KPMG

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Secure in India

Leaders' insights on GCC empowered global cybersecurity delivery

NASSCOM®

June 2018

KPMG.com/in

Foreword

Global organisations recognise the inevitability of cyberattacks, and are enhancing their cybersecurity strategies by bringing together skilled people, cutting-edge technologies and new age processes to secure their organisations. Global Capability Centres (GCCs)[01], by design, allow organisations to insource key functions, retain control and hold on to expertise in-house. When combined with right talent and commercial effectiveness, GCCs are apt for cybersecurity. With over half of the global GCC revenues, and growing at a CAGR of 11 per cent YoY[02], the growth of India based GCCs is already well known.

In this report, we explore a wide range of drivers, capabilities, smart practices, innovation, challenges and offer insights on how India based GCCs are securing their global organisations. The intent of this report is to enable leaders of global organisations make informed decisions on their India-based GCC strategy for cybersecurity delivery.

Talent pool availability emerged as the top most driver (90 per cent respondents) for setting up cybersecurity delivery from India based GCCs (Cyber GCCs[03]). Cost arbitrage as a driver was a distant second (68 per cent). Further, high value generating functions are surging in Cyber GCCs. Over 57 per cent of the Cyber GCCs surveyed had 'cybersecurity strategy and governance' function; and 59 per cent had 'cybersecurity products and new solutions development'. Further, 70 per cent of the organisations surveyed had representation of India based GCC leaders in global committees. These findings are indicative that Cyber GCCs are at the cusp of transformation.

However, the positivity is tempered with realism. Cyber GCC leaders face challenges in meeting ever increasing demand for niche skills, addressing growth path of key people, and are looking for more value creation through collaboration with GCC communities and industry bodies. In this report, we also touch upon the smart practices and innovative methods employed by Cyber GCCs to overcome these challenges.

The insights in this report are prepared in consultation with Cyber GCC leaders, cybersecurity SMEs and industry bodies. It provides key recommendations for Cyber GCCs to sustain their competitive advantage; transform into global 'centres of expertise'; and enable global organisations to 'Secure in India'.

Akhilesh Tuteja

Global Cybersecurity Co-Head
and Head of Risk Consulting
KPMG in India

Rama Vedashree

CEO
DSCI

Debjani Ghosh

President
NASSCOM

[01]. GCCs are captive units which include both MNC-owned units that undertake tasks for the parents' global operations and the company-owned units of domestic firms. Source: NASSCOM Strategic Review, NASSCOM, accessed on 12 June 2018

[02]. GICs In India: Getting Ready For The Digital Wave, NASSCOM, accessed on 19 June 2018

[03]. Cyber GCC' or ' India based Cyber GCC' refers to teams focussed on global cybersecurity delivery located within respective GCCs in India If these facts have been mentioned in the report and have been corroborated in the respective chapter, we do not need to mention sources here.

Key takeaways

1

Global organisations believe in India's GCCs'[01] capability to address their cybersecurity agenda

- Cyber GCC[02] is an integral part of insourcing strategy. 61 per cent say 'retention of cybersecurity expertise in-house' is key
- Average budget allocated to global cybersecurity delivery by India based cyber GCCs (at 18 per cent CAGR in 2018)[03] is increasing rapidly when compared to average global cybersecurity budget (at 8 per cent CAGR in 2018)[04]
- 35 per cent say 'business feasibility' (ease of cybersecurity delivery) is one of the top three drivers for setting up Cyber GCCs

2

Talent pool is at the heart of Cyber GCCs' success story

- Over 90 per cent say 'talent pool availability' drives their global organisations to set-up Cyber GCCs in India
- Cyber GCCs present a distinct opportunity to their global organisations with commercial, competitive and abundant talent pool. 68 per cent say 'commercial effectiveness' is one of the top three drivers
- 62 per cent employ new-age techniques (e.g. hackathons) to upskill cybersecurity teams
- 83 per cent are at high maturity levels[05] in dealing with cyberthreats (e.g.: denial of service (DoS)) and 71 per cent are at equally competent levels in dealing with advance threats (e.g.: malware)
- 96 per cent have adopted pre-planned strategies to combat cyber crisis for their global organisations

3

Think innovation, think Cyber GCC

- 32 per cent say innovation is one of the top three drivers for setting up Cyber GCCs
- About 60 per cent have 'cyber product and new solutions development' capabilities
- Over 64 per cent leverage emerging technologies to handle cyber issues
- 52 per cent are involved in incubation, acceleration and co-creation with start-ups

4

Cyber GCCs continuously adapt to enhance value

- About 70 per cent create value for their global organisations through collaboration with external parties (e.g.: Industry peers, industry bodies, regulators, academia, start-ups, etc.)
- Over 55 per cent have targeted approaches to manage risks (such as distributed functions to reduce concentration risk)

5

Cyber GCC leaders owning global cyber functions[06] are on the rise

- 38 per cent are multi-function centres with influential[07] cybersecurity leadership
- 70 per cent have at least one GCC leader serve in global committees
- 57 per cent have a 'cyber strategy and governance' function
- Cyber GCC leaders continue to gain more experience in dealing with global regulators and auditors

[01] 'GCC' refers to Global Capability Centres as defined in NASSCOM Strategic Review, NASSCOM, accessed on 12 June 2018

[02] 'Cyber GCC' or 'India based Cyber GCC' refers to teams focussed on global cybersecurity delivery located within respective GCCs in India

[03] Average of mean of approximate annual increase in cybersecurity budget of India based Cyber GCCs in 2018 as reported in the 'Secure In India' survey 2018 conducted by KPMG In India, DSCI and NASSCOM

[04] Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017, Gartner, 7 December 2017

[05] High maturity refers to comprehensive risk management policies, implemented across entire organisation; and continuous improvement in cyber risk management as a part of corporate culture

[06] Refer to Annexure 1 for details about the cybersecurity functions considered for the survey

[07] Leadership with decision making capability or having ownership of global cybersecurity functions

Table of contents

01.

Inevitability of cyberthreats

Cyber certainty[01]

With exponential increase and inevitability of cyberthreats, cybersecurity remains a top priority for organisations worldwide and continues to be on the boards' agenda. However, only 51 per cent CEOs worldwide believe that they are well prepared to handle cyberattacks.[02] In this regard, organisations are increasing their budgetary spend and are bringing together advanced capabilities to secure their organisations.[03]

About **50 per cent** of the CEOs globally say that becoming a victim of a cyberattack is a case of 'when', not 'if'. [03,04]

Cybersecurity spend is likely to rise to **USD96 billion** in 2018.[03,04]

India-based Global Capability Centres (GCCs)

With over 1,140 GCCs[05], already established in India, the country's GCC potential in global delivery is already well-established[07]. In the following chapters, the current landscape has been explored to unearth smart practices and innovation potential of India-based GCCs empowering global cybersecurity delivery.

USD25 billion India GCC revenues[05]

900,000 employees[06]

India accounts for about half of global GCCs[08]

India accounts for over 65 per cent of the global captive headcount[08]

[01] 'Cyber certainty' refers to the certainty of occurrence of cyber-attack. Source: 2018 Global CEO Outlook, KPMG International, accessed on 18 June 2018

[02] 2018 Global CEO Outlook, KPMG International, accessed on 18 June 2018

[03] Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017, Gartner, 7 December 2017

[04] Global CEOs realistic about growth in the face of unprecedented headwinds, KPMG, Accessed on 23 May 2018

[05] GCCs are captive units which include both MNC-owned units that undertake tasks for the parents' global operations and the company-owned units of domestic firms. Source: NASSCOM Strategic Review, NASSCOM, accessed on 12 June 2018

[06] Global in-house centres hire more highly-skilled tech professionals, The Economic Times, 13 December 2017

[07] The Future of Me, KPMG, accessed on 11 June 2018

[08] Why India is seeing a fresh wave of global innovation centres, and how it could be a lifesaver for IT firms, The Economic Times, 29 August 2017

02.

India's tryst with 'Cyber GCCs'

Cybersecurity delivery prevalence

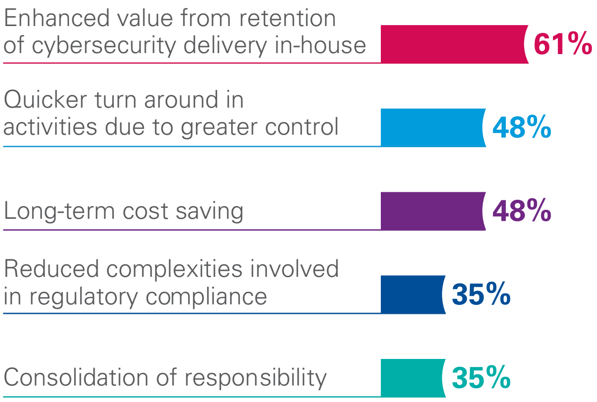
India-based GCCs empowering Global cybersecurity delivery (i.e., Cyber GCCs[01]) are widely prevalent. This trend is noted across twelve sectors studied, viz., banking, technology, energy, infrastructure, investment management, insurance, manufacturing, telecom, consumer and retail, automotive, life science and healthcare and pharmaceuticals.

GCC key to retaining cybersecurity knowledge in-house

Inherent to the nature of cybersecurity is protection of confidential data. Organisations are typically wary of third parties managing a wide range of cybersecurity services.

More than 60 per cent of the respondents see enhanced value from retention of knowledge in-house' as a top driver to leverage the GCC model.

