KPMG

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Secure in India 2026

Cyber GCCs* in the age of AI

September 2026

kpmg.com/in

KPMG. Make the Difference.

Contents

GCC – Global Capability Centre
*Cyber GCC refers to teams focused on global cybersecurity delivery, located within respective GCCs in India. Cyber GCC was coined in 2018 in the first edition of Secure in India.

Foreword

The global business landscape continues to be influenced by complex geopolitical and economic uncertainty, emergence of tariff driven global trade, physical and digital supply chain disruption, proliferating Artificial Intelligence (AI) adoption and exploration. These global trends have resulted in intense global cyber-warfare, relentless, sophisticated and targeted cybersecurity attacks, heightened regulatory scrutiny, unprecedented disruptions in day-to-day life due to cybersecurity incidents, novel risks induced by AI and other advanced technologies including Operational Technology (OT) etc.

GCCs in India have risen to the challenges their global organisations have been dealing with and emerged as strategic pillars of resilience, innovation, and leadership in this Volatile, Uncertain, Complex and Ambiguous (VUCA) world. Cyber GCCs* are no longer limited to augment and help their global teams. They now lead, innovate and strategise cybersecurity and digital risk management, enabling their global organisations realise significant value and business growth.

The current edition of "Secure in India 2026", fourth in the series, builds on the insights from previous editions and explores how cyber GCCs are redefining cybersecurity and digital risk management in an AI-driven world. This edition focuses on the expanding cyber GCC ecosystem, the development of diverse and future-ready cybersecurity talent, the intersection of AI and cybersecurity, the role of research and development in driving innovation, and the current global imperative of building cybersecurity resilience. Through these perspectives, this report aims to provide global leadership with actionable insights and a forward-looking view on how cyber GCCs are enabling organisations to operate securely amidst business disruption and technological transformation noted above.

The insights detailed in this report have been prepared based on an extensive study and in consultation with global cybersecurity and digital risk leaders, cyber GCC leaders, cybersecurity Subject Matter Experts (SMEs) and reputed industry bodies.

Cyber GCCs have become trusted partners for cybersecurity and digital risk management, enabling their global organisations "Secure in India".

Srinivas Potharaju
Partner and Head,
Cyber Security &
Technology
KPMG in India

Foreword

What began as a model focused on operational efficiency has evolved into a strategic ecosystem where enterprises drive innovation, digital engineering, artificial intelligence, advanced analytics, and cybersecurity at scale. Today, Global Capability Centers are not only centers of excellence but also critical contributors to the competitive advantage of global enterprises.

The growing concentration of intellectual property, sensitive data, digital assets, AI-driven systems, and globally interconnected operations has elevated cyber resilience to a boardroom priority. The continued success of GCC ecosystem will increasingly depend on organizations' ability to establish trust, secure digital operations, and maintain confidence among customers, regulators, investors, and stakeholders worldwide.

This report examines the evolving cybersecurity landscape across India's GCC ecosystem and highlights the priorities, challenges, and opportunities shaping the sector. The findings indicate a clear shift toward integrated cyber resilience strategies that align security objectives with business outcomes. Organizations are increasingly investing in advanced threat detection, cloud security, AI-enabled security operations, identity-centric architectures, third-party risk management, and proactive resilience measures to address a rapidly evolving threat environment.

A key observation from the report is that cybersecurity maturity is becoming a defining differentiator for GCCs. As enterprises entrust their Indian centers with greater strategic responsibilities, GCCs are expected to lead in securing digital transformation initiatives. Cybersecurity talent, innovation in security operations, adoption of emerging technologies, and global collaboration are becoming critical pillars of sustained growth and resilience. The report also highlights the changing nature of cyber risk driven by the convergence of cloud computing, artificial intelligence, software-defined infrastructure, operational technology, and increasingly sophisticated threat actors. Addressing these challenges requires organizations to move beyond traditional security models and embrace resilience-focused approaches that prioritize preparedness, adaptability, and continuous risk management. With its deep talent pool, vibrant innovation ecosystem, and growing cybersecurity capabilities, India is uniquely positioned to become a global hub for both business transformation and cyber resilience leadership.

At DSCI, we remain committed to advancing this vision through industry collaboration, capacity building, thought leadership, research, and the promotion of best practices that strengthen India's digital trust ecosystem. We hope this report serves as a valuable resource for business leaders, CISOs, technology executives, policymakers, and GCC stakeholders.

Vinayak Godse
CEO, Data Security
Council of India (DSCI)

Foreword

Global business landscape, amidst geopolitical conflicts, supply chain disruption and energy crisis, is marked by rising AI adoption, innovation, business transformation and technology led change.

One of the biggest challenges the world continues to face is the weaponization of cybersecurity, while the world continues to experience growing shortage of cybersecurity talent. As companies deal with global business disruption and adopt cloud, AI, and automation at a rapid pace, they need more specialized cybersecurity skills than the current global talent pool can supply. This gap is forcing organizations to rethink how they build and scale cybersecurity expertise, often turning to distributed and global teams that can provide more reliable outcomes.

Adding to the pressure is the rise of AI-driven cybersecurity attacks. Cybercriminals are using AI to sharpen their methods, create convincing phishing campaigns, and identity-driven attacks. This creates a double challenge managing the risks that AI introduces externally, while also ensuring their own AI tools are safe, transparent, and well governed. The emergence of new AI models specifically for cybersecurity may have the potential to globally reframe how cybersecurity is managed.

Envisioning this gap and challenge of cybersecurity talent in 2015, Hon'ble Prime Minister of India, Shri Narendra Modi, called upon the Indian IT Industry to focus on cyber security during his address at the programme to mark the 25th Foundation Day of Nasscom. He urged the Indian IT industry to focus on meeting the global challenge of cyber-security. Stating that the entire world is concerned about this issue, the Prime Minister said Indian IT professionals could do a lot for cyber-safety of digital assets across the world.

Today, in 2026, we operate in a dynamic and increasingly complex global environment, where Global Capability Centers (GCCs) have an unprecedented opportunity to create strategic value for their global organizations. India's GCC ecosystem is at the heart of this transformation. Organizations around the world are increasingly looking to India to accelerate innovation, research and development, and business operations for delivering at speed, scale, quality, and commercial efficiency while advancing their critical business objectives.

India's journey in cybersecurity is an equally compelling success story. The country took the Prime Minister's 2015 call to action seriously and has demonstrated its ability to build and provide a world-class cybersecurity workforce to GCCs across the spectrum ranging from operational and tactical capabilities to strategic leadership. At the same time, India has been building a sustainable cybersecurity ecosystem, fostering innovation, developing indigenous capabilities, and creating opportunities to integrate and scale Make in India cybersecurity products to diversify trusted supply chains across these global organisations. The result has been a powerful evolution. Cyber GCCs have emerged as an inherent and increasingly strategic component of the broader GCC ecosystem and a source of competitive advantage for global organisations seeking resilience, innovation, and sustainable growth.

From anticipating risks arising from rapidly evolving business models and accelerating digitisation to enabling the secure adoption of emerging Make in India technologies, Cyber GCCs are playing a pivotal role. They are not merely protecting businesses; they are helping organisations innovate with confidence, nurture world-class talent, strengthen resilience, and deliver measurable business value through the efficiencies of scale.

As Artificial Intelligence continues to redefine business boundaries and reshape the cybersecurity landscape, the global conversation is increasingly centred around three imperatives or 3 T's - Trust, Talent, and Transformation.

Organisations that invest today in strong digital foundations, cyber resilience, future-ready cybersecurity talent, and globally coordinated cybersecurity and digital-risk management will be best positioned to navigate uncertainty, capture new opportunities, and lead in the next era of digital transformation. Thousands of organisations have already invested in India-based Cyber GCCs and are realising significant strategic and business benefits. This report seeks to illuminate this powerful phenomenon in greater depth and demonstrate its potential to the wider global business ecosystem. The opportunity ahead is significant. By combining India's talent, innovation, scale, and growing cybersecurity ecosystem with the ambitions of global organisations, together we can build and transform to a more secure, resilient, trusted and digitally confident future.

Invest in India. Secure in India. Innovate from India. Lead globally.

