KPMG

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Secure in India 2020

GCC at the forefront of managing global digital risks

NASSCOM®

December 2020

home.kpmg/in

Navigator

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

Foreword

While digitisation has long been on the board agenda, the COVID-19 pandemic has expedited and brought to the fore its challenges.

Cybersecurity and digital risks have moved to the forefront, as organisations seek to maximise the benefits from digital adoption. However, in many organisations, several cybersecurity and digital risk management functions continue to be performed in a manual and 'automate only if needed' mode, an approach that urgently needs to be revisited.

One of the key principles of initiating 'Secure in India' in 2018 was to help global organisations uncover their existing or new Global Capability Centre (GCC)-based cybersecurity capabilities in managing their global cybersecurity and digital risks. Cyber GCCs bring in a blend of talent, scale and innovation, along with the commercial leverage of a global business model. This helps global leaders to manage cybersecurity and digital risks following a 'do more with less' approach. If digitisation is a key differentiator for unleashing the power of business beyond traditional models, cybersecurity and digital risk management is at the core of a sustainable and secure digital ecosystem.

While cyber GCCs have continued to solve business problems with proven methodologies and years of experience, they have also constantly challenged themselves with the latest demands of global business, regulations and emerging technologies. Cyber GCCs have made significant progress in the innovation agenda of cybersecurity and digital risk functions of their global organisations.

Secure in India 2020 captures the achievements, challenges and measures of GCCs as they continue to be at the forefront of managing global cybersecurity and digital risks. This report aims to provide innovative insights (across seven domains) that help global leaders take informed decisions, especially on leveraging the talent and experience of the cyber GCC ecosystem. The insights detailed in this report have been prepared basis an extensive study and in consultation with global cyber leaders, GCC cyber leaders, cybersecurity Subject Matter Experts (SMEs) and reputed industry bodies. It provides key recommendations for cyber GCCs to help them sustain their competitive advantage, transform into global 'centres of expertise', and enable global organisations to 'Secure in India'.

Akhilesh Tuteja
KPMG Global Leader for Cyber, Head of Digital in India

Debjani Ghosh
President, NASSCOM

Rama Vedashree
CEO, DSCI

Industry view

Think GCC, think innovation. GCC community in India, especially cyber GCCs have experienced a sea change in the last decade or so and are now uniquely positioned to deliver change when their global organisations need it the most.

'Change while you run' is key for sustaining talent and their skills. Not to mention, it is vital for sustainable business in an ever-changing business environment.

Cyber GCCs offer a unique platform where 'change the bank' meets 'run the bank' on a day-to-day basis, helping 'people who change' work closely with 'people who execute' in transforming the cybersecurity and digital risk functions.

Innovation is a lot faster, more commercial, and closer to the key business challenges that need to be addressed on a priority. Industry has been successful to experience outstanding use cases of innovation when it comes to cybersecurity engineering, digital risk, control automation and emerging technology risk, leveraging cyber GCC platform.

Ramachandra Kulkarni

Managing Director – Technology risk, Goldman Sachs

Global view

Cybersecurity is one of the most systemically important issues facing the global economy today, in under a decade. Collective global spending has now reached USD145 billion a year and it is now at the very top of leaderships' agenda in business and government.

Despite this, incidents and attacks continue to rise, and will only matter more as the global economy increasingly relies on complex interconnected digital processes and infrastructure. There is an urgent need for collective action, policy intervention and new approaches by the Government and business to address risks especially as the global economy faces a major cyber capacity gap.

The experience of the India GCCs is a major example of how the community can look to meet the growing skills and advanced capability requirements that face global businesses across the world. Enterprises require capabilities that can provide the innovation, skills and capacity to act at scale against digital attacks.

The success of the GCC model, and its maturing ecosystem has built real global partnerships and makes India a world leader in providing the global economy with digital resilience. It is a model other countries can look towards, as they face the cybersecurity challenges of the future.

William Dixon

Head of Future Networks and Technology, World Economic Forum (WEF)

Key Takeaways

1

Global organisations continue to invest in cyber GCCs to address their cybersecurity and digital risk agenda

1. Number of cyber GCCs has increased by 30 per cent since 2018. Key factors driving this trend are availability of cybersecurity skills (86 per cent), round-the-clock delivery (74 per cent), cost arbitrage (61 per cent), proximity to other business functions (49 per cent) and innovation, research and development (43 per cent)
2. About 71 per cent of cyber GCCs have their leadership reporting to global heads in parent organisation
3. About 16 per cent of cyber GCCs have more than half of their global cybersecurity staff based out of India. 25 per cent of GCCs have between 24 and 49 per cent of their global cybersecurity staff based out of India
4. More than 40 per cent of cyber GCCs deliver part of all cybersecurity functions from India

2

Cybersecurity skills availability continued to be the top driver for cyber GCCs' success story:

1. About 41 per cent of cyber GCCs have global cybersecurity teams report to the GCC cyber leadership for specific functions
2. Maximum increase in skill demand in cyber GCCs was noted for cloud security (80 per cent), cybersecurity product management and automation (70 per cent), cyber risk assessments (67 per cent), secure development (67 per cent), cybersecurity operations (67 per cent), cyber resilience (64 per cent) and emerging technology risk (62 per cent)
3. About 88 per cent of cyber GCCs believe that diversity is a key agenda for cybersecurity function

3

Systemic focus on innovation makes cyber GCCs key to global innovation agenda

1. About 75 per cent of cyber GCCs have a focused program for innovation
2. About 25 per cent of cyber GCCs collaborate with start-ups for innovation programs to achieve faster and lower cost of innovation
3. About 42 per cent of cyber GCCs have cybersecurity product management and automation function

4

Cyber GCCs getting future ready

1. About 78 per cent of cyber GCCs are using cloud platforms for various cybersecurity functions
2. Artificial Intelligence (AI) technology is currently used by 39 per cent of cyber GCCs and 32 per cent are planning to use it
3. About 40 per cent of GCCs are supporting global agenda to address emerging technology risks and cloud security risks

5

Cyber GCCs enabled global majors respond to the pandemic challenge

1. COVID-19 proved cyber GCCs offer resilience – 69 per cent of the GCCs took less than 24 hours to start working remotely
2. Cyber GCCs helped their global offices win the stress test – 75 per cent of cyber GCCs enabled their global offices in dealing with the COVID-19 pandemic
3. About 39 per cent of cyber GCCs reported no change in the operational efficiency of their cybersecurity team while working remotely. Another 39 per cent of the cyber GCCs reported that the operational efficiency was slightly enhanced

01

Cybersecurity in the digital era

Digital technology adoption has rapidly increased in the last couple of years, especially following the outbreak of COVID-19. While organisations worldwide have been focused on managing cybersecurity and digital risks from known and unknown cybersecurity threats, the rise of digitisation, along with COVID-19 led disruption, has pushed digital risks into the spotlight.

Digital Risk Debt (DREBT) - Global organisations have been responding to the COVID-19 and pre-COVID-19 (DREBT), working closely with their business and operations. They face the twin challenge of protecting business and ensuring growth while riding the digital wave.

Cyber GCCs are at the centre of 'future of work' initiatives of organisations across the world, presenting a reliable, commercial and resilient operating model. Cyber GCCs enable global organisations to not only offer a commercial and scalable solution to plug their DREBT but also help secure the 'future of work' initiatives of their global offices.

Secure in India 2020 - Global CISOs, GCC leaders, GCC cybersecurity leaders and cyber SMEs have participated in the Secure in India 2020 study and shared key insights and perspectives on how global organisations are leveraging cyber GCC capability in managing global cybersecurity and digital risks.

This document also uncovers leaders' insights on cybersecurity in the digital era, empowered by cyber GCCs.

"While digitisation has been on the agenda of every global board, the onset of COVID-19 has accelerated digitisation to the top gear. Globally, cybersecurity has become a key concern in this digital transformation journey and digital risk and cybersecurity are at the core of any global organisation's priorities to ensure business continuity and resilience. India's conducive business environment along with its rich talent pool and innovation capabilities is attracting global enterprises to establish their GCCs in India.

The Indian GCCs bring in a rare blend of talent, experience and innovation, while driving competitive advantage for enterprises from the U.S., Europe and Asia and transforming them into global 'centres of expertise', while enabling them to 'Secure in India'. The Government of India and MeitY are committed to make India a global hub and a preferred destination for Cyber GCCs."

Ajay Prakash Sawhney,
Secretary, Ministry of Electronics & Information Technology

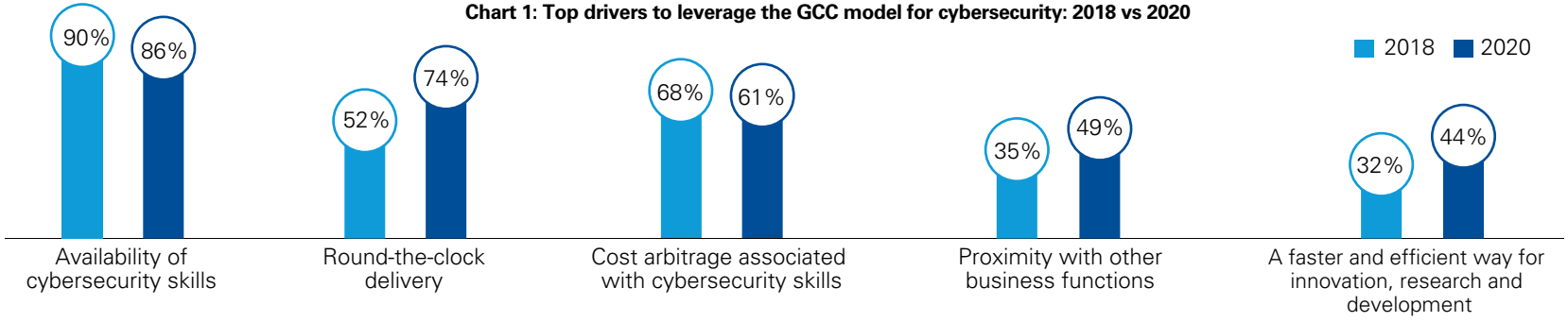
Empowering global cybersecurity and digital risk management with the GCC model

The top three drivers for cyber GCCs

#1 Cybersecurity talent availability continues to be the top driver

'Availability of cybersecurity skills' trumps all other factors in leveraging the GCC model in India. A staggering 86 per cent of the cyber GCCs surveyed believe that this is a key driver. India, with its enormous talent pool, offers a wide variety of skillsets essential to functions across the spectrum of cybersecurity.