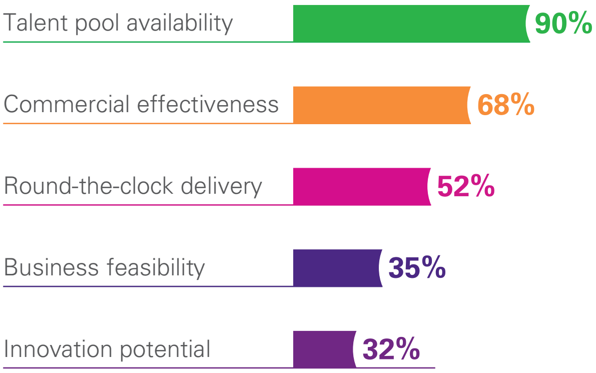
Chart 1: Top drivers for global organisations to adopt the GCC model for cybersecurity delivery



Talent pool topples cost arbitrage as the top driver

Talent pool tops all other factors by a significant margin, with about 90 per cent of survey respondents saying 'talent pool availability' is one of the top three factors driving cybersecurity services. Traditionally, cost arbitrage has been the top most driver for India-based GCCs[02].

Chart 2: Top drivers to set up Cyber GCCs in India

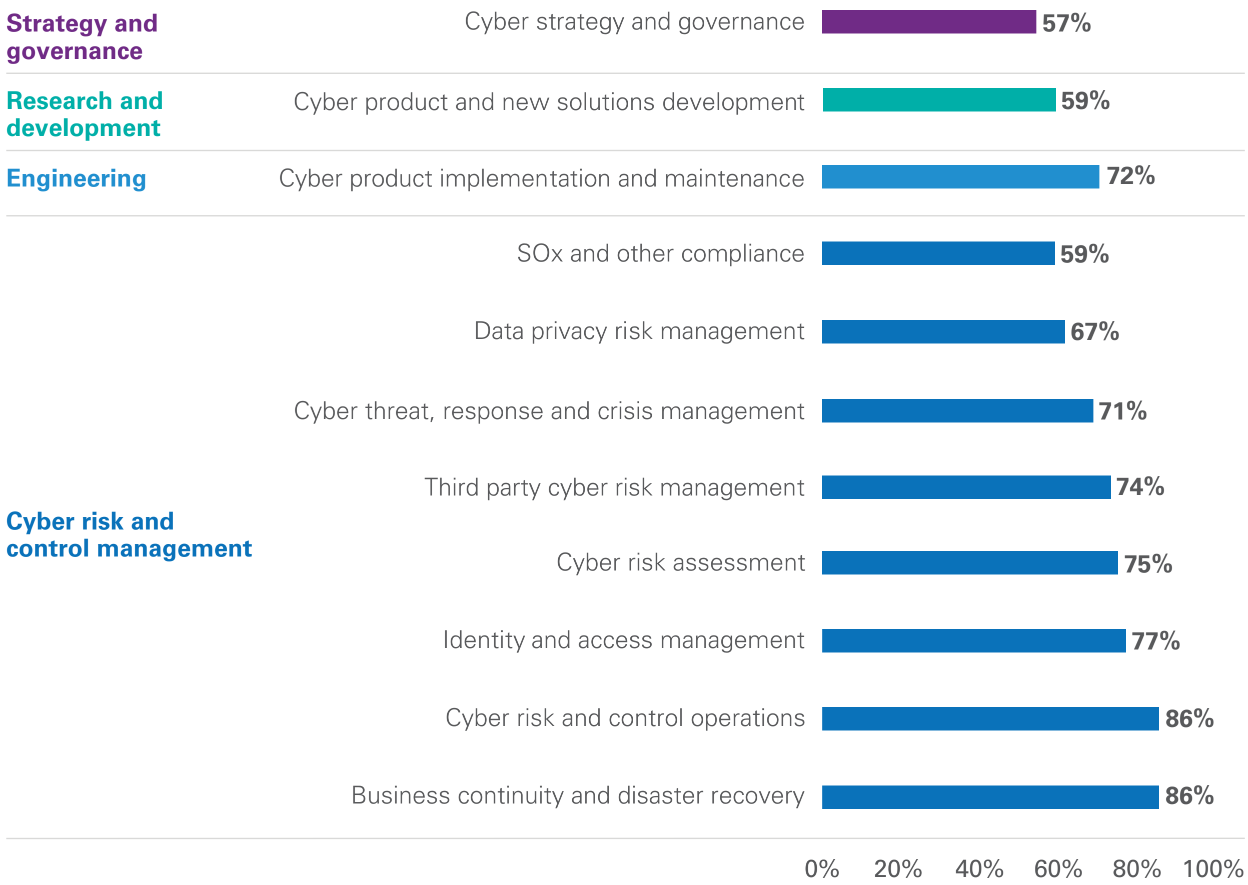


[01] 'Cyber GCC' or ' India based Cyber GCC' refers to teams focussed on global cybersecurity delivery located within respective GCCs in India

[02] Cost Competitiveness of GICs 2014, NASSCOM, 13 June 2016

Wide spectrum of cybersecurity functions delivery capability

Chart 3: Cybersecurity functions delivered from GCCs in India



The variety of cybersecurity functions[03] being delivered from India can be attributed to its broad and abundant talent pool.

The spectrum of cybersecurity services range from task-based functions such as security monitoring to deep thought and research based 'cyber product and new solutions development', and 'cyber strategy and governance'.

Innovation trending as a top driver

Nearly one-third of the respondents say that innovation potential is one of the top three drivers for setting up Cyber GCCs in India. It is interesting to note that for a traditional GCC set-up, this has not typically been a top driver in the past[04].

With a strong technical talent pool, Cyber GCCs are taking up more complex functions over simple operational activities.

32 per cent of the respondents say that the country's strong innovation potential is one of the top three drivers for setting up Cyber GCCs in India

[03] Refer to Annexure 1 for details about the cybersecurity functions considered for the survey

[04] GICs in India-Emerging Centres of Excellence, NASSCOM, 11 July 2017

Strengthening capability up the value chain of cybersecurity functions

There is a steady shift towards higher volume of engineering, R&D and strategy functions in GCCs. About 60 per cent of Indian Cyber GCCs employ teams developing 'cyber products and new solutions' and 'cyber strategy and governance'.

In fact, GCCs established post 2012 deliver cybersecurity strategy and governance services from Cyber GCCs more than those set up earlier.

Chart 4: Cyber GCCs undertaking high value cybersecurity activities, by function

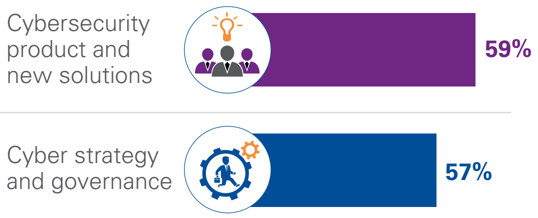
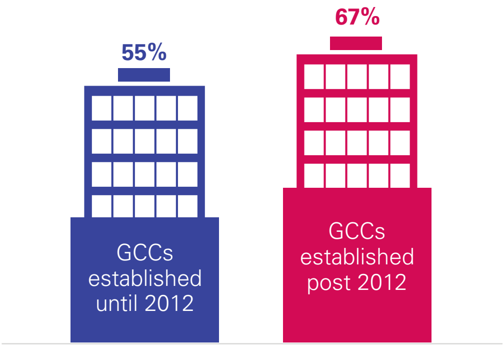


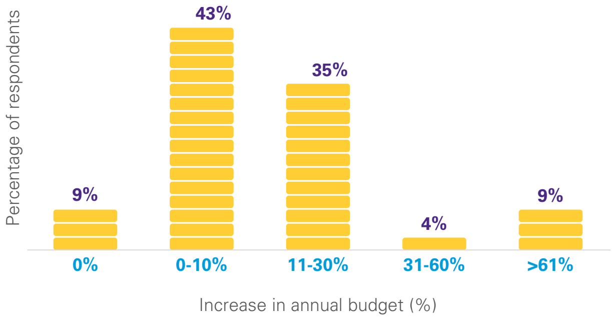
Chart 5: Cyber strategy and governance function in Cyber GCCs, until and after 2012



Increase in share of 'cyber strategy and governance' function in Cyber GCCs

Budget allocated to global cybersecurity delivery by Cyber GCCs is increasing rapidly

Chart 6: Increase in budget allocation to global cybersecurity delivery by Cyber GCCs in 2018



While the global spend on cybersecurity is expected to grow at 8 per cent[05] in 2018, budget allocated by Cyber GCCs has increased by an approximate 18 per cent[06] in 2018.

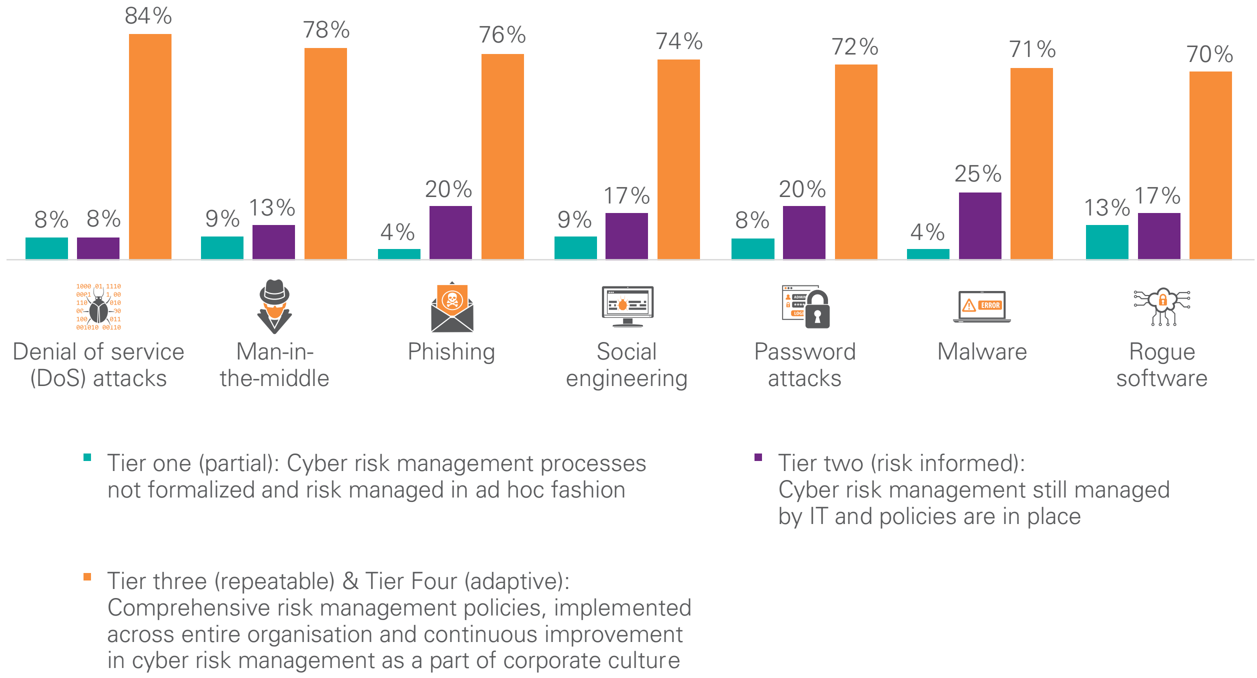
[05] Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017, Gartner, 7 December 2017