Dr. Sanjay Bahl
Director General (DG)
Indian Computer Emergency Response Team (CERT-In)

Key Takeaways

1 Cyber GCC ecosystem

1. **Cyber GCC workforce in India is expanding significantly** - Over 25 per cent of cyber GCCs now have nearly 50 per cent of their global cybersecurity workforce in India, while 22 per cent operate large cyber teams of more than 100 professionals
2. **Role and influence of cyber GCCs is growing** - 51 per cent of organisations have team members outside India reporting into India-based GCC cyber leadership and 80 per cent of cyber GCCs have leadership presence in global cybersecurity committees
3. **Cybersecurity is beyond CISO function** - 98 per cent of cyber GCCs now follow the Three Lines of Defence (3LOD) model for cybersecurity, consistently across sectors, as against 78 per cent in 2023
4. **Top drivers for cyber GCC model** - Availability of skilled resources in cybersecurity continues to be one of the top drivers for leveraging the GCC model, followed by uninterrupted service delivery and continuous innovation and agility
5. **Key factors influencing cyber GCC growth** include increase in scope of cybersecurity functions being delivered, seamless collaboration with the IT and other functions, and budget constraints in global locations
6. **Expanding cyber GCC ecosystem** - 69 per cent of cyber GCCs in India are engaging with a broader ecosystem that includes start-ups, academia, government bodies, PSUs, law enforcement agencies, think tanks, and industry associations
7. **AI security is emerging as a key cybersecurity function**, while cybersecurity risk assessments, cybersecurity operations, Third party Risk Management (TPRM) and Identity and Access Management (IAM) etc., continue to be part of the top ten cybersecurity functions delivered by cyber GCCs.

Key Takeaways

2 Cybersecurity talent

1. **AI security is one of the top priority skillsets for cyber GCCs,** with AI for security and security of AI gaining prominence
2. **Demand for cybersecurity talent within cyber GCCs is rising** sharply in strategic areas such as cybersecurity governance, cyber resilience, AI security, cybersecurity risk assessments, cybersecurity architecture, and cloud security
3. **Top cyber GCC strategies to upskill cyber talent include** training and awareness programmes (17 per cent), active participation in cyber forums (14 per cent), collaborative learning sessions within different cybersecurity functions (14 per cent), knowledge base/online portals (12 per cent), rotational assignments/internal job transfers (12 per cent), gamification (11 per cent), gen AI/AI-powered learning (10 per cent), industry wide cybersecurity attack/crisis simulation (10 per cent)
4. **Cyber GCC attrition has reduced significantly** – Cybersecurity workforce stability in cyber GCCs is strong, with 48 per cent of cyber GCCs reporting low attrition (< 7 per cent) due to structured learning ecosystems, career mobility, AI powered cybersecurity
5. **Key challenges faced by cyber GCCs in attracting and retaining talent** include compensation and rewards (20 per cent), market demand for similar skills (19 per cent), location preferences (11 per cent)
6. **Key initiatives to promote cyber GCC risk culture include** training and awareness (29 per cent), organisational commitment to cybersecurity (21 per cent), gamification/simulation/bug bounties (17 per cent).

Key Takeaways

3 AI and cybersecurity

1. **AI emerged as a force multiplier for cyber GCCs**, with organisations reporting the strongest benefits of AI adoption in greater operational efficiency, more effective risk and threat management and compliance management
2. **Key use cases of AI for cyber** include automation of routine security tasks (46 per cent), improved SOC alert triage (42 per cent), enhanced risk assessment and threat modelling (35 per cent), faster correlation and analysis of adversarial threats (33 per cent) and easier configuration of security controls (31 per cent)
3. **Top AI security challenges** include data security and privacy, governance, regulatory and compliance risks, model and system vulnerabilities, bias, fairness and ethical concerns and AI inventory challenges
4. **Key AI security management activities** implemented by cyber GCCs include AI security policies and standards (47 per cent), establishment of AI regulatory and governance functions (35 per cent), responsible AI functions (33 per cent), AI risk assessment frameworks (31 per cent) and AI-specific security monitoring and incident response capabilities (33 per cent)
5. **Third-party AI security risk management is emerging** with 18 per cent of organisations having defined a mechanism for identifying, assessing and managing third-party AI security risks, 15 per cent having implemented such a mechanism, and a further 15 per cent having progressed to continuous identification, monitoring and remediation.

Key Takeaways

4 Cybersecurity research and development and innovation

1. **Key cyber GCC innovation initiatives** include empowering staff with AI/gen AI training and assistance(19 per cent), idea-based investments and encouraging entrepreneurship(18 per cent), focused innovation programme for idea generation(17 per cent) and incubation events, hackathons, bug bounty programmes(14 per cent), innovation as a KPI for performance review (14 per cent)
2. **Top cyber domains undergoing innovation at cyber GCCs** include cybersecurity operations (e.g. SOC, DLP, etc.) (14 per cent), cybersecurity risk assessments (11 per cent), cybersecurity engineering, product management and automation (7 per cent), and IAM (7 per cent)
3. **Cybersecurity R&D in cyber GCCs has risen significantly** with 65 per cent of cyber GCCs having a cybersecurity lab and 67 per cent increasing overall investment in cybersecurity R&D since 2023
4. **Top trends chosen by cyber GCC leaders in the next three to five years** include increasing demand for specialised, niche cybersecurity expertise (23 per cent), widespread adoption of autonomous cybersecurity operations (agentic AI) (21 per cent), and the rise of India as a global tech product/IP development hub (17 per cent)
5. **Key strategies for dealing with top cybersecurity priorities for the next three to five years,** chosen by cyber GCC leaders, include building deep expertise in emerging tech (Eg. AI, OT and quantum) (23 per cent), developing skilled talent for future technologies (23 per cent) and identifying complex cybersecurity problems and solving them (Eg. post quantum cryptography, medical device cyber protection, bio-medical cyber management etc.) (19 per cent), partnership with universities and startups on niche skills and focused R&D (13 per cent), shifting from support roles to creating new innovation and IP (13 per cent)
6. **Top Centres of Excellence (COE) established by cyber GCCs** include incident response (16 per cent), threat management (13 per cent), AI security (12 per cent), third party cybersecurity (10 per cent), cloud security (10 per cent) etc.

Key Takeaways

5 Cybersecurity resilience

1. **Top cybersecurity challenges of cyber GCC leadership** include navigating a changing regulatory landscape (13 per cent), managing third-party cybersecurity risk (11 per cent), rise in emerging cybersecurity attacks due to adoption of emerging technologies (9 per cent) and embedding a strong risk culture (8 per cent), while AI security, OT security, cloud security, software supply chain security challenges continue to evolve rapidly
2. **Top cybersecurity challenges cyber GCCs are facing during cloud adoption** include misconfiguration and inadequate change control (15 per cent), regulatory compliance (13 per cent), multiple cloud security tools requirement for code to cloud security (10 per cent) etc.
3. **Cyber GCC preparedness in dealing with top cybersecurity threats has matured significantly**, especially against active threats such as insider threats, malware, phishing, etc. AI security threats have become one of the top threats along with Advance Persistent Threat (APT), data breach, etc.
4. **Top cybersecurity risks tracked by global boards** now include AI misuse, OT security risk, software supply chain security risk, third-party security risk, while critical infrastructure risk, cloud expansion risk, regulatory risk etc., continue to be part of the top ten risks
5. **Key strategies cyber GCCs are employing to deal with geopolitical impact,** and other global disruptive trends include 'implementation of stricter access controls and insider threat monitoring', 'upskilling local cybersecurity talent to reduce dependency on global mobility', 'strengthening internal cybersecurity capabilities and reducing reliance on foreign vendors' etc. Mature cyber GCCs with significant cybersecurity workforce and experience were observed to have better ability and preparedness in helping their global organisations deal with these events
6. **Cyber GCC contribution to quantum security, OT security, software supply chain security** etc. has matured significantly
7. **Cyber GCCs have significantly scaled up cyber fusion centres** and dedicated cybersecurity COEs, in addition to maturing and expanding security operation centres. Key benefits experienced include faster incident response time (21 per cent), improved threat intelligence sharing (21 per cent) and better cybersecurity outcomes (21 per cent).