Chart 1: Top drivers to leverage the GCC model for cybersecurity: 2018 vs 2020



#2 Cyber GCCs offer 'round-the-clock delivery' advantage

Of the respondents surveyed, 74 per cent agreed that 'round-the-clock delivery' was a key driver to leveraging the GCC model in India. As cybersecurity and digital risks grow multifold, global organisations see a clear need for round-the-clock capabilities in specific cybersecurity and digital risk functions. Since 2018, 'Round-the-clock delivery' driver has registered the maximum increase of 22 percentage points and reflects the growing importance of managing cybersecurity and digital risks across different timezones.

#3 Cost arbitrage still matters

About 61 per cent of the survey respondents believe that 'cost arbitrage associated with cybersecurity skills' is another key driver to leverage the GCC model for cybersecurity. This reflects that India continues to be efficient in managing cybersecurity and digital risks.

More innovation from cyber GCCs

About 44 per cent of the cyber GCCs surveyed consider 'a faster and efficient way for innovation, research and development' as a key driver for leveraging the GCC model. This has gained 12 percentage points from 2018[1]. Of GCCs established after 2018, 75 per cent hold this view, indicating that newer GCCs are being set up with an innovation focused mindset

Cyber GCCs are a natural choice, as GCCs expand their presence in more business functions. About 49 per cent of GCCs surveyed consider 'proximity to key business functions' as a key driver to leveraging the GCC model. This has gained 14 percentage points since 2018.

- Of the cyber GCCs surveyed, 71 per cent are multifunction centres, with influential leadership seated at GCC, and several of them reporting to global heads in their parent organisations. This is a huge jump as compared with 39 per cent of cyber GCCs that had the same structure in 2018.
- Amongst the cyber GCCs surveyed, those established after 2018 are multifunction centres, with influential leadership seated at GCC, and several of them reporting to global heads in parent organisation. This is reflective of the increased maturity of cyber GCCs setup recently.

The cyber GCC capability is growing

A majority of the cyber GCCs in India are now multifunction centres with influential leadership. The cyber GCCs have been keeping pace with digital technologies and hence, are delivering key functions to their parent organisations. Cyber GCCs have also been expanding beyond major cities in India.

Chart 2: Cyber GCC structure 2018 vs 2020

Single function centre represented by mostly managerial leadership with one local head, reporting to business leaders of parent organisation

Multifunction centre, reporting to multiple business leaders of parent organisation, with only operational oversight by local head

Multifunction centre with influential leadership seated at GCC, and several of them reporting to global heads in parent organisation

1. Secure in India, KPMG in India. Released in June 2018.

02

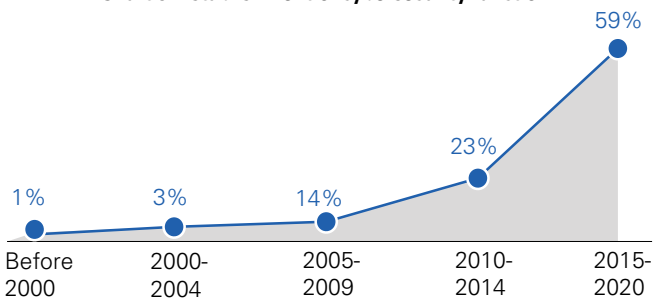
Extended cyber global organisation

Cyber GCCs in India continued on their maturity journey, measured in terms of number of functions, function complexity and function leadership, over the last two years. They have played a vital role in the overall security posture of global organisations.

Cyber GCCs continue to be preferred global delivery partners

#1 Cyber GCCs have consistently grown over the years

Chart 3: Establishment of cybersecurity function

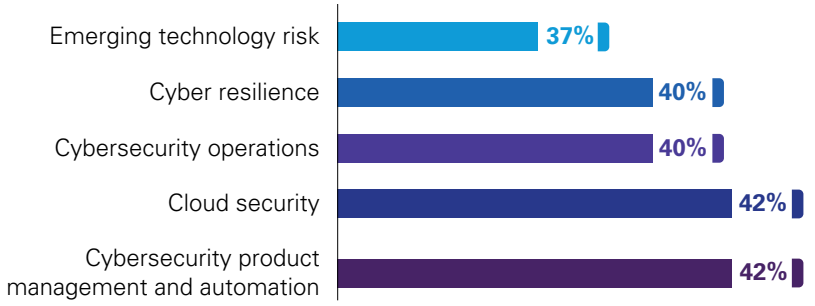


- Cyber GCCs have more than doubled in the last five years. This period witnessed 58 per cent of GCCs establishing their cybersecurity function

#2 Surge in 'next gen'[1] digital risk functions

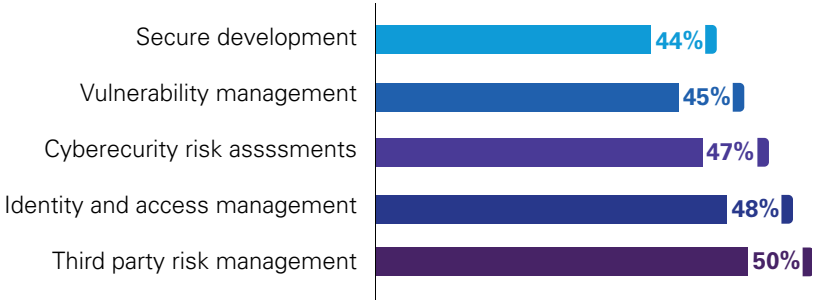
As compared to 2018, digital risk has grown exponentially. To counter this, global majors have started leveraging cyber GCCs to perform 'next gen' functions such as emerging technology risk, cyber resilience, cloud security, cybersecurity operations and cybersecurity product management and automation.

Chart 4: Top 5 'Next gen' cybersecurity functions being delivered from cyber GCCs



#3 'Core'[2] cybersecurity functions continue to register significant growth

Chart 5: Top 5 'core' cybersecurity functions being delivered from cyber GCCs



Functions such as secure development, third party risk management, cybersecurity risk assessments, identity and access management and vulnerability management continue to expand and form part of the core pillars of cyber GCCs.

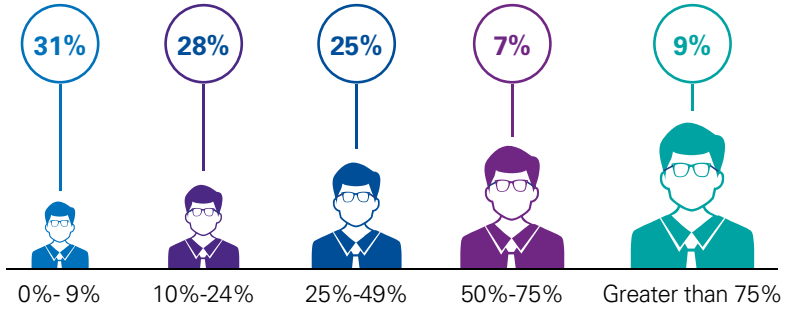
1. 'Next gen' functions refer to cybersecurity and digital risk functions such as emerging technology risk, cyber resilience, cloud security and cybersecurity product management and automation
2. 'Core functions refer to cybersecurity and digital risk functions such as secure development, vulnerability management, cybersecurity risk assessments, identity and access management and third party risk management.

"Global capability centres are extremely adaptable and are generally considered to be higher performing than their counterparts. GCCs with their astute workforce, and swift delivery speeds are highly effective and should be leveraged by private and public sector alike." - **Ben Goerz**, a Fortune 500 company executive

#4 Cyber GCCs emerge as nerve centres of global cybersecurity

A majority of survey respondents highlighted that a significant share of their global cybersecurity workforce is now based in cyber GCCs.

Chart 6: Share of global cybersecurity staff based in India



- About 41 per cent of the cyber GCCs surveyed had at least a quarter of their global cybersecurity teams based in India
- About 16 per cent of the cyber GCCs surveyed have more than 50 per cent cybersecurity staff based in India
- There is further room for expansion for cyber GCCs as 31 per cent of the GCCs surveyed still have less than 10 per cent of their global cybersecurity staff based out of India

Cyber GCCs spend a lion's share on core functions

Cyber GCCs, over the years, have been delivering core functions, aligned with priorities and budget allocation of their global majors. However, it is interesting to note that not all cyber GCCs prioritise the same functions. This could be due to varied organisational and budget priorities.

#1 Top cybersecurity functions based on budget allocation

Chart 7: Top 5 cybersecurity functions based on budget prioritisation

Over and above the top five cybersecurity functions represented in Chart 7, Secure development, technology regulatory, audit and standards compliance management, cybersecurity strategy and governance, data privacy and cloud security are the next five key functions prioritised by budget.

#2 Vulnerability management and Identity and Access Management (IAM) are consistently prioritised across sectors

Although cybersecurity functions are prioritised in a varied manner across sectors, vulnerability management and identity and access management have clearly emerged as two key functions that are in the top five functions across all the sectors. Beyond execution of these functions for day-to-day operation, cyber GCCs have started contributing towards transformation of these functions.

