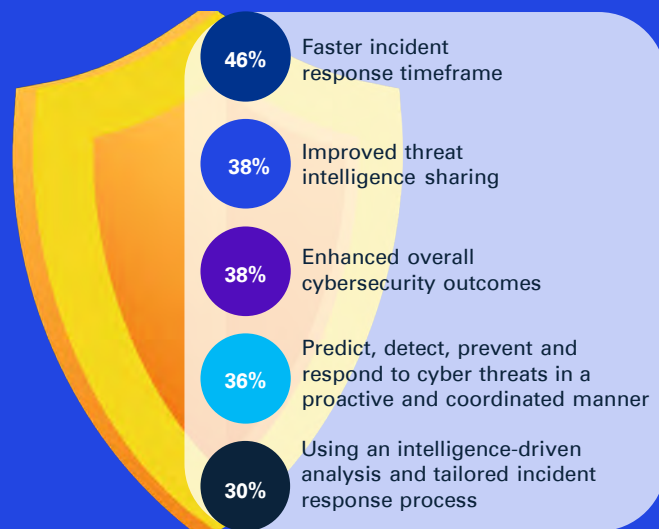
Improved sharing of threat intelligence:

CFCs within cyber GCCs are enhancing threat intelligence processing by contextualising information from diverse data sources, fostering real time collaboration amongst various security teams, leveraging advanced analytics including User and Entity Behaviour Analytics (UEBA). This approach is helping global organisations in gaining a comprehensive understanding of the evolving threats and accelerating distribution of timely information for better response.

Enhanced overall cybersecurity outcomes:

CFCs within cyber GCCs are elevating the overall cybersecurity posture of the global organisations by operationalising a comprehensive framework. They streamline activities from various functions, processes and solutions and build models to anticipate and counter evolving threats and scenarios resulting in more informed decisions and outcomes.

Figure 31: Benefits of utilising CFCs



Cyber GCC Case Studies

AI empowered SOC automation: A leading financial services GCC has developed a solution to automate incident enrichment, analysis and remediation action, in order to enhance the overall incident response efficacy and efficiency. This included:

- GenAI based assistance in incident response templates and queries to aid analysts in their analysis and correlation
- Enhanced incident enrichment through automated Intelligence feeds
- Indicators of Compromise (IOC) based threat hunting
- Streamlined incident response through seamless integration with other security solutions
- AI BOT based quick reporting and dissemination of information (including graphs and reports)

This resulted in reduced manual efforts, enhanced quality control on incident ledgers, reduction of analyst time and incident containment, less than 30 minutes in most of the cases.



#3 Cyber GCCs help in cyber risk quantification and cyber insurance

Global organisations constantly strive to implement robust cybersecurity practices across people, process, and technology landscape. However, due to the ever-evolving cybersecurity threat and attack landscape, regulatory complexities and third party risks, there is a residual risk that organisations need to proactively quantify and manage. Cybersecurity risk quantification exercise followed by procuring suitable insurance coverage continues to be an important initiative in global organisations approach to cybersecurity and digital risk management.

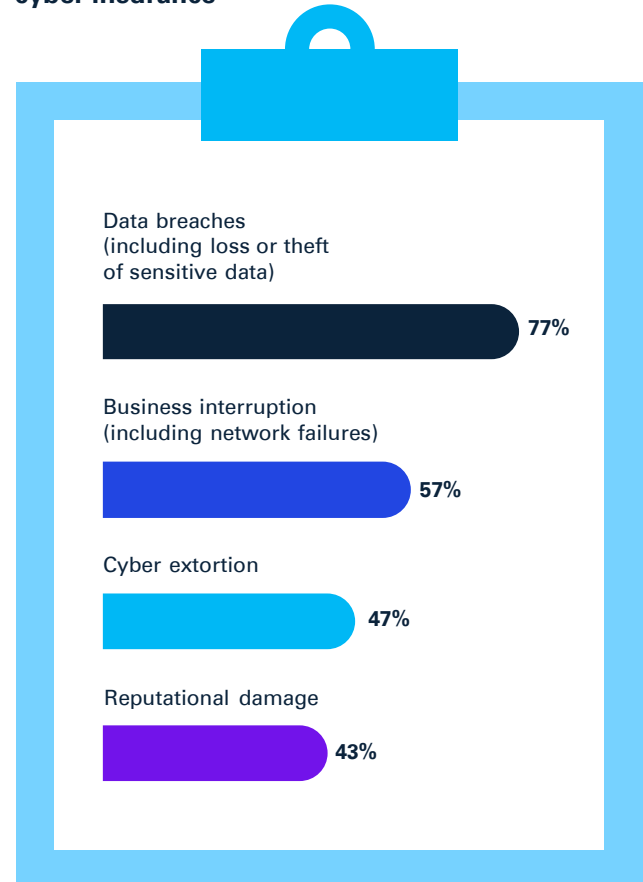
The majority of GCCs (66 per cent) conduct cybersecurity risk assessment and quantification prior to procurement of cyber insurance following a risk-based approach to their cyber insurance strategies.