[06] Average of mean of approximate annual increase in cybersecurity budget of India based Cyber GCCs in 2018 as reported in the 'Secure In India' survey 2018 conducted by KPMG In India, DSCI and NASSCOM

Advanced proficiency levels of Cyber GCCs in responding to cyberthreats

Cyber GCCs have high maturity levels in dealing with a wide range of cyberthreats. While about 80 per cent of respondents said that they are at an advanced state (tier-three and tier-four)[07] in dealing with cyberthreats (e.g.; DoS), about 70 per cent of respondents feel that they are equally competent in combating advanced threats (e.g.: malware). Less than 15 per cent respondents said that they do not have a formalised cyber risk management process to deal with cyberthreats

Chart 7: Readiness of Cyber GCCs, by cyberthreat



As part of this study, various examples of cyber crisis management were shared by Cyber GCC leaders:

Cyber crisis planning and preparedness

- Participate in global, local and individual simulation exercises of crisis events and their ability to respond.
- Collaborate across industry to prepare for such incidents (mock drills, table top reviews, etc.).

Cyber crisis response

- Cyber GCCs house global red and blue teams (cyber-attack and defence experts of global organisation). Global cyber threats (such as 'WannaCry' ransomware attack of 2017) are being managed from their centres.
- Cyber GCCs have already experienced local crisis and business continuity events (as seen in the case of Chennai rains[08], certain events of unrest in Bengaluru[09] and Mumbai[10]) and contributed significantly in managing global events (such as hurricanes, earthquakes etc.) of similar nature (refer to Annexure II for more details).
- GCCs are able to respond to targeted attacks on themselves as well.

Regulatory examination

- Cyber GCCs are experienced in engaging both global and local regulators. Global regulators have inspected and examined some of the GCCs specifically around crisis management and response, business continuity and operational resilience.

[07] Definition of Tier Three and Four – GCCs having comprehensive risk management policies, implemented across entire organisation and continuous improvement in cyber risk management as a part of corporate culture

[08] IT companies invoke alternate plans as rain hits Chennai operations, Business Line, The Hindu, 2 December, 2015

[09] Cauvery dispute: Protests shuts down Bengaluru, Livemint, 14 September, 2016

[10] Heavy rains batter Mumbai yet again; air, rail traffic hit, Reuters, 20 September, 2017

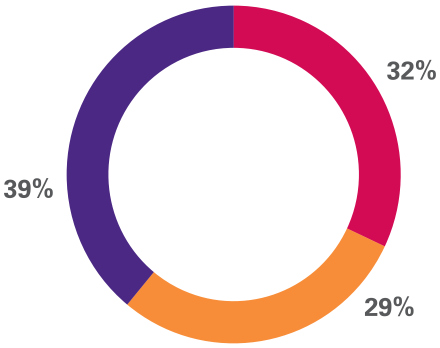
Influential cybersecurity leadership* is on the rise

About 39 per cent of GCCs have multi-function centres with influential cybersecurity leadership based in India. This trend is more prominent with GCCs that emerged after 2012, wherein nearly 43 per cent of GCCs have influential cybersecurity leadership based in India.

70 per cent of all respondents have at least one GCC leader serve in one of the global committees.

*Influential leadership refers to Leaders with decision making capability in global cybersecurity strategy, governance and operations

Chart 8: Reporting structure of Cyber GCCs to global organisation



68%

of GCCs are multi-function centres reporting to business leaders and global heads

- 🟥 Single function centre, mostly managerial leadership with one local head, reporting to business leaders
- 🟧 Multi-function centre reporting to multiple business leaders, with only operational oversight by India head
- 🟪 Multi-function centre, with influential leadership seated in GCC, and several of them reporting to global heads

03.

Smart practices

Cyber GCCs are using smart practices to address challenges and capitalise on opportunities in areas such as talent management, collaboration, working with global organisations, spreading to value-based locations and leveraging emerging technologies to enhance efficiencies.

Talent management

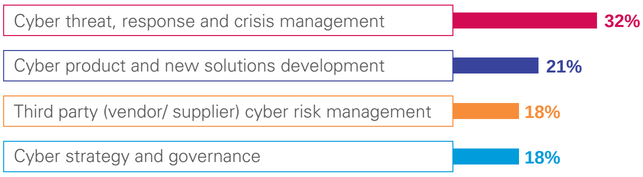
Challenges and opportunities

Cybersecurity requires continuous and rapidly evolving skills, along with a large work force to meet the increasing demand. While talent is available in abundance in the country, there are certain areas where Cyber GCCs are facing challenges in sustaining experienced hands.

#1: Lack of niche skills in required volume:

Out of all cybersecurity functions, cyberthreat, response and crisis management (32 per cent) followed by cyber product and new solutions development (21 per cent) are experiencing challenges in addressing ever increasing demand

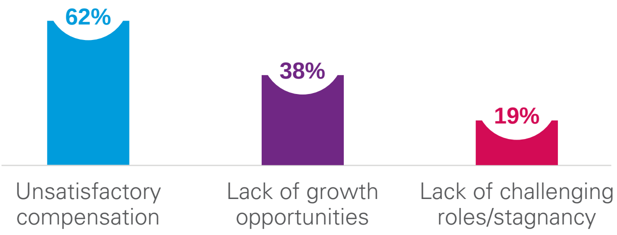
Chart 9: Skill gap faced by Cyber GCCs, by function



#2: Talent retention:

Most survey respondents experienced attrition of about 10-15 per cent in their cybersecurity teams. Unsatisfactory compensation (62 per cent), lack of growth opportunities (38 per cent) and stagnancy (19 per cent) are the top reasons

Chart 10: Key reasons for attrition in Cyber GCCs



#3: Untapped cyber leadership potential:

Only 22 per cent say 'senior management expertise' available with Cyber GCCs is one of the top drivers. While talent pool availability and innovation potential offered by Cyber GCCs are tapped well, confidence in cyber leadership potential is gaining momentum

[01] Why India is seeing a fresh wave of global innovation centres, and how it could be a lifesaver for IT firms, The Economic Times, 29 August 2017

Smart practices for effective talent management

#1: Tie-ups with academia for nurturing niche skills, retaining the 'right' talent, and develop cyber leaders

Nearly 30 per cent of Cyber GCCs have tie-ups with universities. The tie-ups are focussed on acquisition of talent, assistance with curriculum development and learning programmes in cybersecurity. Several GCCs have established learning centres[01] with colleges.

Nearly 50 per cent of GCCs leverage universities (and start-up forums) for market research on cybersecurity.

These practices are focussed on nurturing niche talent, motivating existing talent and developing cyber leaders.

Nearly **30 per cent** of cybersecurity GCCs are collaborating with academia for acquiring better talent and conduct research

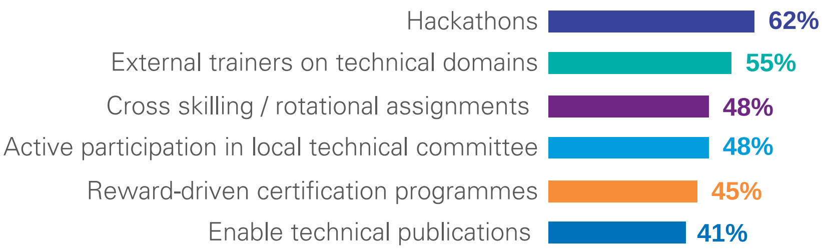
Examples of GCC - Academic collaboration

- A U.S. based communications giant having their GCC in India runs a network academy to train and certify students in the areas of computer networks and network security.[02]
- GCC of a German automotive major signed a MoU with the Indian Institute of Technology Madras (IIT M) to set up a Data Science and Artificial Intelligence centre.[03]
- A number of global organisations have collaboration with IIMs, for leadership programmes.

#2: New-age techniques to upskill and cross-skill cybersecurity talent

While traditional methods of reward-driven certification, external training and enabling staff for technical publications are still relevant, Cyber GCCs are also employing new-age techniques to upskill and cross-skill their staff. 'Hackathon' is a case in point.

Chart 11: Techniques employed by Cyber GCCs for up-skilling



Other new-age techniques such as bug-bounties, war-rooms, and gamification are gradually gathering steam.

62 per cent of survey respondents said that "hackathon" is their most preferred mode for upskilling.