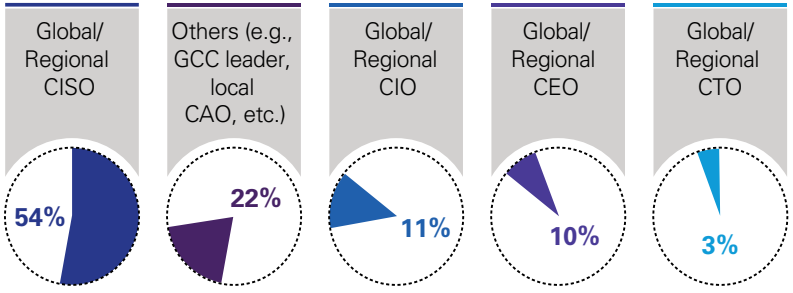
Growing stature of GCC cybersecurity and digital risk leadership

The increasing scope and complexity of cybersecurity and digital risk functions delivered from cyber GCCs has been accompanied by the rise of GCC cyber leadership profile. Teams focused on cybersecurity and digital risks in GCCs have grown significantly over the last two years, and there has also been a significant increase in contribution to global cyber leadership matters.

#1 Cyber GCC leaders reporting more to global/regional executives

About 78 per cent of cyber GCCs surveyed have their cyber leaders reporting into global executives

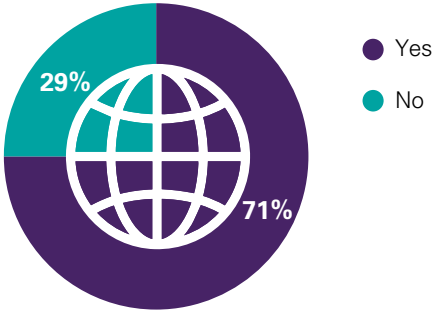
Chart 8: Whom does the GCC CISO report to?



- Reporting lines for the GCC CISO[3] reflect the growing importance of cybersecurity functions. About 24 per cent of GCC CISOs report into global executives other than global CISOs
- About 54 per cent of the survey respondents reported that their GCC CISO reports to the global/regional CISO
- About 10 per cent GCCs have their CISOs reporting to global/ regional CEOs.

#2 Cyber GCC leaders are key members of global cybersecurity and digital risk committees

Chart 9: Does the cybersecurity leadership serve on global committees?

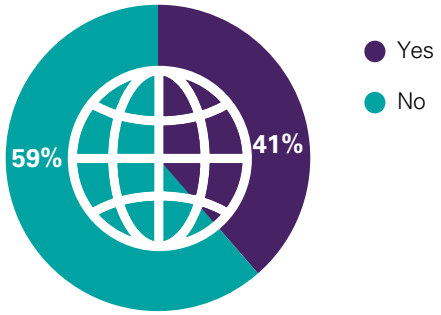


- Around 71 per cent of GCCs surveyed have their GCC CISO or other members of cybersecurity leadership of cyber GCCs serve on the global committees (e.g., global cybersecurity committee, global risk committee, etc.)
- Many GCCs have cyber leaders managing governance and agenda of key global cybersecurity committees.

3. GCC CISO could refer to the chief information security officer, cybersecurity head, IT security head, digital security head or technology risk head.

#3 Rise in global cybersecurity and digital risk teams reporting into cyber GCC leadership

Chart 10: Are global teams reporting to India GCC CISO?



- About 41 per cent of the survey respondents concur that employees from global teams report to the GCC CISO
- This represents an increase in GCC cybersecurity and digital risk leadership taking up global leadership roles.

#4 Cyber GCCs focus across lines of defense

About 88 per cent of the survey respondents highlight that they perform cybersecurity and digital risk activities relevant to the Three Lines of Defense (3LOD).

Chart 11: Cybersecurity presence across the three lines of defense

03

Cybersecurity and digital risk workforce

The availability of the cybersecurity and digital risk workforce continues to be the primary factor for the rise of Cyber GCCs. A large skilled cybersecurity workforce with sustained growth has enabled round-the-clock delivery model with significant cost arbitrage. To address the exponential increase in demand for cybersecurity and digital risk skills, cyber GCCs have implemented various talent retention and management strategies.

Cybersecurity and digital risk workforce continue to grow

#1: Rise in demand for digital risk skills

In line with the global demand of next generation cybersecurity digital risk functions, cyber GCCs registered the highest rise in skill demand in the domains of cloud security, cybersecurity product management and automation and emerging technology risks.

The surge in cyber-attacks and increased regulatory focus on operational resilience across the globe have resulted in cyber GCCs strengthening their regulatory compliance and cyber resilience skills further.

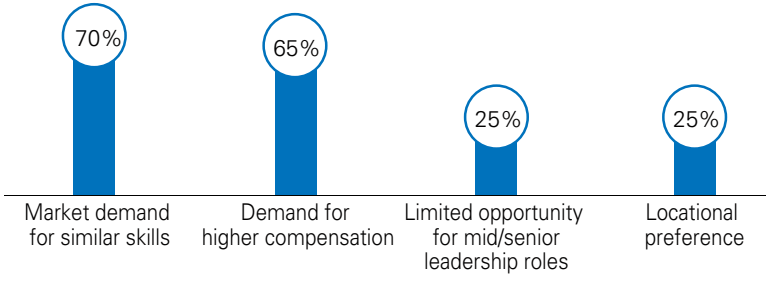
Chart 12: Cybersecurity functions with rising skill demand

#2: Supply for specific cybersecurity and digital risk skills continues to be a key challenge

Cyber GCCs continue to face challenges (refer to chart 13) in specific cybersecurity and digital risk skill areas (refer to chart 12). Top challenges faced by cyber GCCs in attracting and retaining talent are market demand for similar skills and persistent demand for higher compensation.

Some respondents have experienced that the brand visibility of their respective GCCs is limited. Additionally, awareness of development opportunities, advanced cybersecurity and digital risk functions and opportunities for global assignments in organisations with limited brand visibility in the cyber GCC market are key challenges faced by new cyber GCCs.

Chart 13: Challenges in attracting and retaining talent



"While talent attraction is important, retention is more important. An organisation which encourages rotation across diverse roles within cybersecurity stands a better chance of lower attrition rate than the one which does not.

Continuous upskilling and engagement through well-planned training initiatives, cybersecurity events and conferences might sound like a no-brainer; but needs to be exceptionally executed to further help in nurturing the growth environment."

Vikas Kapoor,
VP – Cyber security
Vodafone

#3: Annual cybersecurity attrition rate dwindles

In 2018, survey respondents experienced an average attrition rate of 10-15 per cent for their cybersecurity and digital risk workforce. This has declined substantially in 2020, with over 59 per cent of survey respondents highlighting that their annual attrition rate is around 0-7 per cent and 28 per cent highlighting it as 8-15 per cent.

Many cyber GCC leaders participating in the survey attributed the reduced attrition rate in 2020 to a combination of better talent management strategies and the pandemic.

Chart 14: Cybersecurity attrition rate across GCCs

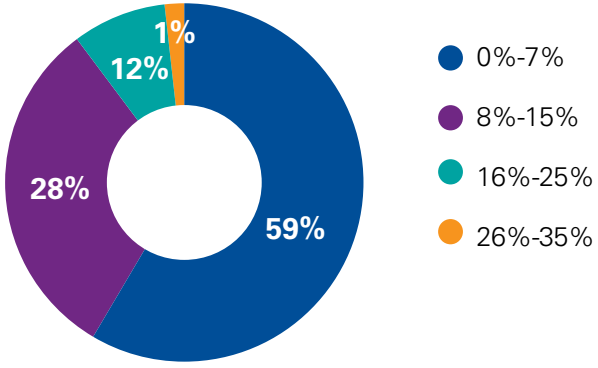


Chart 15: Cybersecurity attrition rate over the years

Addressing the demand for cybersecurity and digital risk skills

As the demand for cybersecurity skills increases, cyber GCCs are implementing strategies such as reskilling (46 per cent), hiring externally (35 per cent), using service providers (17 per cent) and leveraging the gig workforce (2 per cent).

#1: Getting the right skills

Cyber GCCs have identified preferred mode of talent acquisition basis skill required. They have chosen external hiring and in-house training for cybersecurity and digital risk functions, where scale or technical depth or future-oriented skill is involved.

Chart 16: Top cybersecurity functions with external hire as the preferred option

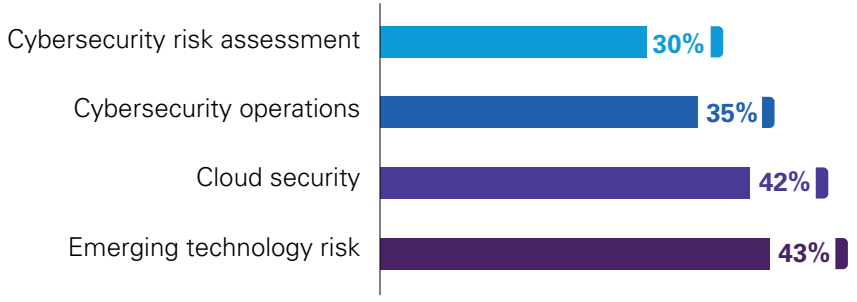
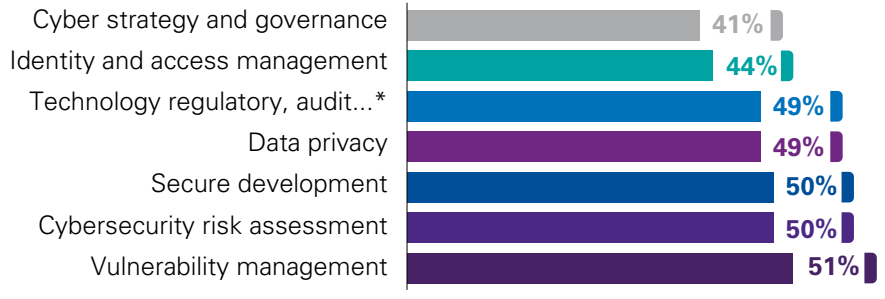


Chart 17: Top cybersecurity functions with In-house training as the preferred option



* Technology regulatory, audit and standards compliance management

- Service providers are the preferred mode for talent sourcing in the following scenarios:

    1. Necessitated by the type of function (technology regulatory, audit and standards compliance management - 21 per cent and cyber forensics - 12 per cent)

    2. Functions requiring additional capacity (cybersecurity operations - 16 per cent)

    3. New age skill sets, where not available within cyber GCCs (emerging technology risk - 22 per cent and cloud security - 15 per cent)

- Cyber GCCs in India have started exploring gig workforce to deliver short assignments, as and when required. From being virtually non-existent a few years ago, 2020 has seen notable functions delivered via the gig workforce mode, especially secure development, cloud security, cybersecurity operations, emerging technology risk and cybersecurity product management and automation.