1

Cyber GCC ecosystem

1.1 Cyber GCCs have consistently grown over the years

With the growing number of GCCs in India in the last decade, cybersecurity functions have witnessed an exponential growth. 61 per cent of GCCs established their cyber presence in India in the last decade.

Before 2008	2008-2015	2015-2026
13%	32%	61%

1. Most of the GCCs established after 2023 have incorporated cybersecurity functions
2. Even the GCCs established before 2023, have expanded cybersecurity functions between 2023-2026

1.2 Cyber GCCs in India emerge as nerve centres of global cybersecurity

Cybersecurity teams in GCCs are diverse and rapidly expanding.

Over 25 per cent of cyber GCCs now have nearly half of their cybersecurity workforce based in India. This reflects a significant surge in cybersecurity team strength, since 2023. In addition, 23 per cent of cyber GCCs maintain cybersecurity teams with at least 100-200 members.

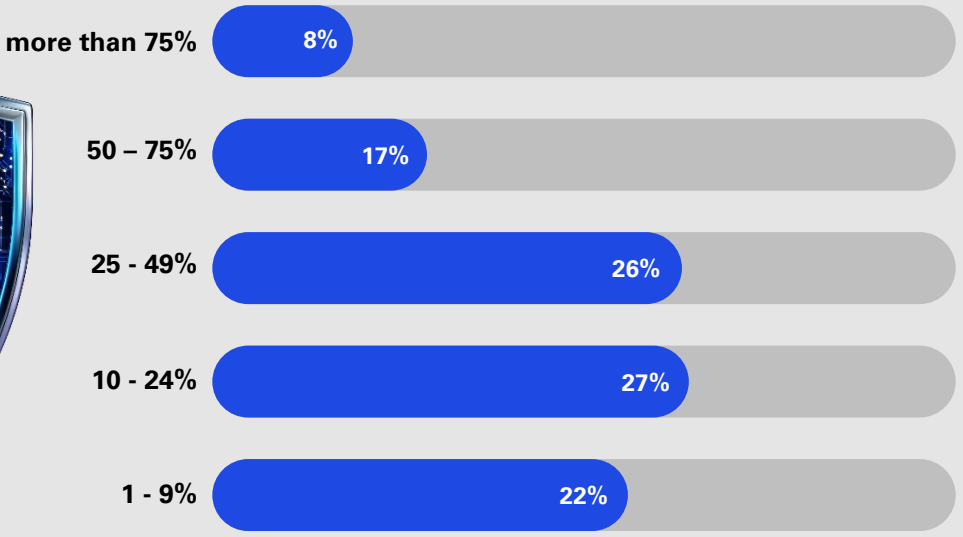


Figure 1: Percentage of cybersecurity staff based out of Cyber GCCs

1.3 More global cybersecurity teams reporting into cyber GCC leadership

51 per cent of cyber GCCs have global teams reporting to India based cyber GCC leadership. Cyber GCCs, operating over a period, have more global cyber leadership resident in the cyber GCCs, indicating maturity in delivering cybersecurity and digital risk management to their global organisations.

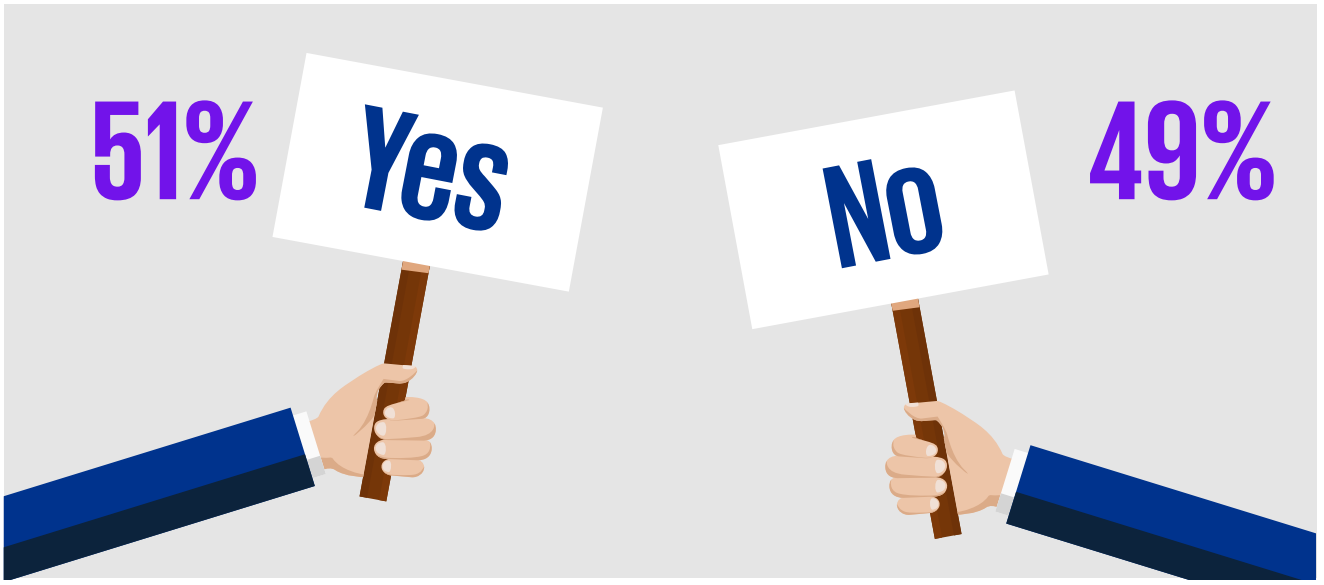


Figure 2: Cyber GCC leadership participation in global cyber security committees

1.4 Cyber GCCs focus across lines of defence

98 per cent of cyber GCCs in India follow Three Lines Of Defence (3LOD) approach to identify, manage and monitor cybersecurity risks effectively and efficiently. Additionally, cyber GCCs in each sector follow 3LOD model, which highlights that the approach is sector agnostic.

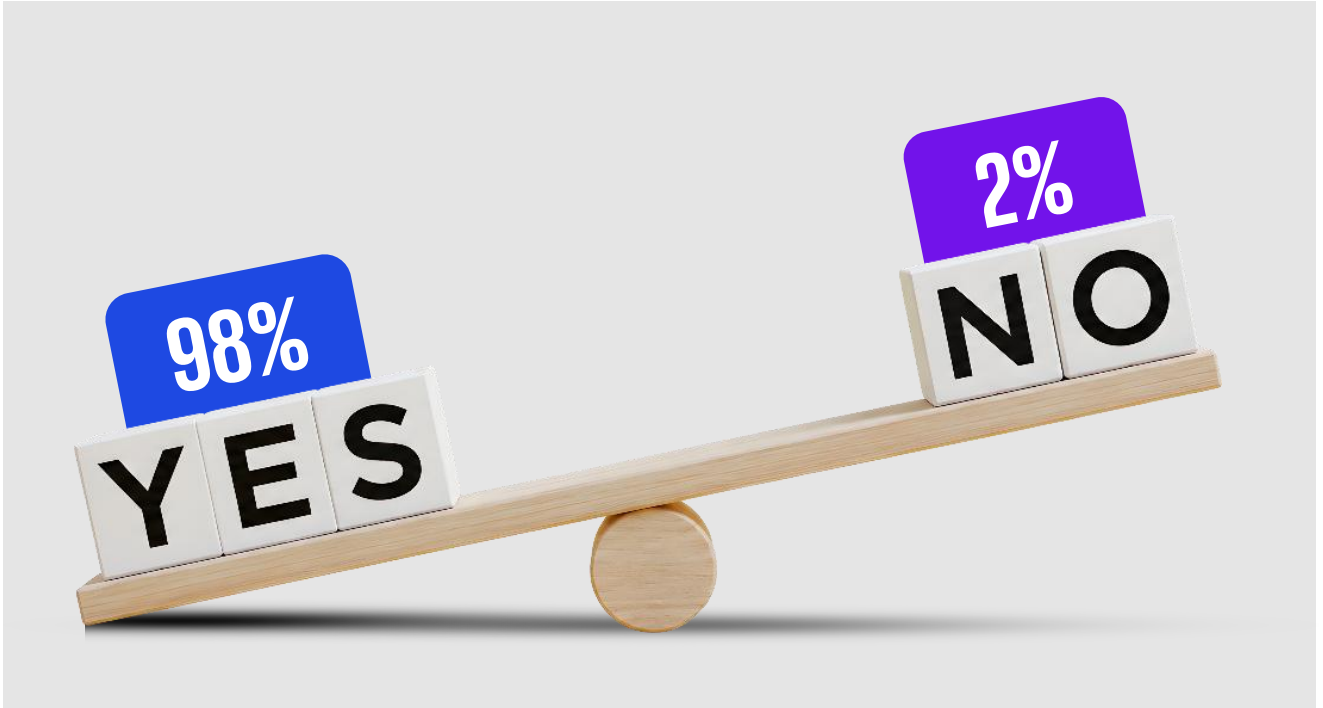


Figure 3: 3LOD model adoption by cyber GCCs

1.5 Cyber GCC activities across lines of defence

The top five cybersecurity activities undertaken across three lines of defence are:

Top five activities	LOD1	LOD2	LOD3
1	Implement and enforce cybersecurity policies, standards and governance frameworks	Assess cybersecurity processes, systems and operations	Conduct random/adhoc/on-demand cybersecurity audits
2	Measure control effectiveness and report findings	Coordinate with LOD1 and LOD3 for regulatory compliance, external audit readiness and any external activity impacting cybersecurity functions	Provide independent oversight/observation on cybersecurity activities, as required by the board, committees, leadership etc.
3	Define and implement risk and control management framework and approach	Perform thematic reviews and provide findings and recommendations	Execute cybersecurity audits, per defined plan
4	Assess, report and mitigate control gaps	Identify and report cybersecurity systemic risks and issues with cybersecurity functions	Report appropriate cybersecurity audit findings to the board, committees, leadership and management
5	Plan and implement resilience functions (BCP, DR, enterprise resilience, operational resilience etc.)	Develop cybersecurity policies, standards and governance frameworks	Register cybersecurity audit observations and findings and provide recommendations

Table 1: Top five 3LOD activities in Cyber GCCs

Cyber GCC case studies 1

Cybersecurity audits in LOD3: A leading financial services GCC has a robust technology aUdit programme delivering global risk-based cybersecurity internal audits, providing integrated assurance over technology environments supporting critical financial services functions, including payments, asset and wealth management, global markets and compliance.

Audit scope covered cyber resilience, cloud security, privileged access, security operations, technology governance, and enterprise risk management, alongside AI governance and end-to-end AI/ML lifecycle controls. This has strengthened oversight of technology and AI risks, enhanced governance of emerging AI capabilities, and increased confidence in the security, resilience, and integrity of business-critical platforms.

1.6 Cybersecurity talent continues to be the top driver for cyber GCC model

Availability of cybersecurity resources has been a top driver for leveraging the GCC model, followed by uninterrupted service delivery and continuous innovation and agility.

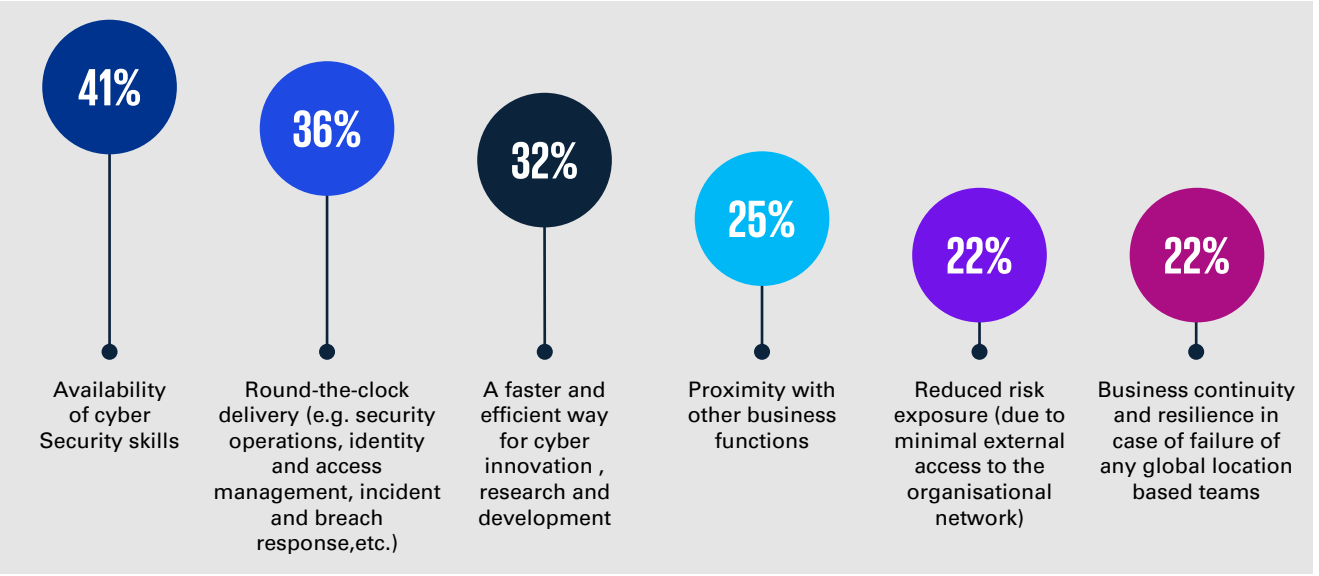


Figure 4: Key drivers to leverage cyber GCC model

1.7 Core cybersecurity functions continue to register significant growth

As more GCCs are setup and existing ones continue to grow, cyber GCCs continue to setup and expand various cybersecurity functions. Most of the functions reported in 2023 edition continued to grow, while AI security, OT security, quantum security etc. have been setup in the last few years.

Figure 5: Top ten 'core' cybersecurity functions delivered from cyber GCCs

Cyber GCC case studies 2

Technology risk management : A leading investment banking GCC manages the end-to-end technology controls management lifecycle, driving global control programmes and strategic initiatives across risk and controls transformation. This includes modernising Risk and Control Self Assessment (RCSA) frameworks through technology-enabled solutions, establishing monitoring and testing programmes for cybersecurity controls across business units, and leading large-scale cybersecurity issue management and remediation initiatives. These efforts enhanced control effectiveness, enabled real-time risk visibility, strengthened regulatory compliance, and improved the organisation's ability to proactively identify, monitor, and mitigate technology and cybersecurity risks across the enterprise.

1.8 Top five cybersecurity functions based on budget allocation

2023	2026
Cybersecurity strategy and technology regulatory audit and standards compliance management	**Cybersecurity strategy**
Third party risk management	**Cybersecurity operations**
Cybersecurity engineering, product management and automation	**Cloud security**
Application security and vulnerability management	**Identity and access management**
Secure development	**AI security**

Table 2: Budget allocation comparison between 2023 and 2026

Over and above the top five cybersecurity functions, cybersecurity governance, cybersecurity risk assessments, cyber resilience, emerging technology risk, data privacy, threat management, data governance, digital security, cyber fusion centre and insider risk management are also considered key from a budget perspective.

1.9 Catalyst of cyber GCC growth

Global organisations continue to experience intense and ever-expanding cybersecurity attacks, which is resulting in expansive cybersecurity functions with limited or minimal increase in cybersecurity budgets. Cyber GCCs have become an important part of the cybersecurity strategy for their global organisations, as they deliver significant value. Apart from these, cyber GCCs are also focusing on cost arbitrage, competency and agility of the teams in India.