Hackathons have dual advantage – while enabling employees to collaborate and upskill, the outcome of a typical hackathon session is a collaborative product which otherwise takes significantly more effort to develop

[01] Why India is seeing a fresh wave of global innovation centres, and how it could be a lifesaver for IT firms, The Economic Times, 29 August 2017

[02] 'Secure in India' Survey, KPMG in India, June 2018

[03] Data science and AI lab set up at IIT Madras, The Times of India, 5 August 2017

# 3: Global mobility

Several GCCs have global mobility programmes to provide their people with enriching opportunities to work in offices around the world. Generally, the assignments vary from short-term (three- six months) to long-term (between one and three years). These programmes aim to develop global skills development, promote knowledge transfer across borders and foster cultural orientation. Needless to say, many GCC heads say this provides their people with challenging and growth enablement opportunities.

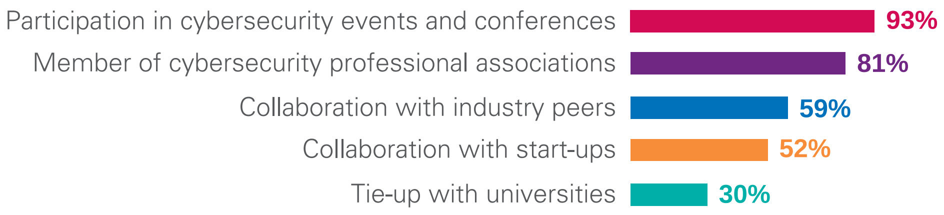
Collaboration to create value

#1: Collaboration with external parties

Over 90 per cent of survey respondents see value from active participation in focussed and relevant cybersecurity events and conferences and over 80 per cent of them see enhanced value from being members of relevant professional associations.

These associations are promoting R&D and technological developments in the cybersecurity space. They are also implementing a workforce upskilling road map. In addition, Cyber GCCs are collaborating with start-ups to provide for new technology exploration.

Chart 12: Collaboration practices adopted by Cyber GCCs

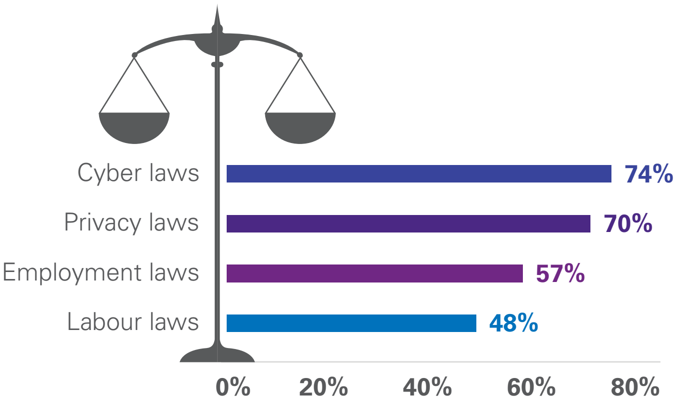


> GCCs actively collaborate and engage with their peers, academia, start-ups, consultants, industry bodies and regulators. Cyber GCCs share key challenges, smart practices and continually enable themselves to provide significant value to their global organisations.
>
> **Srinivas Potharaju**
>
> *Partner and GCC Leader for Risk Consulting*
>
> KPMG In India

#2: Working with governments and regulators

Several leaders surveyed say that the following initiatives have had or expected to have a positive impact on their Cyber GCCs, viz. 'Skill India', SEZ polices, 'Start-up India' and 'Make in India'.

Chart 13: Local laws and regulations impacting Cyber GCCs



Over **70 per cent** leaders say that local cyber and privacy laws impact their Cyber GCCs

Industry body speak

> The ongoing changes in policies and regulatory environment in India are conducive to global businesses. This optimism is also shared by multiple GCC heads who believe these changes will impact their GCCs positively. As long as policies continue to favour moving business to India, GCCs will continue to expand cybersecurity delivery from India
>
> **Vinayak Godse**
>
> *Senior Director*
>
> DSCI

India's Supreme Court's decision in favour of privacy as a fundamental right, and the governments focus on creating a comprehensive privacy law in the country[04], is likely to contribute to an enforceable privacy regime in the country. In which case, movement of operation and data to India is expected to be smoother.

Examples of evolving policies[05,06,07,08]

IP laws: The government released the National Intellectual Property Rights (IPR) Policy in 2016, which aims to create and exploit synergies between all forms of intellectual property.

Enforcement of contracts: On the back of government reforms, the country jumped 14 positions in the context of enforcing contracts over the last three editions of the World Bank's ease of doing business report.

Cyber security policy: India already has a National Cyber Security Policy (2013) and efforts are in place to update it as per latest business needs.

States have also started coming out with cybersecurity policies and specific ministry departments have stepped up cyber focus in their sectors.

[04] Srikrishna committee report on data protection and privacy by May-end, Hindustan Times, 19 June 2018

[05] Centre working to reintroduce draft encryption policy, Sunday Guardian Live, 18 May 2018

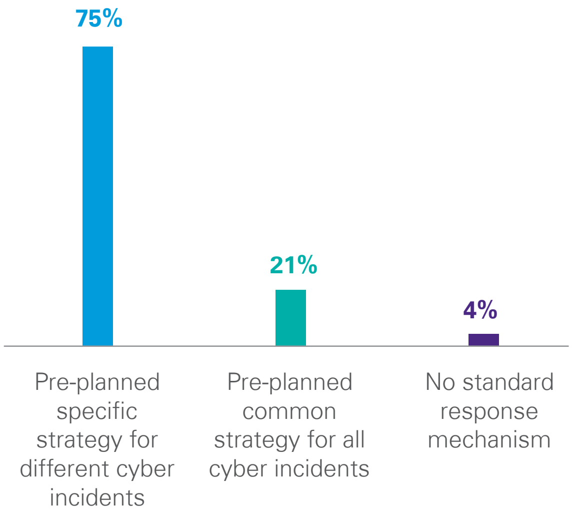
[06] Enforcement of contracts: Need to focus on ramping up court infrastructure, Business Standard, 5 November 2017

[07] All you need to know about the new IPR Policy, The Hindu, 12 September 2016

[08] Telangana government formulates cyber security policy, New Indian Express, 16 September 2016

Cohesive units of global organisations

Chart 14: Response strategies adopted to tackle cyber incidents



96 per cent of GCCs have pre-planned strategies (in line with the global organisation needs) for dealing with cyberattacks

As GCCs in India make the shift from being siloed centres controlled through service level agreement measures, to becoming centres of strategic importance[09], the need to work cohesively with their respective global organisations is pertinent. This trend has assimilated into cybersecurity operations smoothly.

A case in point is how smoothly Cyber GCCs have adopted the advanced pre-planned strategies to deal with attacks. This is indicative that Cyber GCCs are transforming as a strategic centre working cohesively with the head office, rather than SLA driven back office of parent organisations.

Chart 15: Response strategy adopted by GCCs with cybersecurity staff <=100

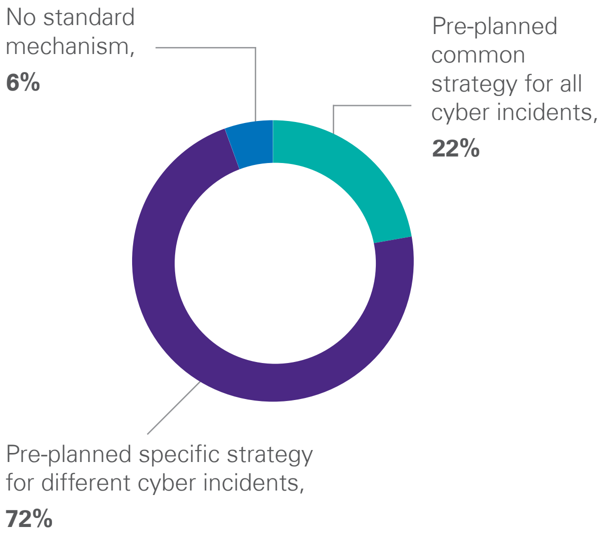
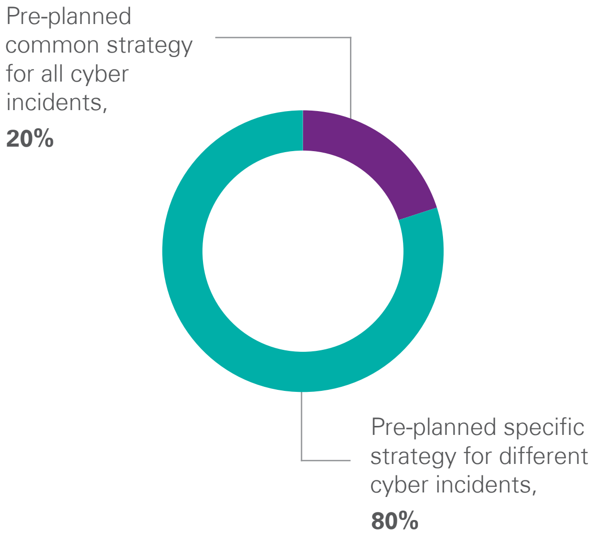


Chart 16: Response strategy adopted by GCCs with cybersecurity staff >100



Understandably, 100 per cent of larger Cyber GCCs (staff strength of over 100) have pre-planned strategies, while fewer (80 per cent) smaller GCCs (staff strength of 100 or less) have pre-planned strategies. Clearly, scale of operations brings in standardisation to Cyber GCC operations and has its advantages.