#2: The cyber GCC reskilling revolution

Majority of respondents said that the preferred mode of talent acquisition is in-house training (46 per cent).

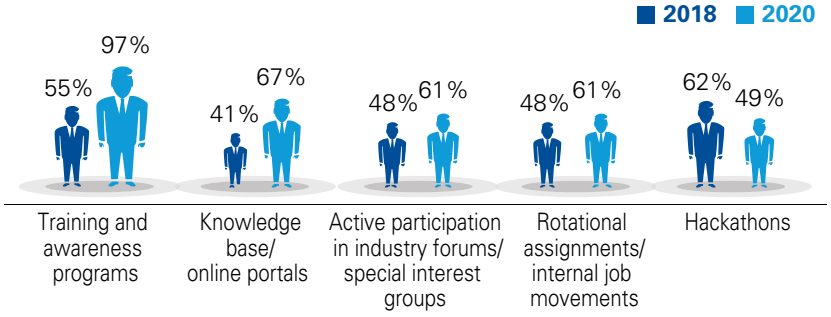
Reskilling initiatives dominate talent acquisition methods. Many cyber GCC leaders highlighted that lateral movement of staff from technology-based functions to cybersecurity has proven to be a successful approach to leverage contextual, business, technology, organisational skills and experience for managing cybersecurity and digital risk functions.

#3: Training and awareness programs lead the way

For cyber GCCs, training and awareness programs (e.g., external/internal/digital learning, certification programs, professional examinations, workshops, etc.) remain the most popular means to upskill and reskill in both 2018 and 2020. Cyber GCCs are also investing in maintaining an organisation-wide knowledge base/online portal (technical publications, thought leadership reports, research reports, survey reports, etc.) to upskill talent.

In 2020, Cyber GCCs are also employing a range of initiatives like collaborative learning (64 per cent), gamification (including war games, hackathons, bug bounties, Capture The Flag (CTF), immersive labs and simulations) (49 per cent), and crisis simulation (26 per cent).

Chart 18: Initiatives employed to upskill talent



"Compensation is not the only driver for employees in India. The realisation that their work and individual contribution can affect thousands of other people is an important motivator. Upskilling is key to talent retention. Focused upskilling strategies at the individual's level should be aligned with the organisation's aspirations in a holistic manner." **Shobha Jagathpal,** Director - Information security, Walmart Global Tech

#4: Diversity empowers cybersecurity

Inclusion and diversity across the cybersecurity and digital risk functions, have become key for cyber GCCs in the recent years. About 88 per cent of the survey respondents highlighted that diversity was a key agenda for their GCC cybersecurity and digital risk function.

Visagan Subburayalu,
Director-Technology,
Target in India

"Diversity is a business imperative at Target and for our cybersecurity teams as well. That's why, we're investing in developing a strong pipeline of diverse talent right from hiring to talent retention and development.

We've created an award-winning forum - Security Women at Target in India (SWATI) that encourages women in technology to share their knowledge externally via. white papers, participate in industry gatherings/conferences, host hackathons and participate in community initiatives.

We're also providing exclusive development opportunities for women in engineering through the Engineering Manager Immersion Program (eMIP) which aims to increase the number of women leaders in our technology teams."

Cyber GCCs are investing in focused programs such as Returnship, Working Mothers Assistance, communities of interest initiatives etc to encourage and sustain diverse talent.

Many cyber GCCs are leveraging their global organization engagement with global, regional and local platforms (e.g., Women in Cybersecurity - WiCyS and International Women of Risk - IWOR) and are aligning their cyber GCC talent to participate in the forums organised by such platforms.

04

Innovation @ cyber GCCs

In 2020, 43 per cent respondents believe that innovation is a key driver to leverage the GCC model for cybersecurity. This number has increased by 13 per cent from 2018.

"India provides a unique opportunity to the world in providing innovative solutions to address the cyber risks. GCCs are very well positioned to leverage this potential and create next generation solutions for global organisations.

We have already experienced outstanding GCC contribution to global cyber innovation, whether it is process or service innovation, platform and asset oriented innovation and also believe that there is lot more where GCCs will be able to contribute."

Atul Gupta,
Head IT Advisory and Cyber Leader, Digital - KPMG India

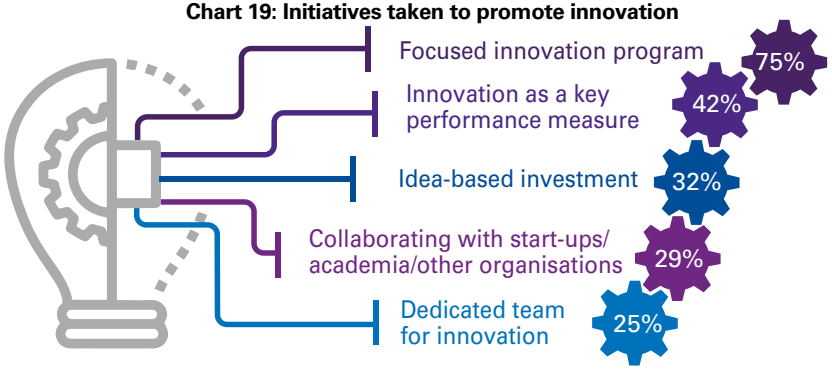
Cyber GCCs building innovation momentum

#1: Focused programs are top drivers for cyber GCC innovation

Cyber GCCs are focused on promoting system or program-based innovation (75 per cent of survey respondents) as well as employee KPI driven innovation programs (42 per cent of survey respondents).

Other initiatives include integration and engagement with the parent organisation teams for innovation and setting up innovation hubs.

Chart 19: Initiatives taken to promote innovation



As an external lever for innovation, GCC community has harnessed the collective capability of the larger ecosystem beyond their organisational boundaries, collaborating with other GCCs, academia and start-ups.

Various GCC forums, start-up engagement events, academia, community exercises and hackathons/events have been organised time to time, in order to learn, experience and fast track innovation.

An industry-wide GCC Ideathon was recently organised, where GCCs along with selected technology alliance and innovation partners gathered to conduct hacks focused on emerging technologies (such as Artificial Intelligence (AI), Machine Learning (ML), Distributed Ledger Technology (DLT), etc.) to solve curated business problems.

#2: Key cyber innovation use cases

Most of the surveyed cyber GCCs have embarked upon innovation initiatives and some of them have shared a few select examples, as part of the survey response.

Below is a select list of cyber innovation use cases:

Process Innovation:

1. Improvement in security monitoring and incident response processes by leveraging Robotic Process Automation (RPA) for end-to-end cyber defense processes
2. Crisis simulation and response (including regional handover testing)
3. Development of in-house 24/7 Capture The Flag (CTF) platform, used to upskill employees in both tech and non-tech roles
4. Service automation to streamline the approval process to change firewall rules
5. Use of RPA for automated execution of user access management functions
6. Leverage RPA for seamless service account password changes
7. User Developed Application (UDA) risk management
8. AI and ML risk management
9. RPA and low code/no code platform risk management
10. DLT risk management.

Platform Innovation:

1. Development and maintenance of automated risk and control measurement engines (integrated risk assessment platforms, automated continuous control monitoring, automated issue assignment, escalation and remediation, etc.)
2. Development of third party risk management platforms
3. Customisation of open-sourced application security platforms
4. Development and maintenance of global cybersecurity reporting and dashboarding
5. Implementation of Security Orchestration, Automation and Response (SOAR) for Security Operations Centre (SOC) automation to accelerate incident detection and response
6. Digital risk insights platform for continuous risk profiling of key business relationships
7. Development and maintenance of various in-house eGRC (governance risk and compliance) platforms
8. ML empowered surveillance analytics
9. Development and management of technology risk data lake
10. AI empowered assessment platforms to process third party submitted compliance evidence reports
11. Cloud security automation (including compliance as a code)
12. Internet of Things (IoT) security monitoring
13. Operational Technology (OT) security monitoring.

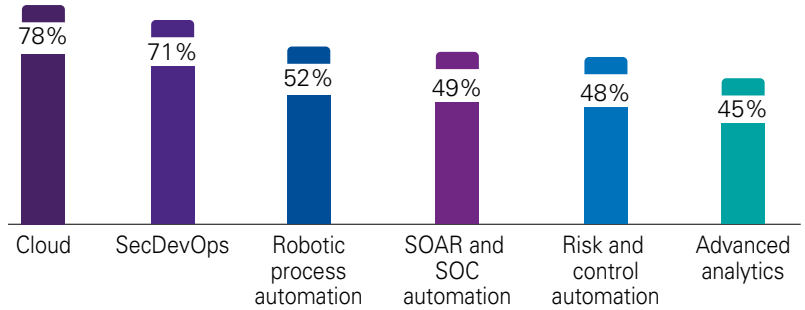
Increased adoption of emerging technologies across cybersecurity and digital risk functions

#1: Focus on secure cloud enablement and automation

Enterprise-wide cloud adoption of cybersecurity functions has accelerated (78 per cent of cyber GCCs surveyed).

Cyber GCCs have a clear focus on automation of cybersecurity functions leveraging RPA (52 per cent), SOAR and SOC automation (49 per cent), risk and control automation (48 per cent) and advanced analytics including ML (45 per cent).