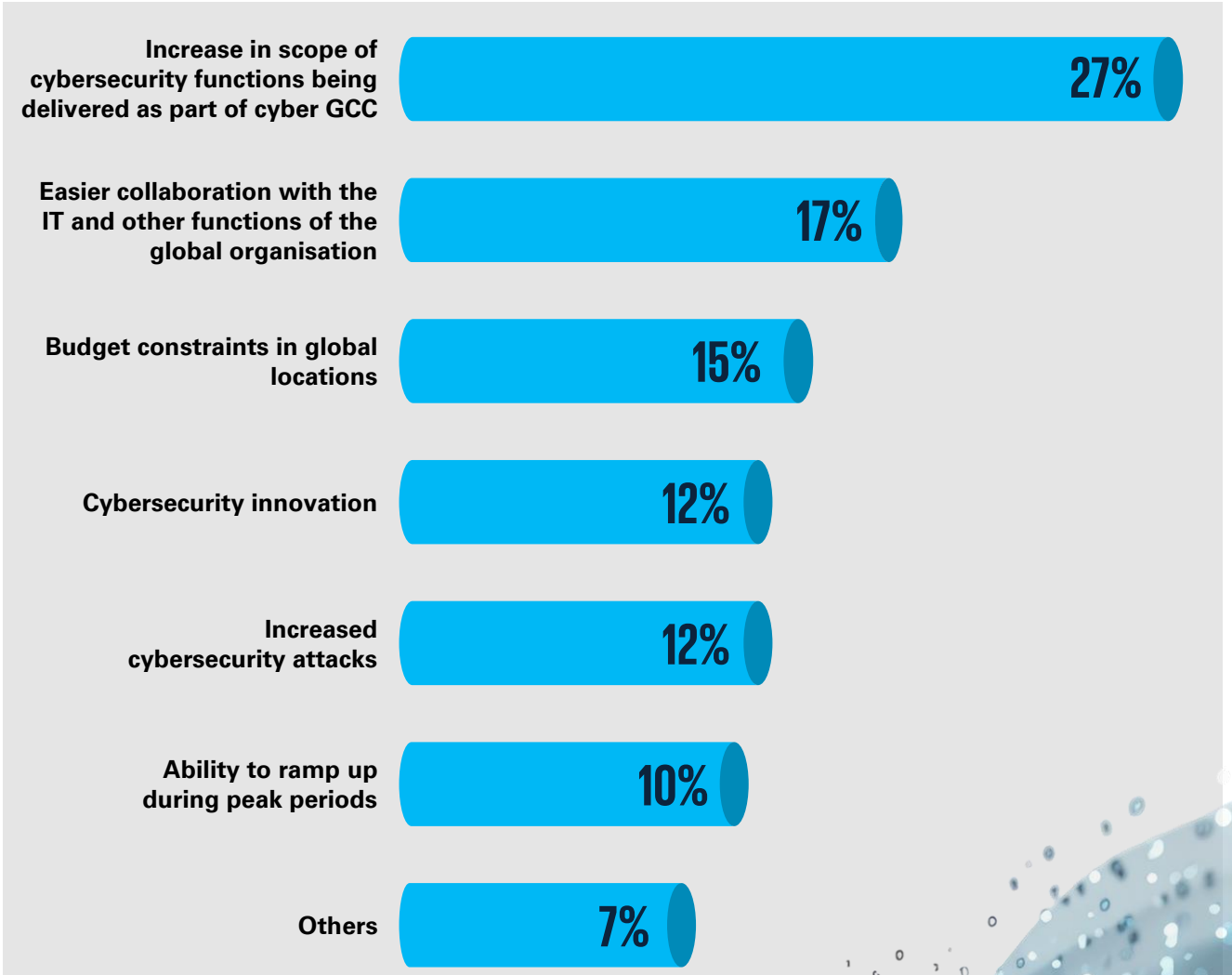


Figure 6: Cyber GCC growth factors

Cyber GCC case studies 3

AI powered vulnerability management: A leading global financial services organisation leveraged its cyber GCC to improve the prioritisation and remediation of security vulnerabilities across a complex technology estate. Cyber GCC supported the programme through AI-enabled remediation and decision support, using technology and business context to help identify the vulnerabilities requiring priority action. The engagement strengthened the transition from severity-based processing to a more risk-led remediation model. The resultant impact was improved focus of remediation teams, greater consistency in vulnerability treatment and a scalable operating model capable of supporting a large enterprise environment.

1.10 Cyber GCC strategies to deliver value

Global organisations are leveraging cyber GCCs to realise significant value, through various fit-for-purpose strategies including significant share of cybersecurity function delivery from the cyber GCCs, process re-engineering and automation for optimisation of cybersecurity functions and governance of outsourcing of specific cybersecurity functions etc.

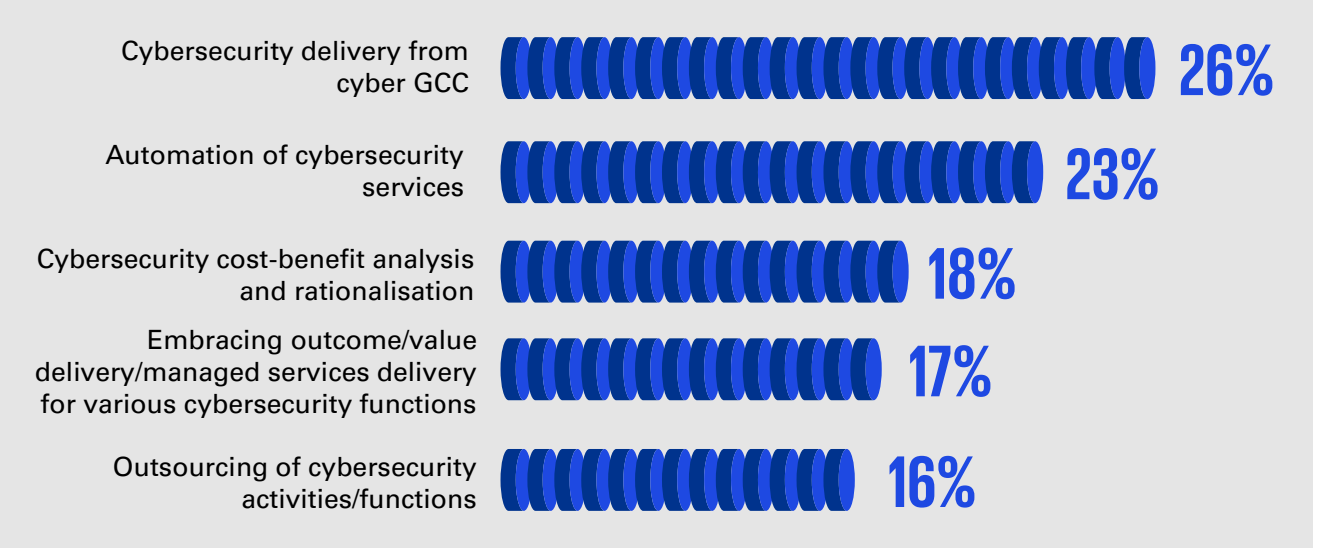


Figure 7: Cyber GCC value delivery strategies

> ***GCCs are moving towards strategic trust building with their global organisations and the wider business ecosystem, beyond operational trust. Cyber GCCs are making this happen***
>
> ***- Devinder Singh, Global Head Cyber Governance & Risk Tower at Carrier***

4 Cyber GCC case studies

Compromise assessment and threat hunting : A leading global technology services GCC performed a comprehensive threat hunting and compromise assessment across their customer-managed enterprise environment. The assessment analysed telemetry from SIEM, XDR and EDR platforms to identify indicators of compromise, suspicious endpoint activity, anomalous authentication patterns and potential misuse of privileged access. The assessment provided independent assurance over the environment's security posture, strengthened visibility of potential threats that may have bypassed routine monitoring and identified opportunities to improve detection, monitoring and incident response readiness.

1.11 Cyber GCC collaboration with the ecosystem

Cyber GCCs are increasingly engaging with a broader ecosystem, which includes start-ups, academia, government bodies, PSUs, law enforcement agencies, think tanks, and industry associations. This collaboration is not just symbolic—it's strategic. By tapping into the agility of start-ups, the research depth of academia, and the regulatory guidance of government entities, cyber GCCs are building more adaptive and resilient cybersecurity functions.