[09] 'Secure in India' Survey, KPMG in India, June 2018

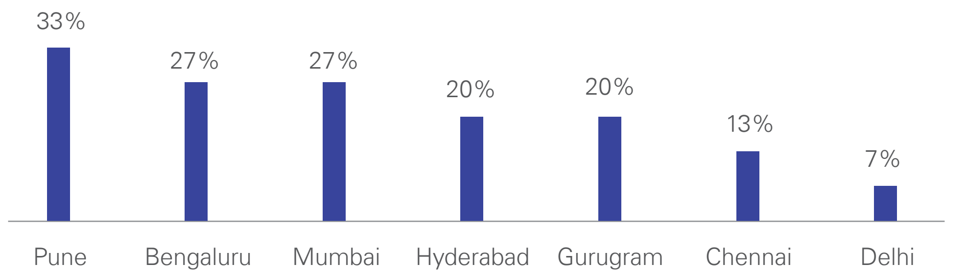
Enhancement of efficiencies through location strategies

#1: Spread to value based locations to improve efficiencies

Amongst the GCCs that were surveyed and set up in the last decade (since 2007) in India, cyber delivery capabilities are spread across Indian cities of Bengaluru, Pune, Hyderabad, Chennai, Gurugram, etc. Organisations are also considering emerging locations like Ahmedabad, Vadodara, Coimbatore, Trivandrum and Kolkata[10].

This is unlike the GCCs set up in the past (before 2007), wherein Bengaluru was the top destination for cybersecurity global delivery.

Chart 17: Presence of Cyber GCCs established since 2007, by city

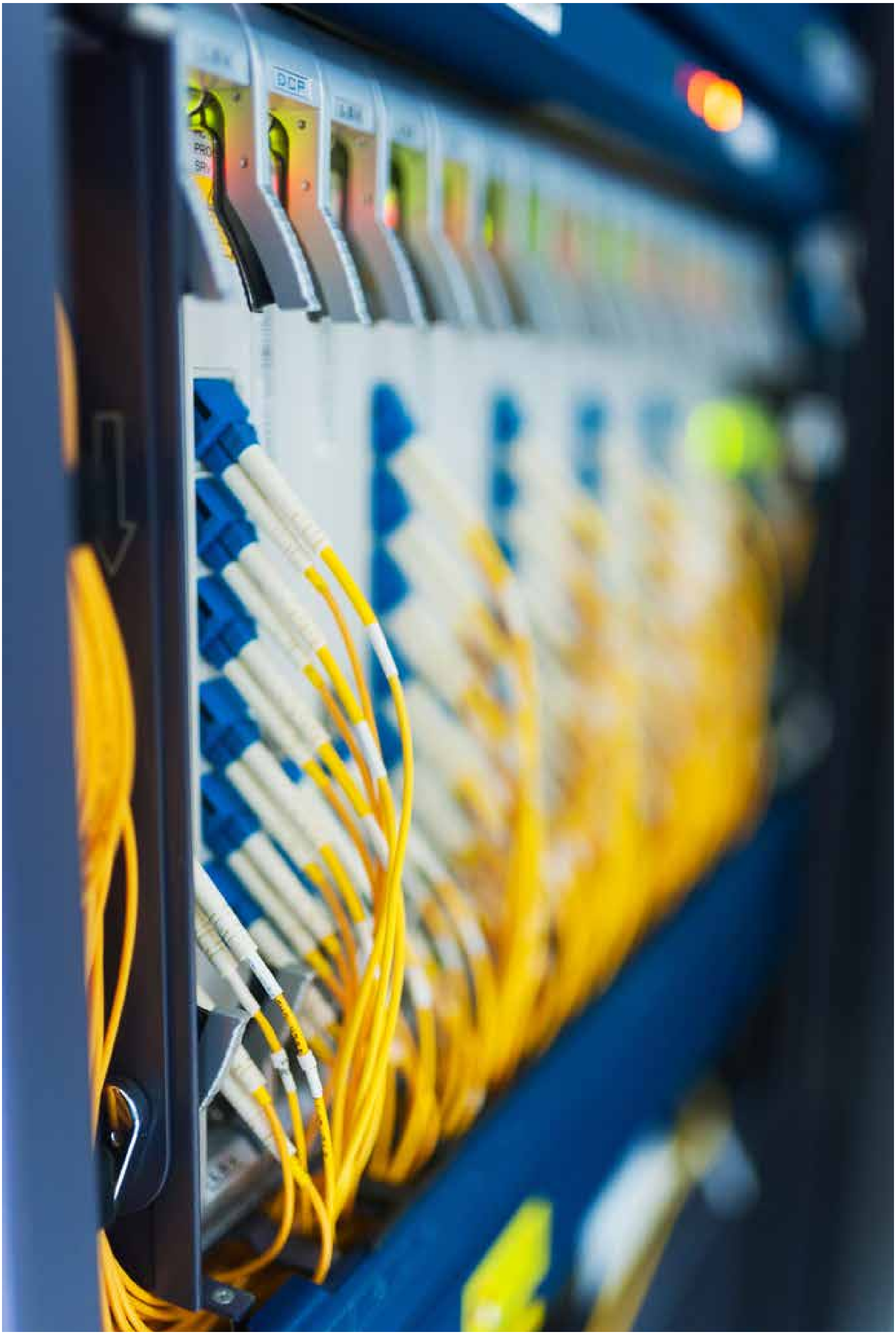


#2: Tackle concentration risk through distributed functions

Concentration of critical cybersecurity functions in a single GCC centre could result in increased systemic risk for the parent organisation. As a result, several GCCs have distributed presence across Indian cities. This also serves as a resilience measure.

Over **55 per cent** of cybersecurity GCCs in India have distributed presence to reduce concentration risks

[10] GICs in India – Emerging Centres of Excellence, NASSCOM, accessed on 12 June 2018



04.

Innovation and value creation

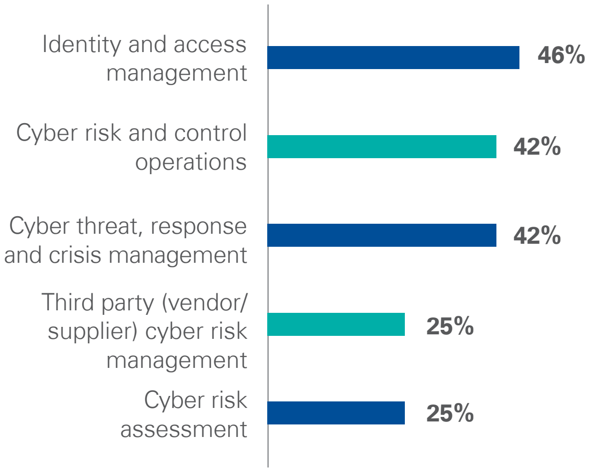
Cyber GCCs are transforming themselves as innovation hubs. Nearly 60 per cent say that 'cyber product and new solutions development' function (which fundamentally requires skilled workforce oriented towards innovation) is being delivered from Cyber GCCs, and 57 per cent say that 'cyber strategy and governance' function is being delivered from Cyber GCCs. Therefore, it comes as no surprise that over 30 per cent say that innovation potential is one of the top three drivers for setting up Cyber GCCs.

Innovation across cybersecurity functions

Nearly 50 per cent of Cyber GCCs see most innovation happening in 'identity and access management' function. Innovation across other cybersecurity functions share almost equal attention.

Privacy regulations (such as GDPR) have led most global organisations to focus on compliance and five per cent of organisations have started innovating in this space as well, within a year of privacy regulatory developments[01].

Chart 18: Cybersecurity functions which experience most innovation in Cyber GCCs

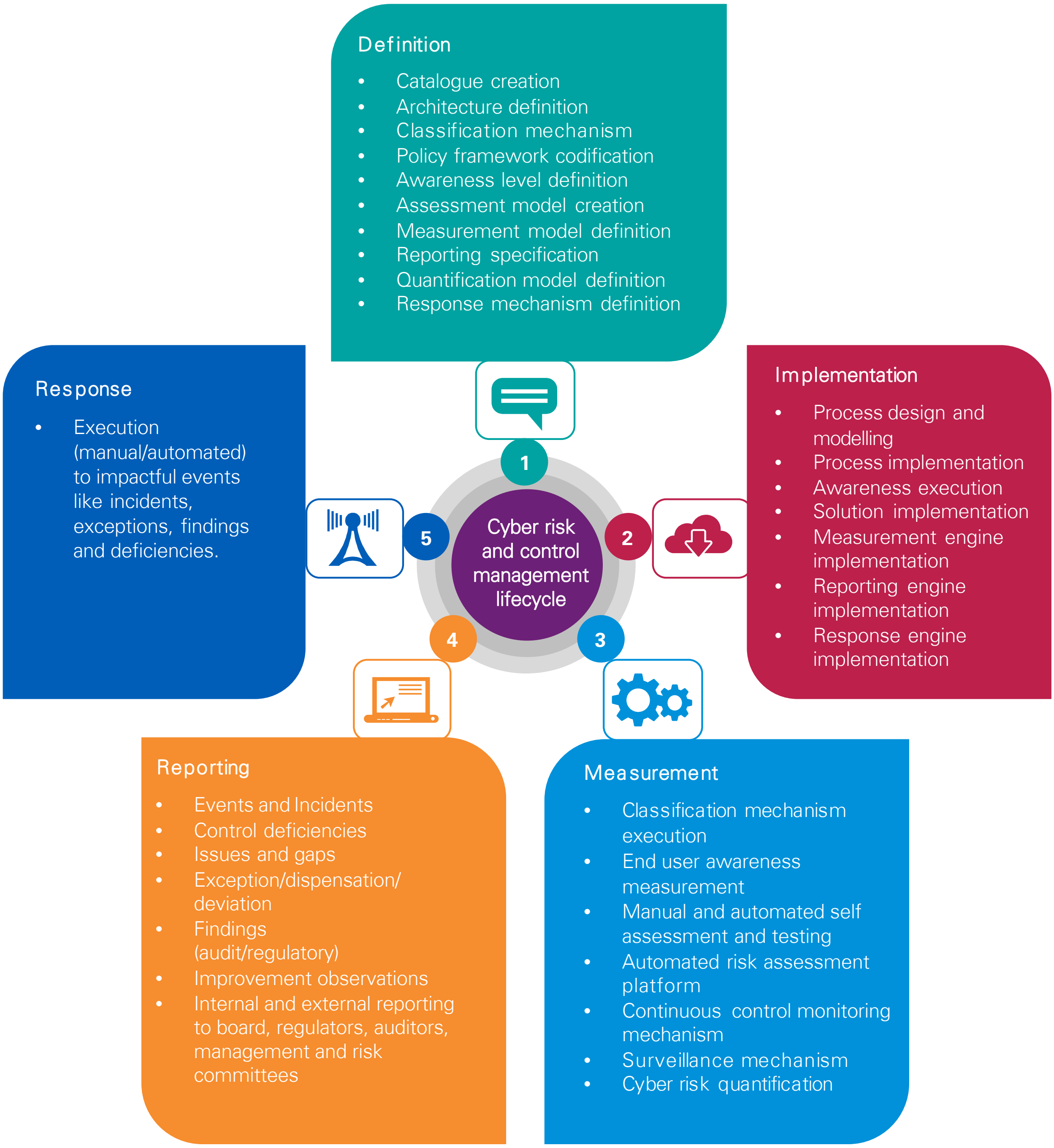


> Cybersecurity centres at GCCs provide unique opportunity to support global organizations and also simultaneously act as innovation hubs.
>
> India's ability to provide talent with sharp acumen and ability to experiment with cutting edge technologies are truly acting as catalysts
>
> **Atul Gupta**
>
> *Partner and National Leader - IT Advisory (Risk Consulting) and Cybersecurity*
>
> KPMG in India