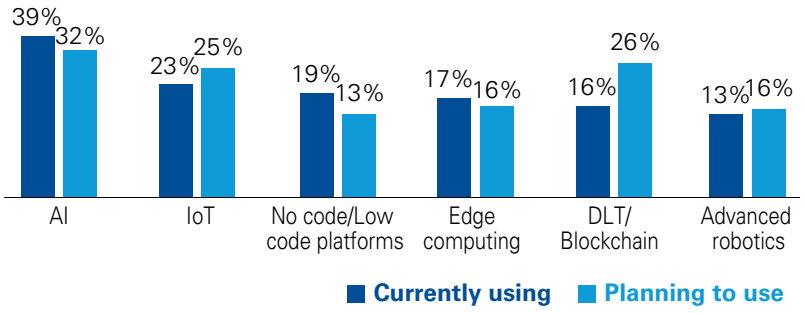
Chart 20: Top 5 emerging technologies leveraged by cybersecurity functions in cyber GCCs



#2: AI – The next big move

About 71 per cent of surveyed cyber GCCs highlighted the importance of AI to their global organisations. AI is already being used for cybersecurity by 39 per cent of the survey respondents and is the most planned to use technology (32 per cent).

Chart 21: Top six emerging technologies explored by cyber GCCs



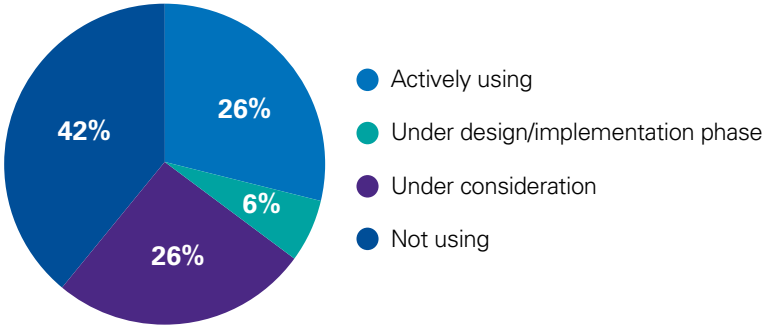
Key cyber GCC use cases for emerging technologies

- Leverage risk and control automation to automate privilege recertification
- Use of AI for detection of sophisticated multistage attacks
- Use of AI to prevent mobile devices from clicking pictures of the screen
- Protect public cloud infrastructure using advanced analytics and machine learning
- Use of machine learning techniques for User and Entity Behaviour Analytics (UEBA)
- Automation of Identity and Access management using RPA for end-to-end identity management journey
- Automated cybersecurity monitoring, alert management and content enrichment using RPA and SOAR
- Leverage No code/Low code platforms for serverless infrastructure to handle file transfers and sandboxing
- Use of No code/Low code platforms to supplement Security Information and Event Management (SIEM) capabilities including additional cloud developments
- Edge computing technology to facilitate zero trust security and conditional access, mobile device management, multi-factor authentication using biometrics.

#3: Adoption of open-source technologies for cybersecurity is growing

About 52 per cent are either using or considering open-source technologies for cybersecurity and digital risk functions.

Chart 22: Adoption of open source technologies



Key cyber GCC use cases for open-source technologies:

Incident Management:

- Kafka and KSQL - Real time threat monitoring by integrating KSQL and Kafka
- Log stash – Log collection and monitoring using log stash
- Big data platform for log collection - Log collection and repository in a big data platform and near real time search using elastic search
- NX Log – real time log monitoring and threat detection using NX Log
- Syslog NG - Log collection and monitoring using Syslog NG
- Osquery – End point security posture monitoring using Osquery
- OSINT - Integration of OSINT based Threat intel platform with SIEM for efficient threat detection.

Application Security:

- ZAP based custom solutions for Dynamic Application Security Testing (DAST)
- Open-source technology for source code review – Cyber GCCs are leveraging open-source tools to facilitate continuous code review processes and support collaboration across teams, in addition to commercial off the shelf products
- GitHub containers - Secure code storing and handling using GitHub containers.

Security Awareness:

- Gophish - phishing simulation using gophish.

Cyber GCCs play a key role in software asset management

Most of the cyber GCCs surveyed have a dedicated cybersecurity function to secure their global organisations throughout the lifecycle of Software Asset Management (SAM).

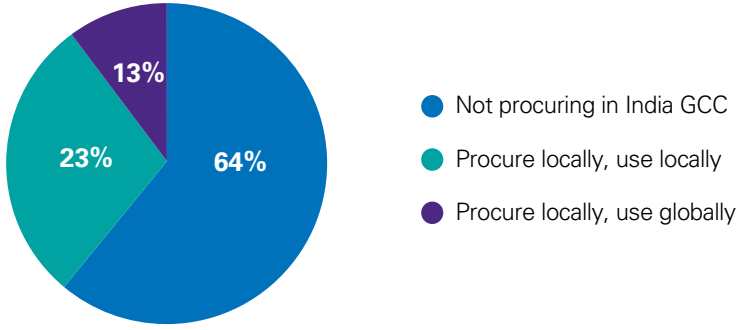
#1: Opportunity to optimise cost – GCC led software procurement

About 64 per cent respondents stated that they are not procuring software locally for use in cyber GCCs. However, it is interesting to note that 23 per cent of GCC respondents are now procuring software locally for use in cyber GCCs.

Whereas almost 13 per cent of respondents have claimed that they have gone a step ahead and are now responsible for procuring software locally for use both locally and globally.

Apart from the cost, companies may want to evaluate tax implications arising from any change in procurement model.

Chart 23: Mode of software procurement



#2: Cyber GCCs securing the software lifecycle

Cyber GCCs are emerging as hubs for assessing the security of software products used across the organisation, throughout their lifecycle (71 per cent of cyber GCCs surveyed).

End-of-Life (EoL) and End-of-Support (EoS) tracking

Many GCC leaders have highlighted that tracking critical business application run on EoL software and change or remediation strategies is one of the top ten risks presented to their global boards. About 74 per cent respondents have maintained a track of End-of-Life (EoL) and End-of-Support (EoS) of software.

Chart 24: Security review of software

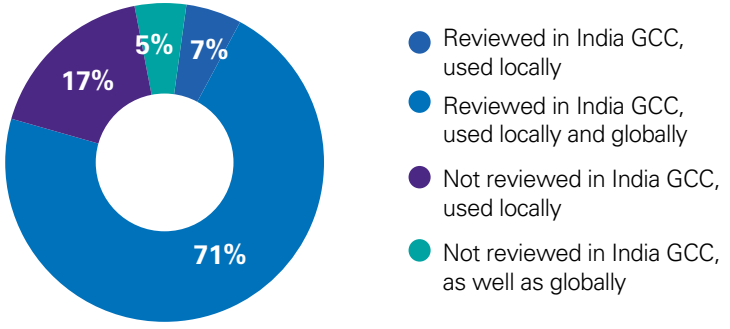
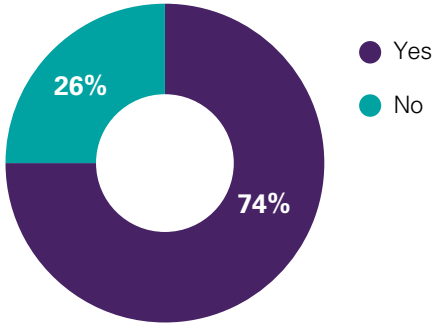


Chart 25: EoL/EoS Tracking



05

Cyber GCCs fostering risk Culture

What keeps the cyber GCC leadership awake?

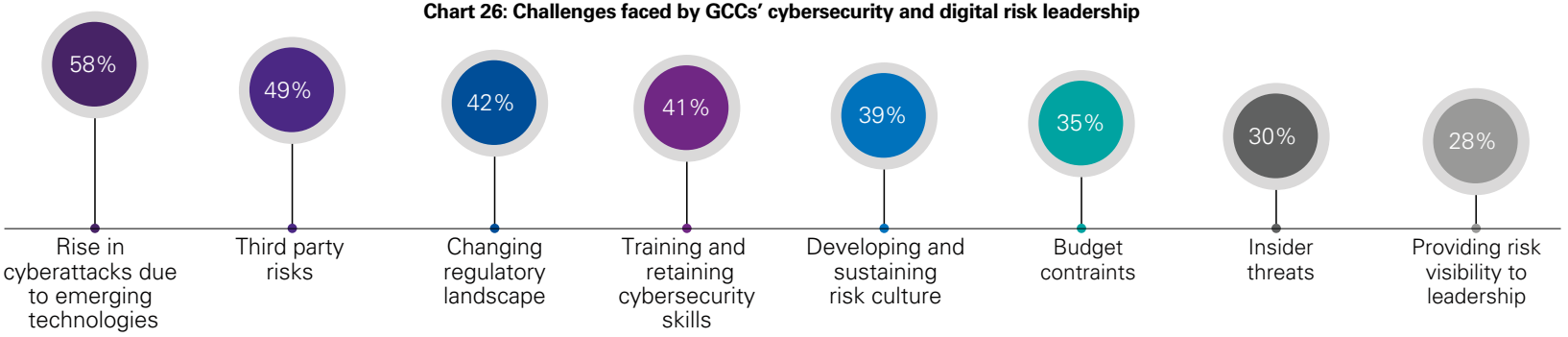
#1: Key challenges faced by cyber GCC leadership

Cyber-attacks have shown an elevating trend including rise in risks associated with emerging technology (58 per cent), attacks originating from third parties (49 per cent) and insider threats (30 per cent). Additionally, GCC cybersecurity and digital risk leadership faces challenges from a continuously changing regulatory landscape (42 per cent) and increasing budget constraints (35 per cent).

While cyber GCCs in India are trying to foster a cyber risk culture in their organisation, 39 per cent respondents are dealing with the highs and lows of developing and sustaining risk culture. About 28 per cent also agree that providing risk visibility to the leadership or the board is a challenge.

Other challenges, especially in the light of the pandemic, involve the effectiveness of the cyber resilience framework of the organisation.

Chart 26: Challenges faced by GCCs' cybersecurity and digital risk leadership



#2: Top ten cyber threats

Many cyber GCCs are now looking at themselves at Tier 4 (processes are continually improved and automated) when it comes to dealing with cyber-attacks like phishing, malware, password attack, etc.