For most of the global organisations (73 per cent), the global cyber insurance policy extends to their cyber GCC entities as well. This helps them bring a global risk lens and comprehensiveness in coverage.

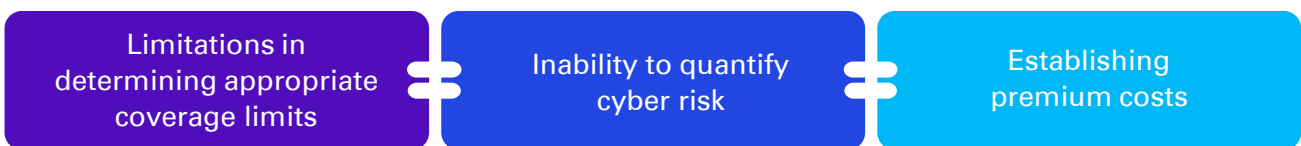
Cyber insurance is leveraged to protect from financial losses due to cyber incidents. The costs including forensic analysis, regulatory fines or penalties, losses in business operations, data recovery, and reputational management may be recovered based on the nature of the policy.

According to the survey, top three cybersecurity incidents covered under cyber insurance include data breaches, business interruption and cyber extortion.

Figure 32: Type of incidents covered under cyber insurance



Cyber insurance has been evaluated for appropriate risk management in the last few years. Some of the challenges encountered by GCCs in selecting cyber insurance include:



#4 Cyber GCCs proactively leverage global privacy practices to comply with DPDP Act

Digital Personal Data Protection (DPDP) Act emphasises organisations’ duty to protect digital personal data, while safeguarding the freedom of individuals.

While the privacy principles are fundamentally aligned to the principles of the global regulations defined in the last few years, DPDP Act has some unique requirements including applicability to digital personal data, non-distinction between Personally Identifiable Information (PII) and Sensitive Personal Information (SPI), etc.

Cyber GCCs have already been on privacy compliance journey, and this experience will be an advantage in meeting the DPDP Act requirements. Additional considerations for GCCs in implementing DPDP Act requirements include stakeholder complexity (internal employees, contractors, third parties, customers etc.) and regulatory penalties.

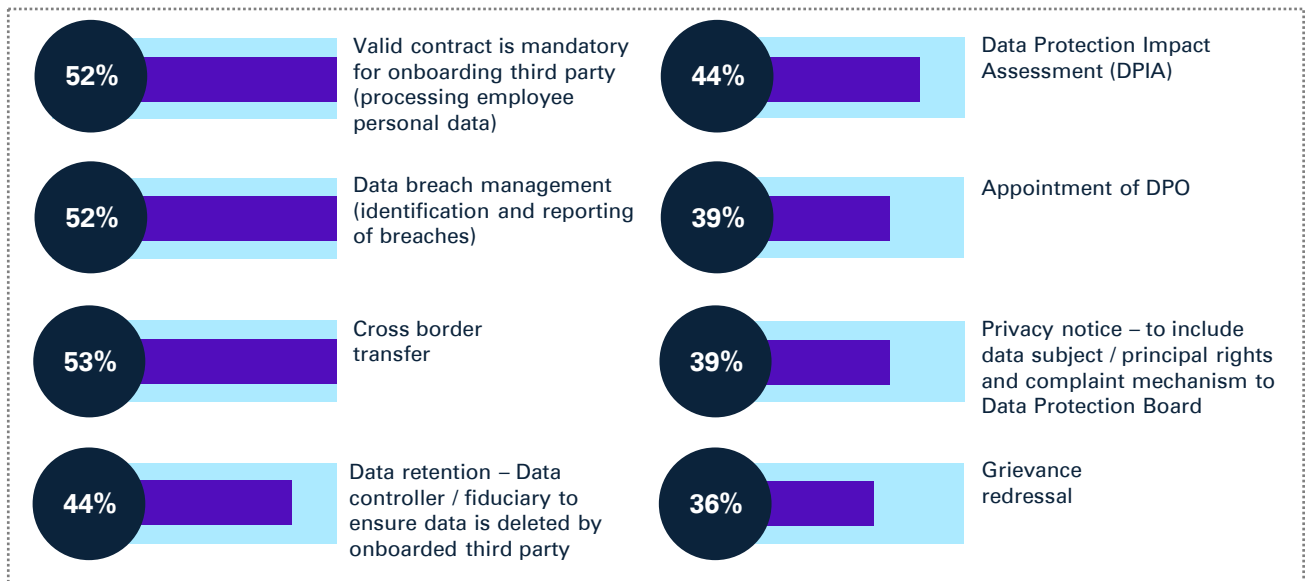
Cyber GCCs internally have identified key focus areas pertaining to DPDP Act including defining