[01] 'Secure in India' Survey, KPMG in India, June 2018

As part of this study, various examples of cyber innovation and change initiatives were shared by Cyber GCC leaders spread across cybersecurity life cycle:

Cyber GCCs present an opportunity to their global majors in incremental and transformational cyber change delivery. As Cyber GCCs understand finer aspects of cyber functions including associated solutions, their ability to re-engineer processes, enhance or build solutions and help global organisations adopt them, is naturally stronger.



Cyber risk and control management lifecycle

1 Definition

- Catalogue creation
- Architecture definition
- Classification mechanism
- Policy framework codification
- Awareness level definition
- Assessment model creation
- Measurement model definition
- Reporting specification
- Quantification model definition
- Response mechanism definition

2 Implementation

- Process design and modelling
- Process implementation
- Awareness execution
- Solution implementation
- Measurement engine implementation
- Reporting engine implementation
- Response engine implementation

3 Measurement

- Classification mechanism execution
- End user awareness measurement
- Manual and automated self assessment and testing
- Automated risk assessment platform
- Continuous control monitoring mechanism
- Surveillance mechanism
- Cyber risk quantification

4 Reporting

- Events and Incidents
- Control deficiencies
- Issues and gaps
- Exception/dispensation/ deviation
- Findings (audit/regulatory)
- Improvement observations
- Internal and external reporting to board, regulators, auditors, management and risk committees

5 Response

- Execution (manual/automated) to impactful events like incidents, exceptions, findings and deficiencies.

Source: 'Secure in India' Survey, KPMG in India, June 2018

Incubation, acceleration and co-creation with startups

India strengthened its position as the third largest start-up ecosystem in the world[02]. The start-up ecosystem naturally supplements the growth of Cyber GCCs towards innovation. In fact, 52 per cent of the Cyber GCCs have active collaboration with start-ups.

Further, industry bodies in India have programmes to assist with incubation and acceleration of start-up programmes. For instance, the NASSCOM Industry Partnership Program (NIPP) seeks to foster sustained engagement between large corporations and innovative technology ventures in India. Similarly, '10,000 Start-ups' is another NASSCOM initiative which aims to establish a cross-collaborative platform that enables start-ups to grow to the next level[03].

More Cyber GCCs with capabilities in 'cyber strategy and governance' **(64 per cent)** see value from tie-ups with start-ups, than those without **(50 per cent)**. This is indicative of the contribution of start-ups towards cyber strategy development

Expectedly, more GCCs with capabilities in 'cyber strategy and governance' (34 per cent) are able to create innovation through start-up incubations, compared to those without (28 per cent).

Chart 19: Cyber GCCs collaborating with start-ups

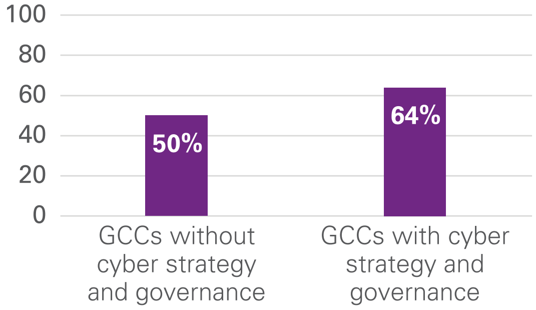
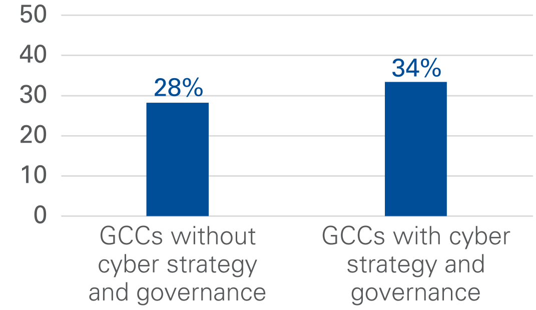


Chart 20: Cyber GCCs innovating with start ups through sponsored incubation centres



[02] Indian Start-Up Ecosystem – Traversing The Maturity Cycle - Edition 2017, NASSCOM, accessed on 19 June 2018

[03] NASSCOM Industry Partnership Program website, NASSCOM, accessed on 19 June 2018

Emerging technologies to create value

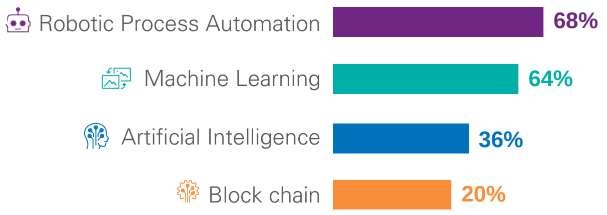
Nearly 70 per cent of GCCs say that they leverage robotic process automation (RPA) for global cybersecurity delivery, while 64 per cent say they use machine learning for global cybersecurity.

What is interesting to note is that 36 per cent are experimenting with artificial intelligence, and 20 per cent are experimenting with technologies like block chain.

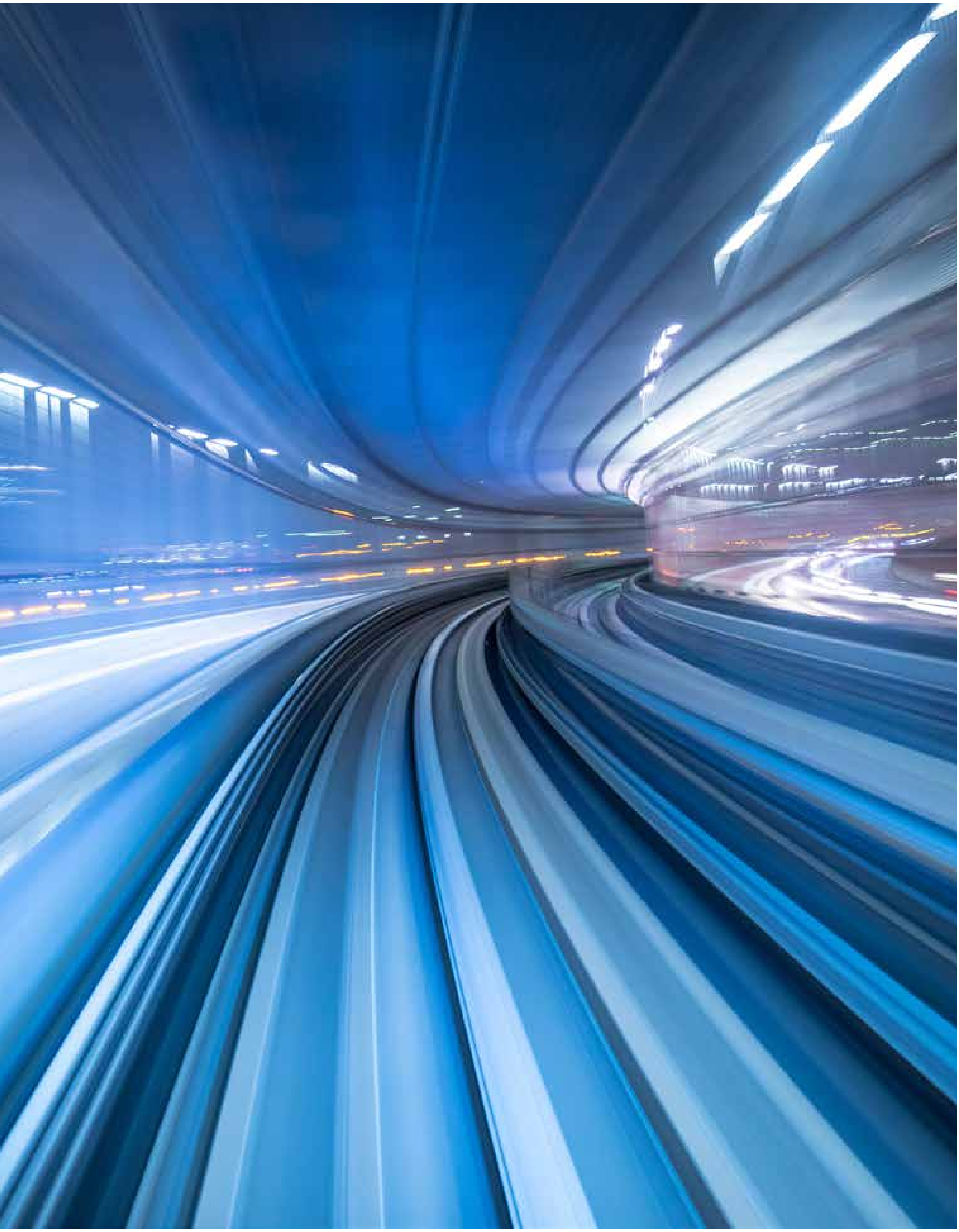
Some examples noted in the survey include bots being used to pre-empt a cyberattack and take necessary actions to prevent losses. This is reflective of the clear movement towards innovation in Cyber GCCs.