Top Cyber threats GCCs deal with

1. Insider threat
2. Drive-by Download
3. Rogue software
4. Advanced Persistent Threat (APT)
5. Man-In-The-Middle (MITM)
6. Social engineering
7. Data breach
8. Ransomware
9. Denial of Service (DoS)
10. Password attacks

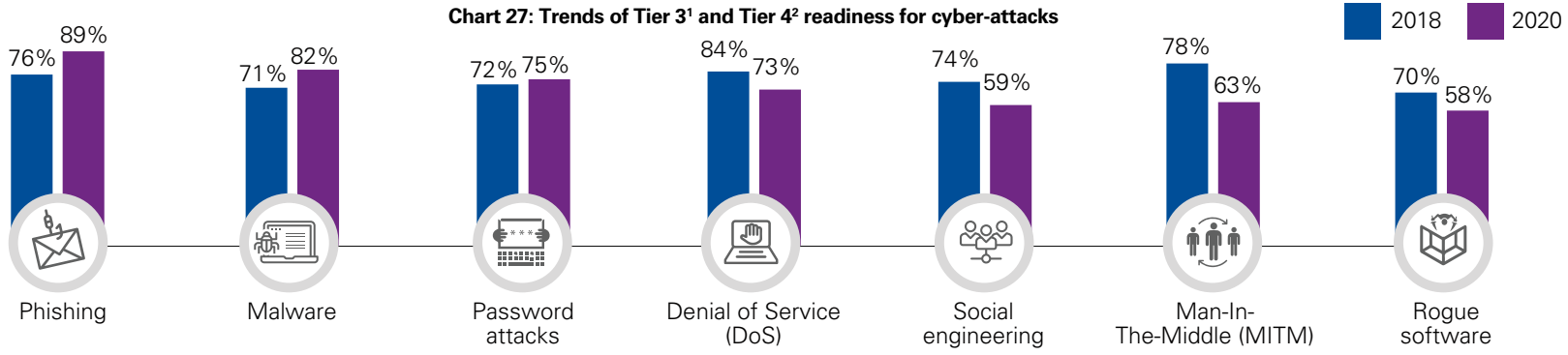
#3: Dealing with sophisticated cyber-attacks

A comparison of trends between 2018 and 2020 provides deeper insight into the rapidly evolving cyber threat landscape.

Cyber GCC functions in 2020 saw an increase in readiness level for attacks like phishing (13 per cent), malware (11 per cent) and password attack (3 per cent) as compared to 2018.

Although cyber GCCs are now more mature, the increase in sophistication of cyber-attacks has outpaced the level of preparation of GCCs. It was noted that there has been a significant decrease in readiness levels for cyber-attacks like DDoS (11 per cent), social engineering (15 per cent), man in the middle (15 per cent) and rogue software (12 per cent) when compared to 2018.

Chart 27: Trends of Tier 3[1] and Tier 4[2] readiness for cyber-attacks



GCCs imbibing cyber risk culture

Most cyber-attacks occur due to human error or behaviour which may be malicious in nature. It is now crucial for organisations to shift their focus on the capability building and cultivating a risk aware culture.

"CISOs need to move beyond being compliance monitors and enforcers, to better integrate with business, manage information risks more strategically, and work towards a culture of shared cyber-risk ownership across the organisation. Organisations will need to re-establish effective controls over new working models (hybrid, home & office), re-visit their business resilience and embrace newer security models based on zero trust principles, orchestration & automation."

Tarun Kumar, Nissan Digital India

1. Tier 3 - The processes to address cyber-threats is measured and improved.
2. Tier 4 - The processes to address cyber-threats is continually improved and automated.

#1: Training and awareness programs key to develop a cyber risk culture

Training and awareness remains fundamental to promoting risk culture (93 per cent). This is well supported by an organisation's commitment to promote cyber risk culture (87 per cent), and implementation of recognition and incentivisation measures (46 per cent).

Other 15 per cent respondents have also explored gamification, simulation and bug bounty programs to promote risk culture.

Chart 28: Initiatives taken to promote risk culture

Training and awareness in the form of classroom/online trainings, flyers/posters/public display/videos/newsletters, role-based trainings, annual risk week, risk day/cyber day, phishing simulations, tabletop exercises, encouragement to undertake risk certifications, etc. is the most common way to instill a cyber risk culture throughout the organisation.

Senior management and overall organisational commitment to cybersecurity closely follow training and awareness programs in the way of fostering a cyber risk culture.

Senior management and overall organisational commitment includes

- Regular leadership communication on importance of cybersecurity
- Inclusion of cybersecurity specific requirements in all roles and responsibilities
- Monitoring for security breaches or violations
- Disciplinary action against violations
- Chatbots to immediately address risk related queries.

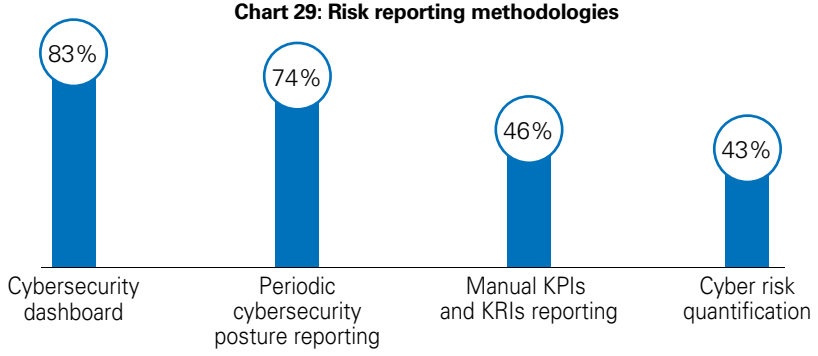
#2: Cybersecurity dashboards and periodic cybersecurity posture reporting are preferred risk reporting mechanisms

Cybersecurity dashboards have been a mainstream method for tracking and reporting cyber security risks (83 per cent) to board and senior management.

Other methods of cyber maturity assessment are also well accepted instruments for cybersecurity posture reporting (74 per cent).

Additionally, adoption of new age techniques such as cyber risk quantification has also shown an upward trend (43 per cent).

Chart 29: Risk reporting methodologies



06

Partnering with cyber ecosystem

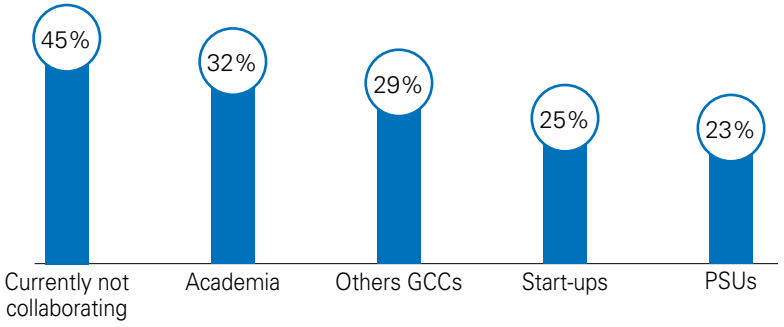
Cyber GCCs continue to develop partnerships and collaborate with various stakeholders outside their organisation. These stakeholders include academia, start-ups, other GCCs and government bodies.

#1: Collaboration with the wider ecosystem - A key focus area for the future

Among the options available, working with academia is the foremost form of collaboration leveraged by cyber GCCs with the wider ecosystem (32 per cent).

While collaboration with stakeholders has picked up in the recent years, there is still scope for improvement (45 per cent). As cyber GCCs mature further, collaboration across the ecosystem remains key.

Chart 30: GCC's collaboration with key stakeholders over the years



"The challenges of finding quality employees necessitates having strong, meaningful relationships with talented people, to attract other similarly talented people. Business in India is driven by relationships. Other tangible parameters, while important must be complemented by meaningful relationships amongst various stakeholders." - **Ben Goerz**, a Fortune 500 company executive

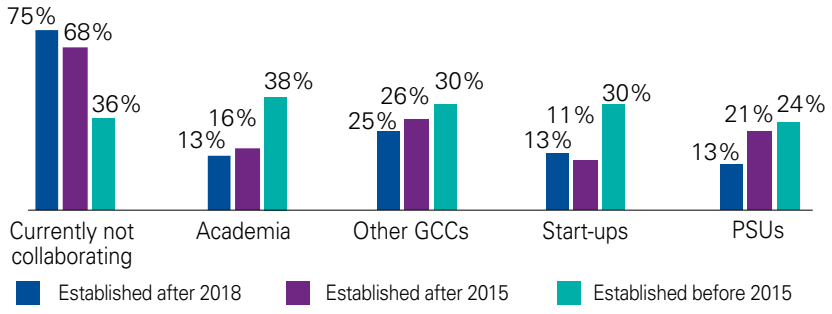
#2: Collaboration increases as cyber GCCs mature

Cyber GCCs established before 2015 have a considerably higher percentage of collaboration across their ecosystem.

The necessity of interacting with other stakeholders in the ecosystem increases as a cyber GCC gains maturity in terms of number and complexity of cybersecurity functions delivered.

Cyber GCCs established after 2018 have an advantage of drawing from the experience of mature cyber GCCs. Many cyber GCC leaders highlighted they collaborate with mature cyber GCC leaders and identify specific actions already implemented by their industry counterparts.

Chart 31: GCC's collaboration with key stakeholders as a function of GCC's age



Stakeholder	Top reasons for collaboration
Academia	Tie-up for continuing professional and technical education, branding for talent acquisition and co-creation of solutions
Start-ups	Niche product line, co-creation/co-development of products, access to ready talent and low cost of innovation
Other GCCs	Learning from other GCCs, industry representation to the regulators/government bodies on specific issues and organising events/hackathons/accelerator programs
Industry bodies/ PSUs	Sharing key challenges with regulators/government bodies on specific issues, conferences/ workshops/seminar on cybersecurity and assisting in drafting standards and policies

#3: Active partnerships with academia for skills and research

Several prestigious academic institutions such as IIIT Hyderabad, IIT Kanpur, IIT Madras and IIT Roorkee amongst others, offer Master's and Ph.D. courses related to cybersecurity, information security and other similar digital risk skills.