a unified privacy governance program, personal data discovery, mapping and inventory, data protection impact assessments, data breach management, security for privacy, data principals rights management, third party privacy management, cross border data transfer, privacy by design, training and awareness programs and privacy monitoring and reporting.

The survey highlights that fewer than 50 per cent of GCCs have formalised and implemented processes to comply with DPDP Act requirements of appointment of Data Protection Officer (DPO), grievance redressal, Data Protection Impact Assessment (DPIA), data retention, data deletion and privacy notice.

However, majority of the cyber GCCs (> 50 per cent) have already formalised and implemented processes to comply with data breach management, cross border transfer and contractual requirements of the act.

Figure 33: Cyber GCCs formalised and implemented processes vis-a-vis DPDP Act requirements



Global regulatory compliance has always been a key focus for cyber GCCs due to business and reputational impact leading to financial penalties. It is encouraging to note that most of the cyber GCCs have experience in addressing local (e.g., DPDP, RBI etc.) as well as global regulations (e.g., HIPPA, GDPR, PIPEDA, CCPA etc.) applicable.



Vinayak Godse, CEO, DSCI







Methodology

The premise of this report is based on sources of information, meetings and brainstorming sessions undertaken by KPMG in India, nasscom, DSCI and industry leaders between August 2023 and December 2023.

Information used for comparison amongst the years 2023, 2020 and 2018 within this report is sourced from previous editions of Secure in India.

Survey

The insights published in this report are primarily based on the response received from the 'Secure in India' survey rolled out to Global Capability Centres (GCCs) in India.

Respondents of this survey are GCC leaders, Chief Information Security Officers, Chief Technology Officers, their equivalent or their delegated designates involved in leadership and management functions of global cybersecurity delivery.

This survey has representation from GCCs belonging to following sectors, namely:

- Agro chemical
- Automotive
- Banking
- Consumer goods
- Energy
- Entertainment
- Electronics
- Financial services
- Fin-Tech
- Healthcare
- Insurance
- Investment management
- Life Sciences
- Manufacturing
- Publishing
- Retail
- Technology

Meetings with industry leaders

Inputs were sought from industry leaders through multiple meetings, discussions, and brainstorming sessions throughout the development of this report.

Secondary research

The industry experts at KPMG in India conducted detailed secondary research. The team relied on proprietary databases and public websites to gain better understanding into each insight.

Content review

Multiple sets of reviews were conducted by the leaders from KPMG in India, nasscom and DSCI. Inputs received from esteemed industry leaders were also considered prior to finalising the content of the report.

Acknowledgements

Our sincere thanks to all the GCCs who invested their valuable time to give us inputs and contribute to this report.

Our special thanks to the advisory panel including Ramachandra Kulkarni and Vinayak Godse for their strategic direction, right from conceptualisation to the launch of the report.

Our thanks to all the KPMG in India Partners, Directors and colleagues who assisted in survey formulation and completion. We acknowledge the efforts put in by the following team members for publication of this report.