Also, as security software generates massive amounts of data, organisations are using advanced data analytics to gain a better picture of what is going on in their IT environments.[04]

Chart 21: Emerging technologies explored by Cyber GCCs for effective and efficient cybersecurity global delivery



[04] Cyber-security and the blockchain: evolving technology for our safety, The Next Web, accessed on 6 June 2018



05.

Stepping towards the future

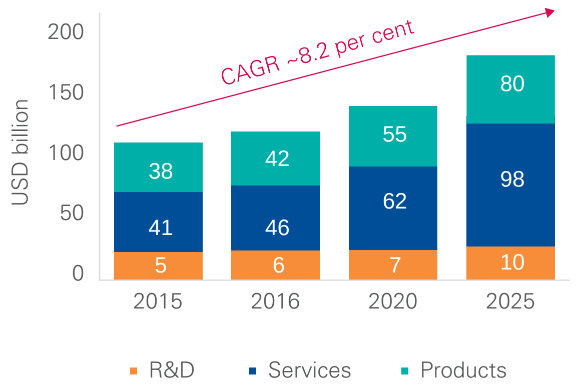
More volume, complexity and velocity of cyberthreats

The sharp rise of cyberthreats is likely to experience an upward trend, increasing at a pace, volume and complexity higher than before.

Cybercrime damages are expected to cost the world USD6 trillion annually by 2021.[01] The global cybersecurity market is expected to double to USD187 billion by 2025 from USD 94billion in 2016.[02]

68 per cent of data breaches in the past year required several months to discover, while 87 per cent had their data compromised within minutes of the attack[03]. Further, with digital transformation and emergence of new age-technologies (Industry 4.0), threats are likely to be even more complex.

Chart 22: Growth of global cybersecurity market, across different verticals



Source: Global Cyber Security market, DSCI, accessed on 7 June 2018

Recommendations for future-ready Cyber GCCs

In the wake of increasing volume, complexity and velocity of cyberthreats, it is imperative for organisations to stay abreast and manage cyber risk in order to remain in business ('business imperative'). Therefore, it is important for Cyber GCCs to be well-positioned to meet the business imperatives. A mutually beneficial ecosystem of GCCs, policy makers and industry bodies is key to continued sustenance and transformation of Cyber GCCs.

Business imperatives to manage cyber risk

- Board and leadership require enhanced risk visibility
- Regulators seek risk data aggregation, near real-time risk analysis and faster breach reporting
- Management requires to take informed and data-driven risk decisions
- Risk leadership monitors 'conduct risk' (market, employee, insider, third party) more closely
- Changing business requires business unit leaders to manage emerging technology risks
- Automated business functions require automation of risk and control functions
- Growing business and threats require better and commercial risk management models

[01] Cybercrime Damages $6 Trillion By 2021, Cyber Security Ventures, 16 October 2017

[02] Global Cyber Security market, DSCI, accessed on 7 June 2018

[03] Ransomware reigns supreme in 2018, as phishing attacks continue to trick employees, Tech Republic, 9 April 2018

Recommendations for GCCs

In our survey, we noted Cyber GCCs are employing a number of smart practices and innovative methods for smooth and secure operations of their global organisations; ranging from talent management, collaborating with external entities for value creation, to leveraging emerging technologies for smarter cybersecurity delivery. Cyber GCCs should continue to adopt these smart practices to sustain their competitive advantage and further enhance their focus and investment on innovation to transform into global centres of expertise. Below are a set of recommendations for Cyber GCCs, in order to 'score' better and 'Secure in India'.

	Skill up	Create CoEs	Expand ownership	Comply with regulations	Enhance efficiency
Transform	• Upskill to niche and expert skills, re-skill staff to stay relevant at own organisation and at an aggregate level • Cross-skill to be agile and create fungible talent pool	• Create high value generating 'centres of expertise' • Explore virtual captives to leverage vendor expertise, yet retain control • Experiment further with new-age cyber solutions using emerging technologies	• Own global functions. Move beyond SLA to outcomes. • Transform cost centres to the ones that generate revenue • Enhance brand proposition of the Cyber GCC to make stakeholders aware and attract talent	• Proactively track and manage regulatory change • Formulate inter-entity outsourcing contracts • Simulate cyberattacks and stress test in line with regulatory requirements (community model with peers, where possible)	• Develop a 'Cobot' environment, for smooth co-existence of human and robotic environment • Expand Agile and DevSecOps[04] paradigm to fast-track value creation
Sustain	• Retain 'right' skill by providing growth opportunities • Tie up with academia to develop niche cyber programmes, nurture talent and create immersive learning opportunities	• Incubate, accelerate, and co-create with start-ups to fortify innovation hubs • Learn from experiences, experiments and innovation of peers to scale up and better the value chain • Collaborate with subject matter experts in areas of demand and growth	• Invest in high quality leadership with deep domain and technical expertise • Create leadership accelerator programmes • Invest in personal coaching for top leadership	• Collaborate with regulators and industry bodies to understand industry wide issues and response strategy • Invest in automation for regulatory testing, analysis and reporting • Involve in policy matters, that can potentially impact cybersecurity and privacy domains	• Continue investing in productivity enhancements like automation and collaborative workspaces • Engage with local government and regulatory initiatives • Enhance exploration of high value locations

[04] DevOps and security: An important intersection, KPMG Advisory Institute (US), 12 September 2017

Industry body recommendations

	Policy makers	GCC Community (Industry bodies, GCC forums etc.)
Brand	• Enhance the focus on GCCs' potential in creating high value careers in cybersecurity and privacy, as part of the government's drive towards employment growth • Promote 'Secure in India' branding, leverage existing and new policy initiatives to champion India as a global destination for cybersecurity and privacy capabilities	• Track and communicate the Cyber GCC capability within and outside the country • Create a pitch for attracting global companies to look at India for delivering their security capabilities
Skill	• Enable and contribute to skill development in abundance which is required for 'Secure in India'	• Enhance the supply of skills for realising the potential
Collaboration	• Continue to work towards enhancing policies for attracting more global organisations and GCCs to set up and expand global cybersecurity delivery from India	• Continue to work towards enhancing the policy environment that is more conducive and incentivises delivery of cybersecurity from India • Put concerted efforts for realising cybersecurity and privacy potential and scaling up deliveries from India

Additional Insights noted in the 'Secure in India' survey

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

Respondent profile

1. Distribution of sectors served by survey respondents
2. Establishment year of GCCs surveyed
3. Location distribution of Cyber GCCs

Importance of Cyber GCCs

1. Senior cybersecurity leadership, in India based Cyber GCCs, serving in global committees
2. Global leaderships' view on investment in cybersecurity global delivery capability in GCCs

People and skill matters

1. India based Cyber GCCs' staff strength
2. Years of professional experience of staff in Cyber GCCs
3. Key diversity to Cyber GCCs
4. Innovative and new age methods adopted to upskill employees in Cyber GCCs
5. Annual attrition percentage within Cyber GCCs
6. Primary reasons for attrition within Cyber GCCs
7. Cybersecurity function with the most skill gap

Cyber threats and readiness

1. Top concerns as Cyber GCC global delivery head
2. Obligations or requirements that the Cyber GCCs are most concerned with
3. Readiness of Cyber GCCs to deal with cyber threats

Leading practices

1. How Cyber GCCs provide visibility and assurance on their cybersecurity global delivery to the global leadership
2. Processes, leading practices and innovative approaches within Cyber GCCs to comply with regulatory and auditing requirements

External influences

1. Government initiatives which have had/are expected to have a positive impact on India based cyber GCCs
2. Local laws and regulations impacting Cyber GCCs
3. Global regulations impacting Cyber GCC

Annexure

Annexure I: Cybersecurity functions

In the context of this report, the scope of the term cybersecurity includes below functions

#	Cybersecurity area	Description	Cybersecurity function	Individual description
1	Strategy and Governance	Niche functions involved in cybersecurity strategy and governance	Cybersecurity strategy and governance	Defining the approach to cybersecurity which aligns with the business objective, implementing the plan and monitoring it.
2	Research and Development	Functions involved in product and solution development and research for cybersecurity management, for use either both within the organisation and/or outside. At a functional level, team employs highly skilled personnel with core technical skills to develop IT enabled products.	Cyber product and new solutions development	Research and development of automation solutions, cyber and risk analytics, emerging tech risk management solutions, etc.
3	Engineering	Function implements, and/or performs maintenance of already developed cybersecurity products, for use either both within the organisation and/or outside. At a functional level, team employs personnel with adequate technical skills to implement and maintain cybersecurity products	Cyber product implementation and maintenance	This includes implementation and maintenance of automation solutions, cyber and risk analytics, emerging tech risk management solutions, risk measurement solutions, etc.
4	Cyber risk and control management	Function executes operations either on a need basis, and/or an ongoing basis. At a functional level, team employs personnel with varied technical skills (from high to low technical skills) to execute cybersecurity operations.	Cyber risk assessment	Cybersecurity and regulatory risk assessment exercise (to identify and validate new and current risks) on a periodic basis
5			Cyberthreat, response and crisis management	Identify cyberthreats, plan responses in case of a cybersecurity event, and perform investigations (functions include crisis simulation, awareness, etc.)
6			Cyber risk and control operations	Cyber operations (vulnerability assessments, management of anti-virus and firewall, ISO27001 implementation, network health monitoring, security operations centre, etc.)
7			Identity and access management	Operations and management of identity and access work
8			Business continuity and ITDR	Business continuity and IT Disaster Recovery planning, testing, and upkeep.
9			Third party (vendor/supplier) Cyber risk management	Advisory, management and operations of identity and access work
10			Data privacy risk management	Management and operations of privacy risk (including definition of obligations)
11			SOx and other compliance/audit management	Regulatory compliance related work such as control definition, assessment, reporting on gap remediation