Cyber GCCs collaborate with academia primarily for co-creation (17 per cent) (e.g., joint research and development/co-publication, using incubation facilities for product/service development, etc.) and for branding purposes for talent acquisition (17 per cent).

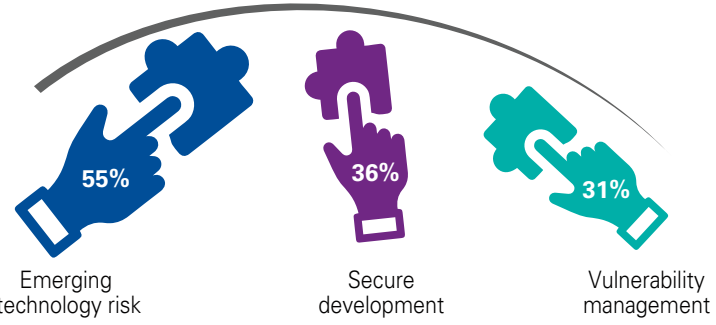
#4: Cyber GCCs partner with start-ups for innovation

Many cyber GCCs are sponsoring and encouraging start-up accelerator programmes as well as exploring other tie-ups with the start-up community for below scenarios:

- Co-creation of products
- Niche product line
- Access to ready talent
- Investment purposes

The functions where collaboration with start-ups is most prevalent are emerging technology risk, secure development and vulnerability management.

Chart 32: Top cyber functions in GCCs collaborating with start-ups



#5: Growing collaboration among cyber GCCs for shared learning and industry representation

Many cyber GCC leaders have collaborated in industry representation forums, working groups etc to the government bodies on various matters related to GCCs. This needs to be continued and expanded further.

- Earlier in 2020, the Prime Minister had announced that the government will be introducing a new cybersecurity policy. This policy is expected to drive key collective strategies to protect information and information infrastructure and build capabilities to prevent and respond to cyber threats and create a secure cyber ecosystem in the country. The regulatory framework is also expected to be strengthened further

- In October, the Department of Telecommunications (DoT) relaxed compliance guidelines for Other Service Providers (OSPs) (under which many GCCs are categorised). The DoT has done away with requirements such as deposit of bank guarantees, static IP addresses, frequent reporting obligations, and other provisions. These changes have also eased the adoption of 'Work From Home' and 'Work From Anywhere' models for organisations

- Key reasons for start-ups to collaborate with Government bodies and PSUs are:
  1. Opportunities to learn by sharing challenges and leading practices
  2. Industry representation to government bodies
  3. Drafting standards and policies
  4. Conferences and events

- The cybersecurity and digital risk functions where collaboration with other GCCs is most prevalent are secure development, cyber risk assessment, cybersecurity operations and identity and access management.

07

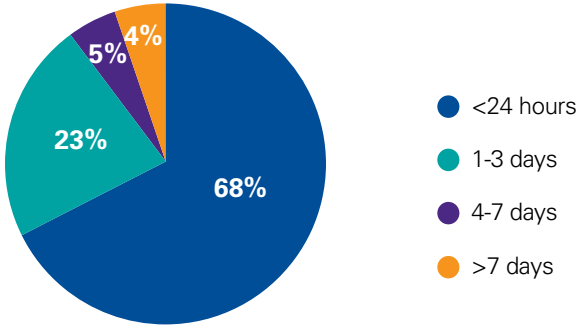
Embracing the new reality with COVID-19

This special feature uncovers insights from the Cyber GCCs' handling of the pandemic including its immediate response, resilient nature of operations and the ability to thrive in the new reality.

Cyber GCCs' effective response to the pandemic

#1 Swift recovery of Cyber GCC operations

Chart 33: The time taken by the GCCs to start working remotely



With the lockdown in place due to the pandemic, most Cyber GCC staff started working from home and continue to do so even post relaxation in the lockdown guidelines (95 per cent of cybersecurity staff).

About 68 per cent cyber GCCs said that it took their cybersecurity team less than 24 hours to enable Work From Home (WFH).

#2 Cyber GCCs central role in recovery of global operations

Chart 34: GCCs having a plan to handle a pandemic

Chart 35: GCCs who have enabled the global offices in dealing with pandemic

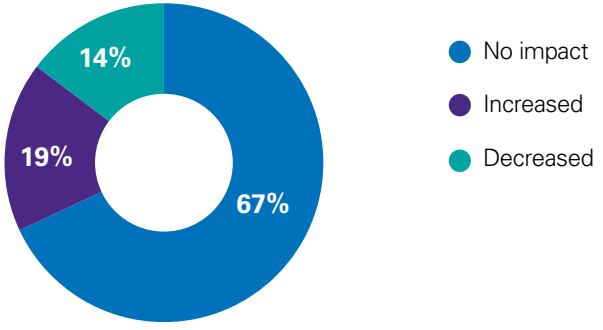
Cyber GCCs not only were prepared with documented pandemic response plans (78 per cent) but were also central to the recovery efforts of their parent organisations (75 per cent).

Key instances of cyber GCCs enabling global offices during the pandemic include:

1. Command centre run by cyber GCCs to support global operations recovery
2. Technology enablement to protect organisations from increased cyber threats during COVID-19
3. Scaling identity and access management controls to fit WFH scenario

While the cyber GCCs have been facing immense challenges, they have weathered the pandemic with no significant change in their cybersecurity budget (67 per cent).

Chart 36: Impact on GCCs' cybersecurity budget for FY20-21



The pandemic has resulted in not only Cyber GCCs amplifying preparedness for cyber threats, but also increased risk acceptance in the following areas:

- Endpoint security risk
- Patch and password update risk
- Privileged access management risk

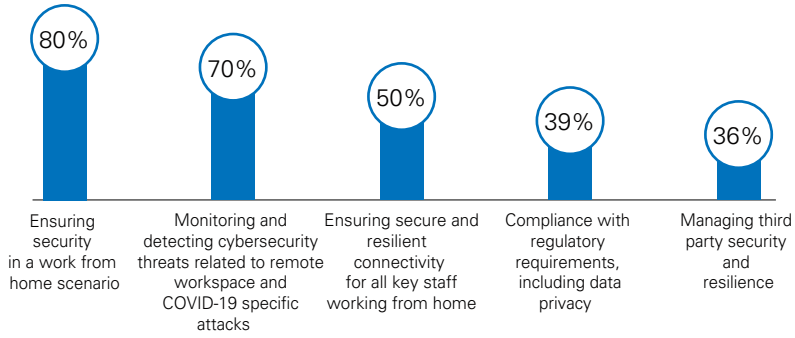
Resilient nature of Cyber GCC operations

#1 Cyber safe – A key challenge during the pandemic

With the onset of remote working, Cyber GCCs faced three types of cyber challenges:

- Work from home (WFH) related
  1. Ensuring security in a work from home scenario (80 per cent) (e.g., access control, patching, endpoint security, network security and availability, etc.)
  2. Monitoring and detecting cybersecurity threats related to remote workspace and COVID-19 specific attacks (70 per cent)
  3. Ensuring secure and resilient connectivity for all key staff working from home (50 per cent). A major challenge faced pertains to risk arising from Internet Service Provider (ISP) concentration.
- Regulatory related - Compliance with regulatory requirements, including data privacy (39 per cent)
- Third party related - Managing third party security and resilience (36 per cent)

Chart 37: Top Cybersecurity challenges faced by GCCs during COVID-19



#2 Cyber GCCs are resilient in the wake of increased threats

About 89 per cent cyber GCCs faced at least a 10 per cent increase in cyber-attacks during COVID-19.

Phishing, social engineering, ransomware and malware attacks contributed most to the increase in cyber-attacks.

Chart 38: Increase in cyber-attacks faced by cyber GCCs during COVID-19

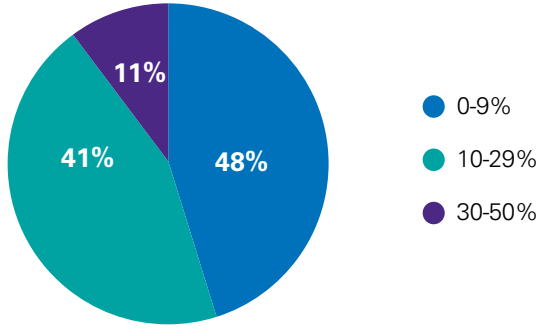
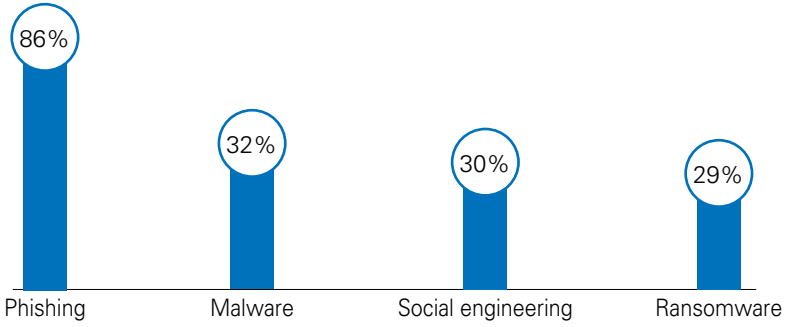


Chart 39: Cyber-attacks faced by GCCs since the onset of COVID-19



#3 Effective third-party resilience measures

Increased regulatory focus on third party risk management and emphasis on operational resilience across organisations has resulted in third party risk emerging as a key focus area.

The pandemic situation stress tested the resilience of the third party ecosystem servicing the organisations. It was noted that cyber GCCs playing a key role in the organisation's third party risk management program had a better visibility on the third party's pandemic readiness status and were able to effectively coordinate recovery activities.

About 91 per cent of cyber GCCs said that they had effective third party resilience measures in place to support the business operations.