KPMG in India

- Abhijith A
- Adithya Jakkaraju
- Adithya V
- Akram Md
- Amal Anand
- Anand Gopalakrishnan
- Anupriya Rajput
- Anushka Khandelwal
- Avanti Premkumar
- Darshini Shah
- Dhruv Tangri
- Harleen Handa
- Harsh Jalan
- Ira Punj
- Karthik JCS
- Karthika Prabasankar
- Mano Lingam V
- Mehul Poojary
- Niharika Pariwal
- Nischay Edmund Paschal
- Nisha Fernandes
- Niveditha Rathore
- Piya
- Poorvi Sahni
- Ravi Ranjan
- Ritwik Tiwari
- Sabi Ul Haque Naimi
- Sameer Hattangadi
- Saritha Naga Rana
- Saumya Mehta
- Sonali Gupta
- Sowmya Sampath Kumar
- Yogesh Gupta
- Zeeshan Khan

nasscom

- Achyuta Ghosh
- Sukanya Roy

DSCI

- Vinayak Godse, CEO of DSCI
- Dr. Sriram Birudavolu, CEO - Cyber Security, CoE
- Atul Kumar, Lead – Government Initiatives & Global Trade
- Ankit Bhadola, Deputy Manager Research

We acknowledge the efforts put in by the core team of **Secure in India 2023**, right from initiation to publication of this report.

About KPMG in India

KPMG entities in India are professional services firm(s). These Indian member firms are affiliated with KPMG International Limited. KPMG was established in India in August 1993. Our professionals leverage the global network of firms, and are conversant with local laws, regulations, markets and competition. KPMG has offices across India in Ahmedabad, Bengaluru, Chandigarh, Chennai, Gurugram,

Hyderabad, Jaipur, Kochi, Kolkata, Mumbai, Noida, Pune, Vadodara and Vijayawada.

KPMG entities in India offer services to national and international clients in India across sectors. We strive to provide rapid, performance-based, industry-focused and technology-enabled services, which reflect a shared knowledge of global and local industries and our experience of the Indian business environment.

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their

agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

About nasscom

nasscom, a not-for-profit industry association, is the apex body for the \$245 billion technology industry in India, an industry that has made a phenomenal contribution to India's GDP, exports, employment, infrastructure and global visibility. In India, this industry provides the highest employment in the private sector.

Established in 1988 and ever since, nasscom's relentless pursuit has been to constantly support the technology industry, in the latter's continued journey towards seeking trust and respect from varied stakeholders, even as it reorients itself time and again to remain innovative, without ever losing its humane and friendly touch.

nasscom is focused on building the architecture integral to the development of the technology sector through policy advocacy, and advocacy and help in setting up the strategic direction for the sector to unleash its potential and dominate newer frontiers.

nasscom's members, 3000+, constitute 90 per cent of the industry's revenue and have enabled the association to spearhead initiatives at local, national and global levels. In turn, the technology industry has gained recognition as a global powerhouse.



KPMG in India contacts:

Anindya Basu

National Managing Partner,
Head of Advisory
T: +91 98101 37997
E: anindyabasu@kpmg.com

Akhilesh Tuteja

Head Clients and Markets,
Global Cybersecurity Leader
T: +91 98710 25500
E: atuteja@kpmg.com

Shalini Pillay

Partner and Head GCC
T: +91 98440 18843
E: shalinipillay@kpmg.com

Atul Gupta

Partner and Head
Digital Trust
T: +91 98100 81050
E: atulgupta@kpmg.com

Srinivas Potharaju

Partner and Head,
Digital Risk and Cyber
T: +91 98459 19740
E: srinivasbp@kpmg.com

Pranav Kathale

Partner,
Digital Risk and Cloud Security
T: +91 97013 13472
E: pranavkathale@kpmg.com

Annapurna Alladi

Partner, Cyber Assurance
T: +91 99893 16555
E: aalladi@kpmg.com

nasscom contacts:

Sukanya Roy

Head, BPM and GCC Initiatives
T: +91 98110 00133
E: sukanya@nasscom.in

Vandhna Babu

Principal Analyst
T: +91 98999 76684
E: vandhna@nasscom.in

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia



DSCI contact:

Ankit Bhadola

Deputy Manager Research
T: +91 83739 92760
E: ankit.bhadola@dsci.in

30 years
and beyond

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is meant for e-communication only. (024_THL_1223_AR)