Annexure II: Leading practices of GCCs handling local crisis situations

#	Challenge	Leading practice
1	Early monitoring potential crisis situation	Organisations which monitor the situation closely are able to initiate evacuation efforts before the situation worsens
2	Handle changed priorities	'Run' vs. 'Change' functions - focus of most business continuity plans is typically to ensure timely recovery of 'Run' functions of an organisation. However, given the duration of disaster and its timing (for e.g. right before year-end freeze and holidays, organisations need to re-prioritize their recovery efforts and ensure that projects go-live dates are not impacted.
3	Leveraging social/ mobile app for 'call tree'	Due to network disruption, most of the traditional call tree invocation methods fail (30-40 per cent failure). This impacts communication and coordination with the identified recovery teams. Social/ mobile app based connect work intermittently and has significantly higher results (60-70 per cent success) compared to traditional call tree mechanisms.
4	Adherence to regulatory requirements	Ensure regulatory requirements are not compromised during and after crisis situation.
5	Work From Home (WFH) strategy may not work all the time	WFH strategy for resources working in affected areas may not work due to disruption in network services and extended power outage.
6	Planning for co-location agreements	Service providers supporting a particular organisation are able to leverage each other's premises to resume critical services to their clients. This can already be worked out as part of the contract.
7	Importance to support services	Strong commitment of the support staff (including administration, plumbing, electricians, and logistic services providers) could be key to recover support infrastructure at affected locations. Logistics department in organisations should be able to leverage their relationship with hotels to arrange for a large number of rooms at a short notice.
8	Leveraging alternate site for network services	Based on the early warning, organisations should switch their international traffic route to other locations.
9	Help desk services	Ensure alternative arrangement for Help desk services.
10	Being aware of fourth party continuity risks	Communication service providers relying on other internet service providers would not be able to meet the committed SLAs due to power outage for a sustained period.
11	Sentiment management –unskilled volunteers may do more harm than good	'Let us do what we can do' and 'let us leave evacuation efforts to experts' should be the leadership direction
12	Focusing on employee and their families' safety	Along with critical team members, organisations also needs to evacuate their families from the impacted areas.

'Secure in India' Survey, KPMG in India, June 2018

Methodology

The premise of this report is based on several sources of information, meetings and brainstorming sessions undertaken by KPMG in India, DSCI and NASSCOM between April 2018 and June 2018.

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) registered with NASSCOM 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.

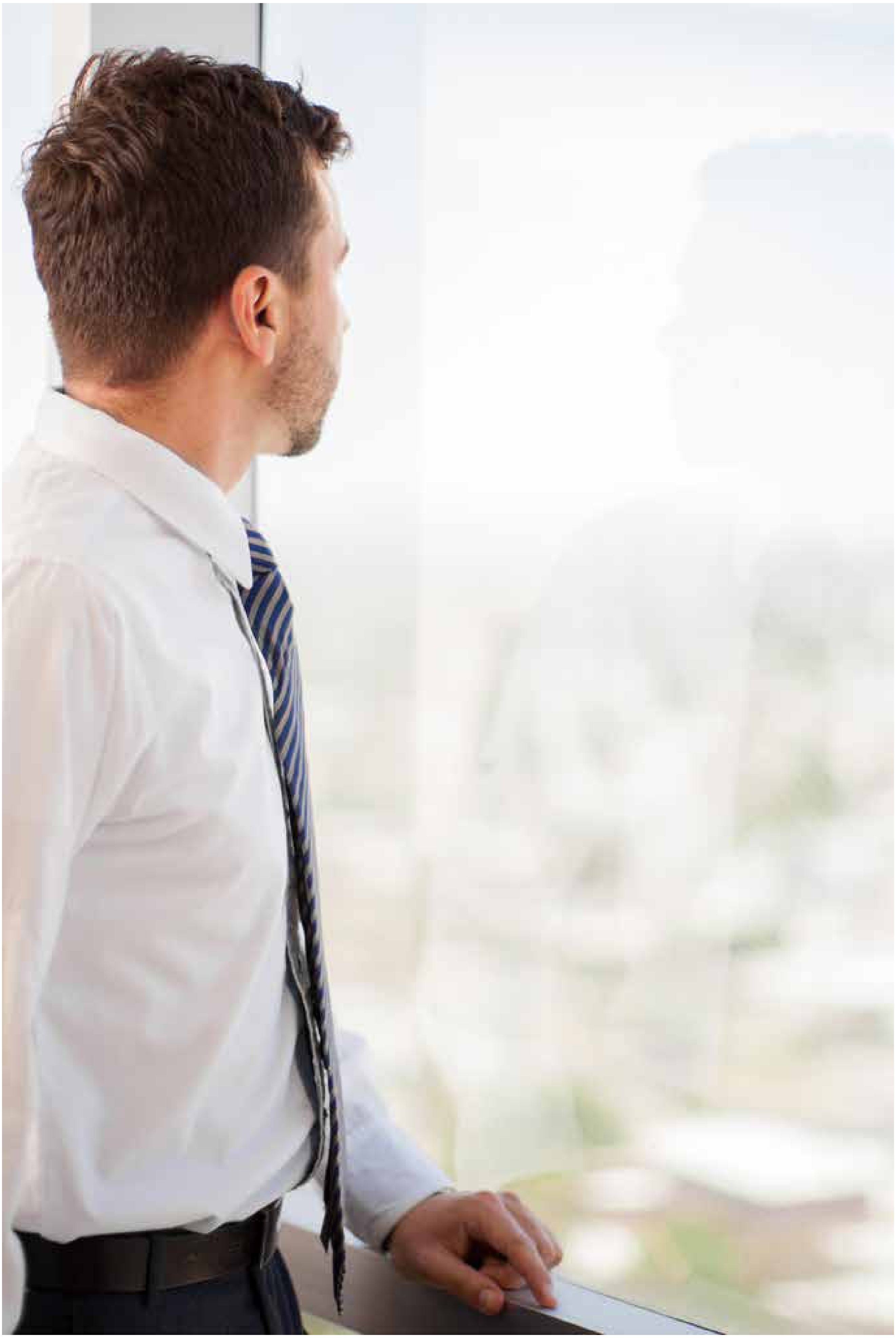
This survey has representation from twelve (12) key sectors, namely, infrastructure, automotive, banking, insurance, investment management, life sciences, technology, telecom, manufacturing, consumer and retail, healthcare and pharmaceuticals, and energy. The survey was conducted between 26 April 2018 and 15 June 2018.

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 each analysis. The team relied on the organisation's proprietary databases and public websites to gain better understanding into each insight.



Acknowledgements

Our thanks goes to all the executives of India-based GCCs who invested their valuable time to give inputs and contribute to this report.

Our special thanks to the advisory panel led by Rishi Mehta, Director, Information Security (Target), Vinayak Godse (DSCI) and Srinivas Potharaju (KPMG) for their strategic direction from conceptualisation to the launch of the report.

Our thanks to all the KPMG Partners, Directors and colleagues who assisted in distributing the survey to GCC contacts.

We acknowledge the efforts put in by the below in preparing this report.

KPMG in India

- Atul Gupta
- Abhijit Varma
- Santhosh Mayanna
- Priyanka Saraf
- Divya Mishra
- Puneet Tandon
- Reetam Sinha
- Sharon D'Silva
- Rishabh Rane
- Shilpa Bhoir

DSCI

- Vinayak Godse
- Mayank Lau
- Aastha Dhamija

NASSCOM

- Paresh Degaonkar
- Rakesh Kumar

About KPMG in India

KPMG in India, a professional services firm, is the Indian member firm affiliated with KPMG International and was established in September 1993. Our professionals leverage the global network of firms, providing detailed knowledge of local laws, regulations, markets and competition.

KPMG in India offers 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 cyber security 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:

Mritunjay Kapur
National Head
Markets and Strategy
Head - Technology, Media and Telecom
T: +91 124 307 4797
E: mritunjay@kpmg.com

Akhilesh Tuteja
Global Cybersecurity Co-Head
and Head of Risk Consulting
T: +91 124 307 4800
E: atuteja@kpmg.com

Atul Gupta
Partner
National Leader - IT Advisory
(Risk Consulting) and Cybersecurity
T: +91 124 307 4134
E: atulgupta@kpmg.com

Srinivas Potharaju
Partner
GCC Leader for Risk Consulting
T: +91 98459 19740
E: srinivasbp@kpmg.com

DSCI contacts:

Vinayak Godse
Senior Director
T: +91- 9873083123
E: Vinayak.Godse@dsci.in

Mayank Lau
Senior Consultant
T: +91- 9717869745
E: Mayank.Lau@dsci.in

dsci.in

NASSCOM contact:

Nasscom
Plot 7 to 10, Sector 126, Noida
201303, India
T: +91 120 499 0111
E: research@nasscom.in

nasscom.in

KPMG in India
25 YEARS
of making a difference

Follow us on:
kpmg.com/in/socialmedia

This report has been jointly developed by KPMG In India and DSCI.

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 survey respondents and do not necessarily represent the views and opinions of KPMG in India.

Although we have attempted to provide correct and timely information, there can be no guarantee that such information is correct as of the date it is received or that it will continue to be correct in the future.

The report may make reference to 'KPMG Analysis'; this merely indicates that we have (where specified) undertaken certain analytical activities on the underlying data to arrive at the information presented; we do not accept responsibility for the veracity of the underlying data.

This document is meant for e-communications only.