Figure 8: Percentage of cyber GCCs collaborating with ecosystem

1.12 Cyber GCC DPDPA* compliance

DPDPA applies to all GCCs in India and cyber GCC leaders are helping their organisations to comply with it. Cyber GCCs have been managing their global privacy function and are now leveraging their global privacy experience and expertise in complying with DPDPA. Key activities for DPDPA compliance being delivered are shown below:

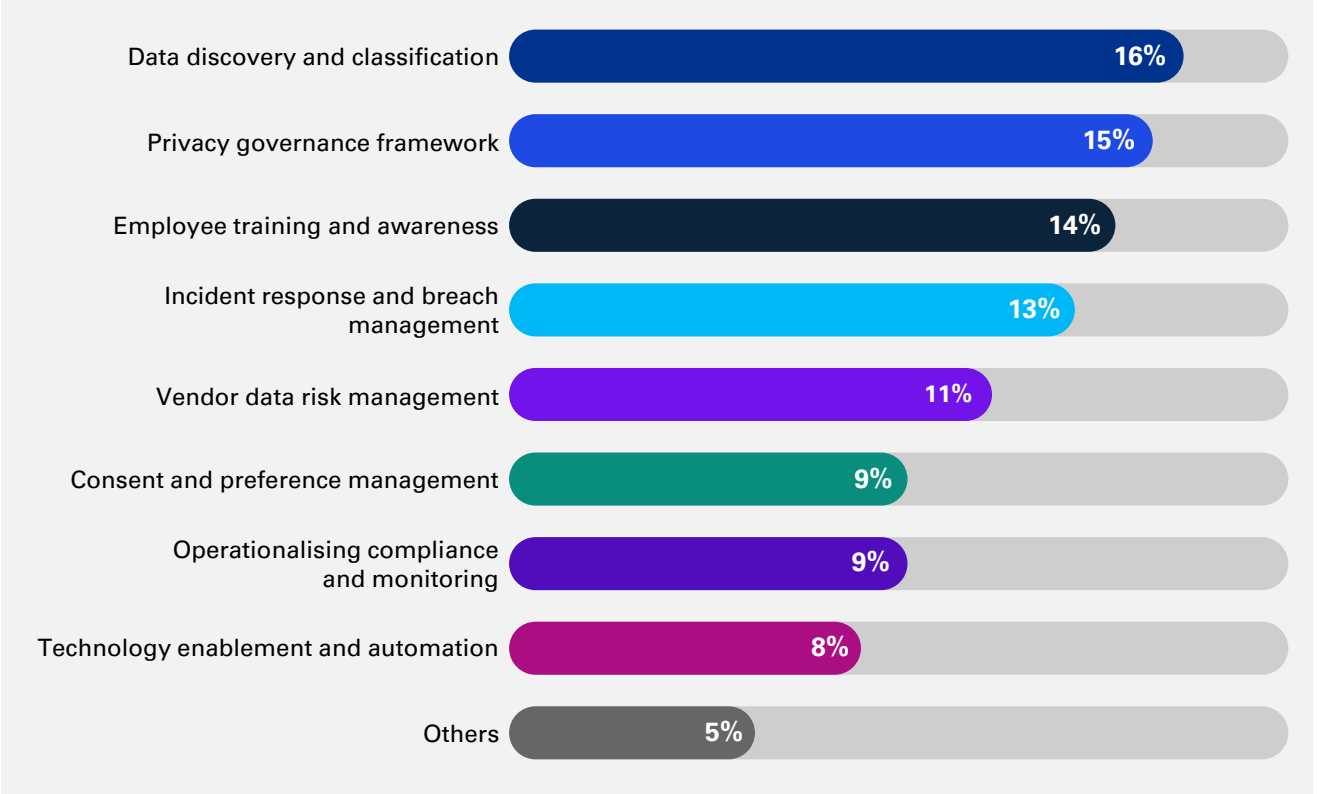


Figure 9: Cyber GCC activities for DPDPA compliance

* Digital Personal Data Protection Act, 2023 (DPDPA)

2

Cybersecurity talent

2.1 AI security is the top priority skillset for cyber GCCs

AI security, cyber resilience, data privacy, data security and data protection, and application security and vulnerability management have registered the highest growth since 2023. Cybersecurity skills demand in cyber GCCs continue to register a significant rise. AI security skillset is being sharpened with religious focus and continuous learning and development.