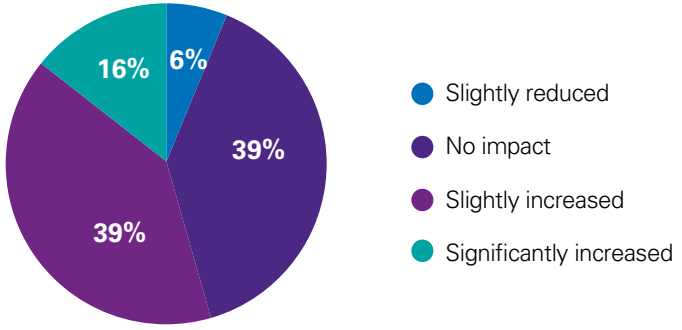
Chart 40: Did the lack of third party resilience impact GCC business operations?

Cyber GCCs thriving in the new reality

About 94 per cent of cyber GCCs say that there was no impact to their operational efficiency.

In fact, 55 per cent cyber GCCs reported an improvement in their operational efficiency.

Chart 41: Impact on operational efficiency while working remotely



Amit Kalra,

Managing Director and Head Global Services, Bangalore, Swiss Re

"The pandemic has reinforced the need for cyber security awareness among employees and improving organisational capabilities to address the increasing sophistication of malicious cyber-attacks.

Organisations have experienced several advantages of remote working and a post-pandemic world will continue to have elements of a more agile and flexible work environment, leading to addition of more and ever-evolving interconnected devices to a network, which will increase the risk of potential attacks."

08

Cyber GCCs - Looking ahead

Protecting the new normal and beyond

Cyber GCCs are recommended to deploy a model of Run, Change and Think (RCT), as they not only embrace the new normal and go a step ahead of securing it. Below is a set of key measures recommended, however these are not exhaustive.

- **Think:**

Cyber GCCs are embracing the new normal and are at the cusp of moving to new models of working such as work from anywhere, agile globalisation and potentially longer-term remote work.

Continued integration of secure, resilient and trusted cybersecurity and digital risk strategies with the above-mentioned business models is key for cyber GCCs to enable their global organisations.

- **Run:**

Short term recommendations:

- Update risk management policies and procedures to mitigate threats associated with work from home
- Conduct mandatory cybersecurity courses and awareness trainings for employees working remotely
- Implement secure virtual desktops (VDI/WVD) or secure containers for end users
- Define orchestrated approach for cyber incident management and response
- Provide access to organisation platforms for all remote users, as per the business requirement, using stringent access controls
- Provide privacy filters to all the employees
- Conduct threat hunts to detect COVID-19 and emerging cybersecurity threats.

Long term recommendations:

- Review and revisit the protection strategies of operating model
- Build capability for on-demand incident response and forensics
- Evaluate and adopt micro segmentation and zero trust network-based architecture
- Implement advanced cybersecurity measures such as SOAR, deception and AI/ML based security operations
- Embrace cloud security measures.

- **Change:**

Global Majors:

- Continue to harness cyber GCC potential for leadership of global functions
- Expand the leverage of cyber GCCs in emerging technologies and digital risks
- Leverage cyber GCCs for cybersecurity innovation further and recognize the contribution coming from cyber GCCs for the same.

GCC cyber leaders:

- Increase collaboration with wider ecosystem – Opportunity to deepen relationship with academia, other GCCs and government bodies to facilitate co-creation, investment opportunities, leadership development and joint representation to regulatory bodies amongst others
- Conceptualise and participate in industry wide crisis simulation exercises. Given the increase in concentration of global functions, cyber GCCs have become vital to the organisation resilience. Participation in industry-wide crisis simulation exercises will increase readiness to respond to emerging and sophisticated cyber threats and signal maturity to the wider ecosystem
- Cyber GCC digitisation – Embrace technologies including AI, ML, RPA and Cloud to increase the efficiency and effectiveness of the cybersecurity functions delivered.

Cyber GCC team members:

- Upskill – The present trends highlight cyber GCCs' focus on adoption of digital and emerging technologies for cybersecurity functions and addressing risks from the said functions. The cyber GCC team members should leverage training opportunities to meet the demand for such future oriented skills
- Aspire to be a cyber leader – In the last few years, the cyber GCC leadership has broken through the glass ceiling and are leading global cybersecurity functions for their organisations. This has opened up a number of cyber leadership opportunities within the GCC for the team members.

Policy makers:

- Continue conducive policy environment to support cyber GCC growth and realise the potential of 'Secure in India' – Continue to work towards enhancing policies for attracting more global organisations and GCCs to set up and expand global cybersecurity delivery from India. Similar to the recently announced relaxed DoT – OSP guidelines, other policy areas which may be relevant to cyber GCCs include – STPI and SEZ related acts, cybersecurity policy and data privacy regulatory requirements
- Continue engaging academia and start-up community – Presence of an academic and start-up ecosystem is a key driver for cyber GCCs to be set up and expand their presence. Recent initiatives for government backed start-up accelerator programs as well as focus on cybersecurity courses in institutions will go a long way in attracting cyber GCCs
- Explore opportunities further to recognise cyber GCCs – Plan initiatives to strengthen the Cyber GCC brand in India and recognise efforts at a national or global stage. Major summits such as the World Economic Forum (WEF), and other such platforms/events may be explored.

Start-ups:

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

Academia:

- The academic bodies should deepen ties with cyber GCCs to:
  - Align their course curriculum with the practices in the industry
  - Create opportunities for joint research, virtual internships and co-development of products
  - Encourage participation from cyber GCCs as part of leadership development programs
  - Help build a robust talent pipeline addressing in-demand and future oriented cybersecurity and digital risk skills.

09

Additional insights noted in the Secure in India 2020 survey

Cybersecurity in the digital era

1. Establishment of cyber GCCs over the years
2. Distribution of employee strength of cyber GCCs
3. Location wise distribution of cyber GCCs

Extended global cyber organisation

1. Correlation between staff strength and functions delivered from India
2. Evolution of cyber GCC organisation structure with time

Cybersecurity and digital risk workforce

1. Trend of budget prioritisation vs. skill demand
2. Attrition rate by cyber GCC location

Partnering with cyber ecosystem

1. Cyber GCCs collaboration with the wider ecosystem over the years

Embracing the new reality with COVID-19

1. Representation showcasing top ways cyber GCCs have engaged with staff

To get detailed insights, please reach out to our team.

10

Methodology

The premise of this report is based on several sources of information, meetings and brainstorming sessions undertaken by KPMG in India, NASSCOM, DSCI, WEF and Industry leaders between August 2020 and December 2020.

Survey

The insights published in this report are primarily based on the responses received from the 'Secure in India' survey rolled out to executives across global organisations who have Global Capability Centres (GCCs) in India.

The respondents of this survey were GCC Heads, 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 fourteen key sectors, namely:

- Automotive
- Banking
- Consumer goods
- Financial services
- Healthcare
- Insurance
- Investment management
- Logistics
- Manufacturing
- Oil and gas
- Pharmaceuticals
- Retail
- Technology
- Telecom.

This survey was conducted between 5 September 2020 to 2 December 2020.

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 a detailed secondary research for every chapter. The team relied on the organisation's 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, 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 executives of India-based GCCs who invested their valuable time to give us inputs and contribute to this report.

Our special thanks to the advisory panel including William Dixon, Ramachandra Kulkarni, Oskar Brink, David Ferbrache and Ravi Jayanti and for their strategic direction 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

- Raghu TVN
- Vamshi Chaitanya Kuchulakanti
- Abhijith A
- Abhishek Kishore Gupta
- Raahul Gautam
- Dave Remedios
- Srinivasan Chinnadorai
- Satyam Nagwekar

NASSCOM

- Sukanya Roy
- Achyuta Ghosh
- Namita Jain
- Ranjita Kamat

DSCI

- Rama Vedashree
- Dr. Sriram Birudavolu
- Anand Raman

We acknowledge the efforts put in by the core team of Secure in India 2020, right from initiation to publication of this report.

- Manoj Kumar
- Sanjana Poddar
- Sangram Keshari Rout
- Divya Mishra
- Sushmita Karmakar
- Karanveer Singh Chawla

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-focussed 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 is the industry association for the IT-BPM sector in India. A not-for-profit organization funded by the industry, its objective is to build a growth led and sustainable technology and business services sector in the country. Established in 1988, NASSCOM's membership has grown over the years and currently stands at over 2,500. These companies represent 95 percent of industry revenues and have enabled the association to spearhead initiatives and programs to build the sector in the country and globally. NASSCOM members are active participants in the new global economy and are admired for their innovative business practices, social initiatives, and thrust on emerging opportunities.

KPMG in India contacts:

Vikram Hosangady
Partner and Head
Clients & Markets
T: +91 98410 85580
E: vhosangady@kpmg.com

Akhilesh Tuteja
KPMG Global
Leader for Cyber,
Head of Digital in India
T: +91 98710 25500
E: atuteja@kpmg.com

Shalini Pillay
Office Managing Partner
Bangalore and GCC leader
T: +91 98440 18843
E: shalinipillay@kpmg.com

Atul Gupta
Partner and National
Leader Cybersecurity
IT Advisory
T: +91 98100 81050
E: atulgupta@kpmg.com

Srinivas Potharaju
Partner and Risk
Transformation Leader
T: +91 98459 19740
E: srinivasbp@kpmg.com

Pranav Kathale
Director
T: +91 97313 13472
E: pranavkathale@kpmg.com

Srijit Menon
Director
T: +91 97317 77099
E: srijitmenon@kpmg.com

NASSCOM:

Sukanya Roy
Director GCC and BPM
T: +91 9611000133
E: sukanya@nasscom.in

DSCI:

Anand Raman
Research Analyst
T: +91 9650438154
E: anand.raman@dsci.in

home.kpmg/in

Follow us on:
home.kpmg/in/socialmedia

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia

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.

KPMG (Registered) (a partnership firm with Registration No. BA- 62445) converted into KPMG Assurance and Consulting Services LLP (a Limited Liability partnership firm) with LLP Registration No. AAT-0367 with effect from July 23, 2020.

This document is for e-communication only. (043_THL1120_DGR)