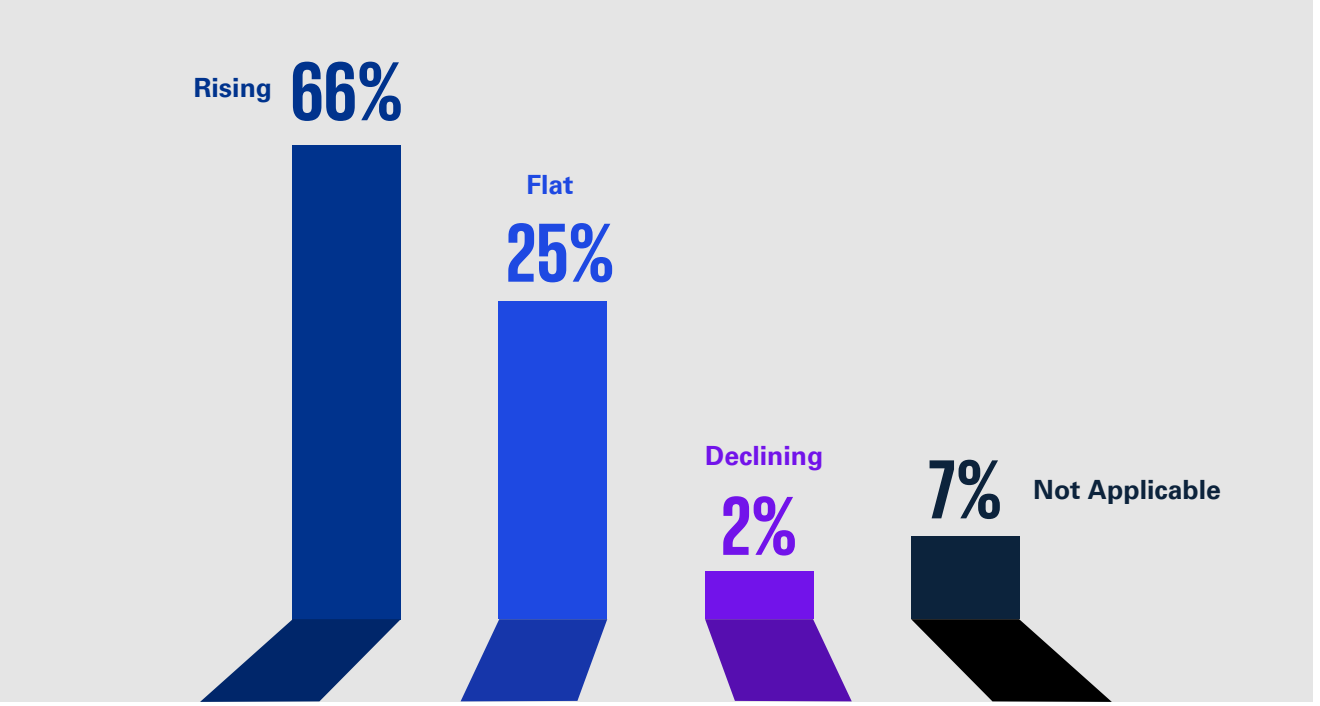


Figure 10: Cybersecurity skill demand compared to 2023

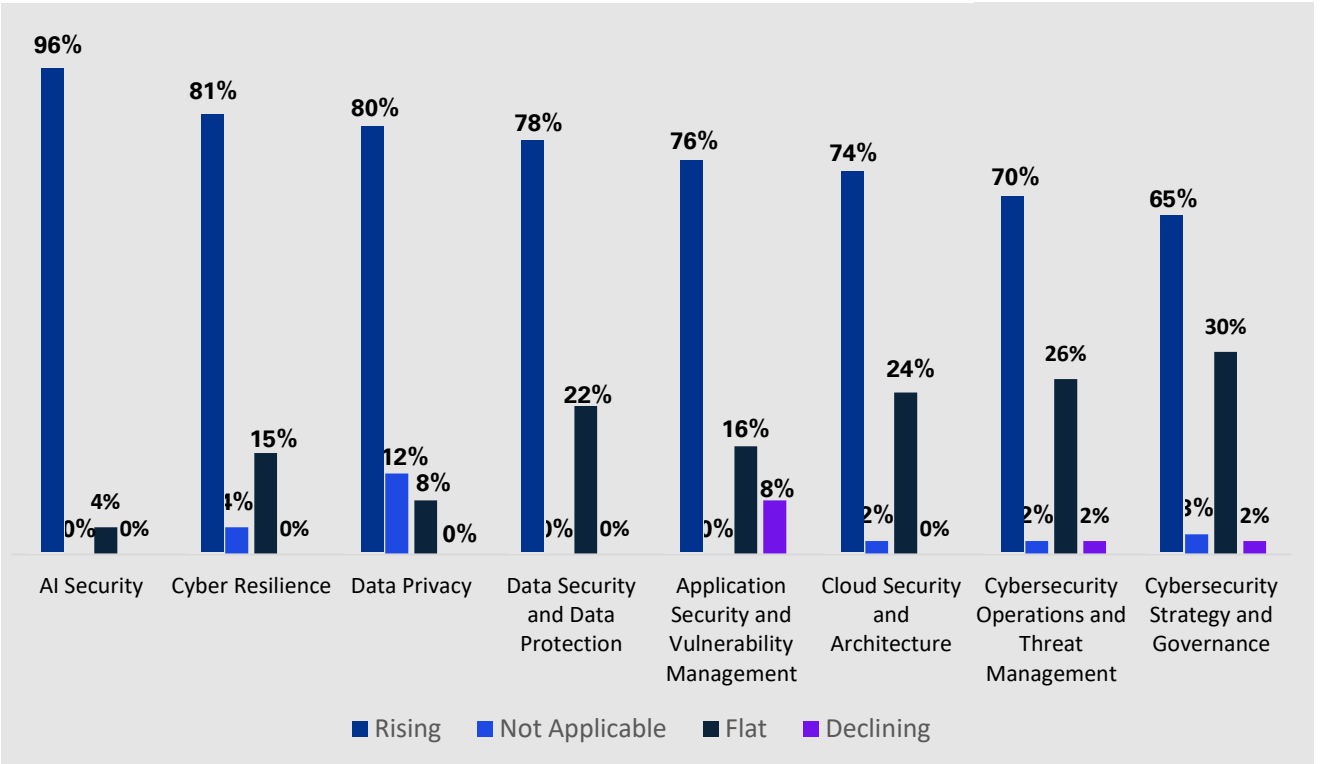


Figure 11: Cybersecurity skill wise demand compared to 2023

Cyber GCCs have preferred external hiring and in-house training to scale-up cybersecurity skills in demand.

Top five cybersecurity functions that hire externally and/or train resources in-house respectively are:

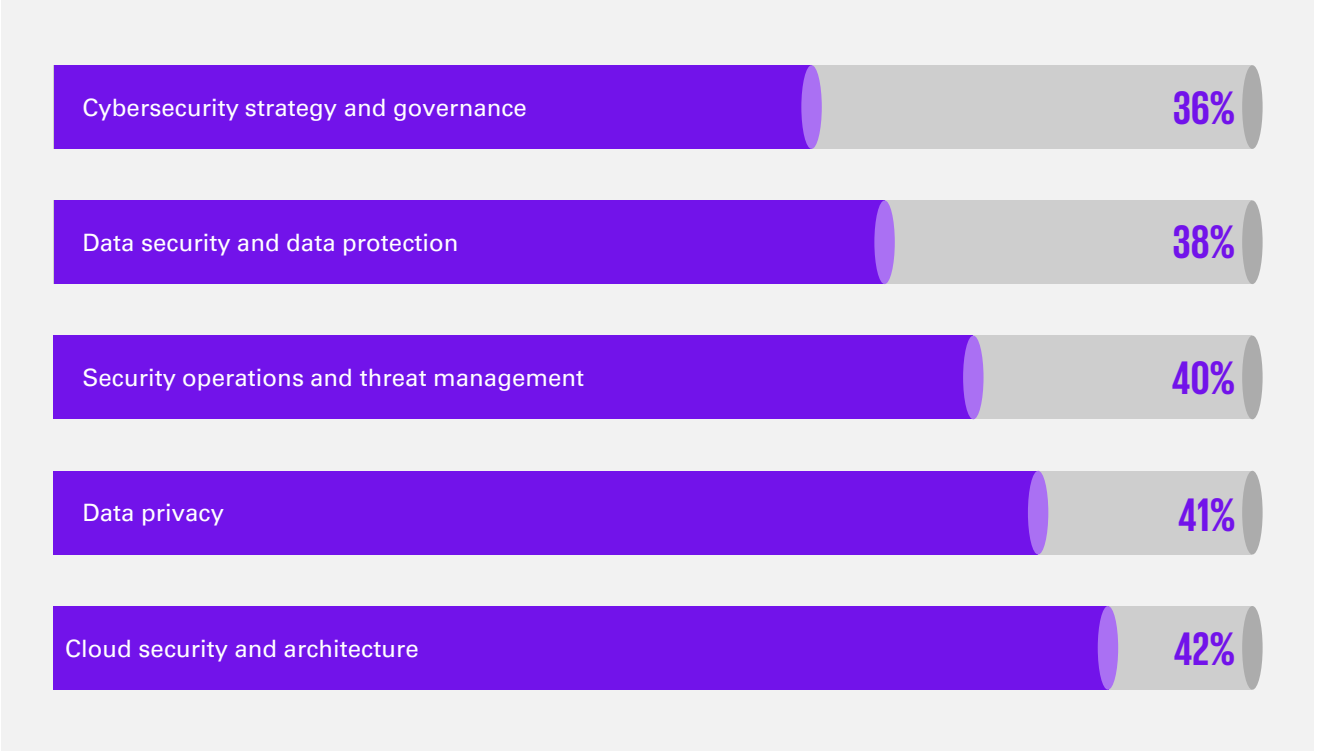


Figure 12: Cybersecurity functions with external hire

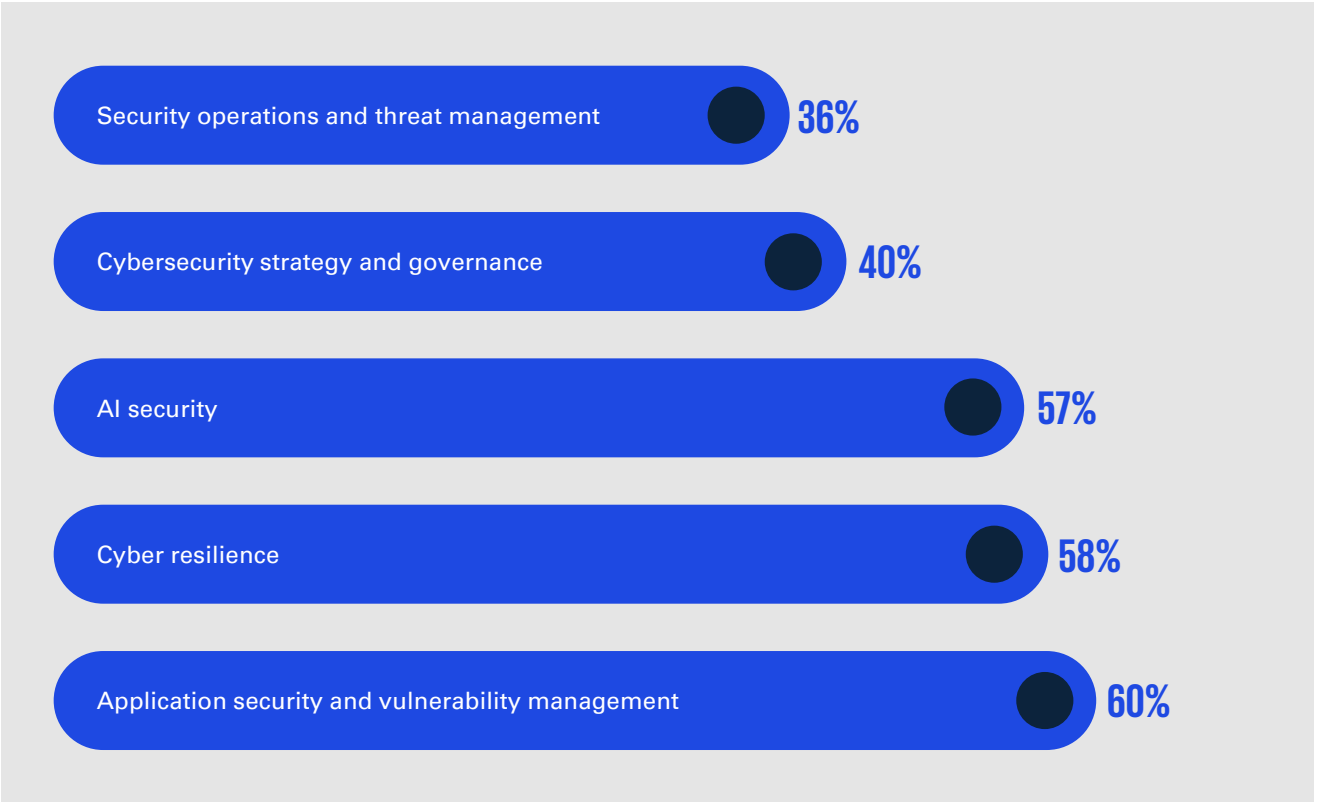


Figure 13: Cybersecurity functions with in-house training

2.2 Cyber GCC talent upskilling practices

When compared to the previous editions, Gen AI/AI powered training and awareness programmes, active participation in industry forums, collaborative learning sessions within different cybersecurity functions and knowledge base/online portals are the most popular means to upskill in 2026.

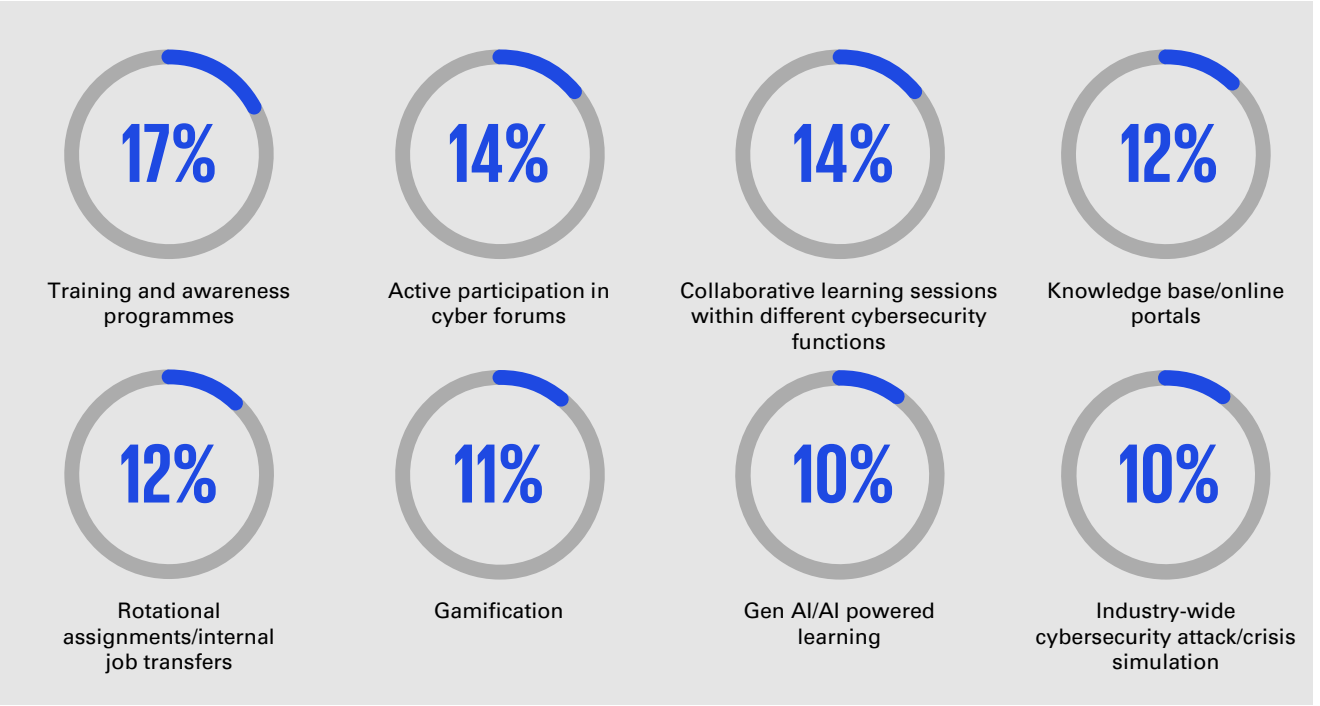


Figure 14: Cyber GCCs practices for upskilling/cross-skilling of cybersecurity teams

2.3 Cyber GCC attrition has declined

Annual attrition rate of cyber GCCs has reduced significantly. About 57 per cent of cyber GCCs have registered less than or equal to 7 per cent, while only 11 per cent of cyber GCCs have registered more than or equal to 16 per cent attrition.

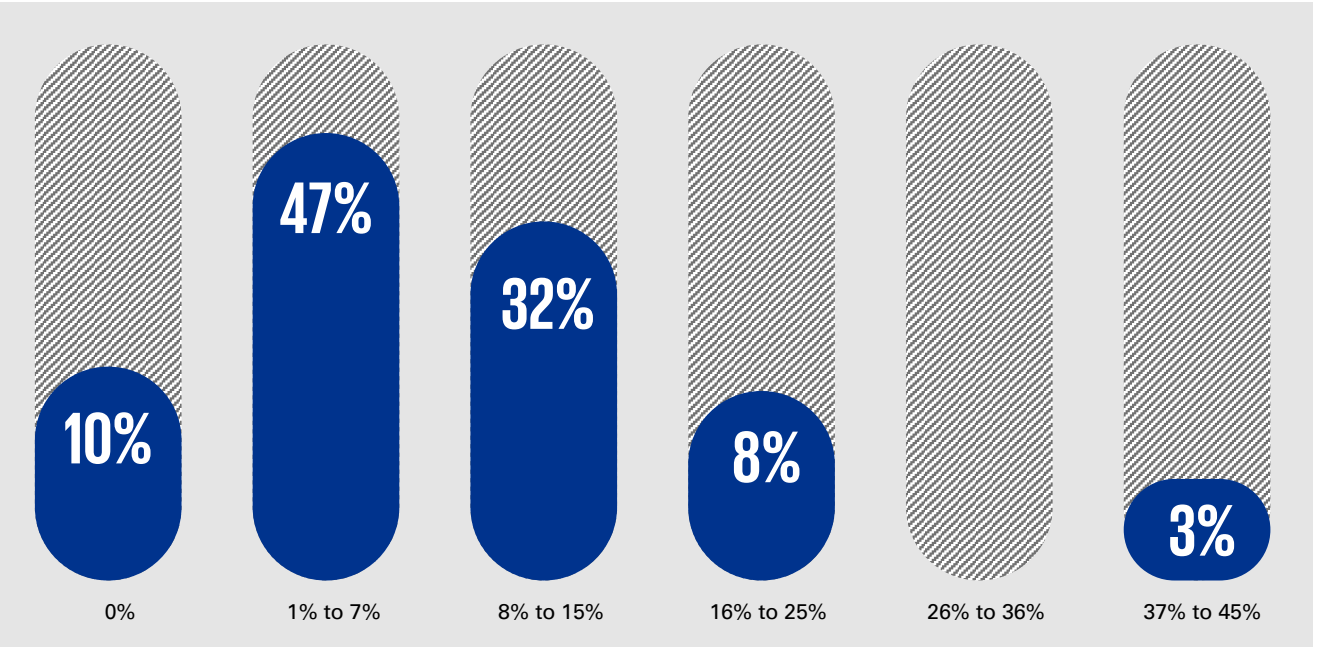


Figure 15: Annual attrition rate of cyber GCCs

2.4 Key cybersecurity talent management challenges

Attracting and retaining top cybersecurity talent in cyber GCCs requires a strategic and multifaceted approach. Cyber GCCs continued to face various challenges in attracting and retaining cybersecurity talent.

Cyber GCCs have identified ‘compensation and rewards', 'market demand for similar skills' and 'location preferences' as the key challenges in cybersecurity talent management.

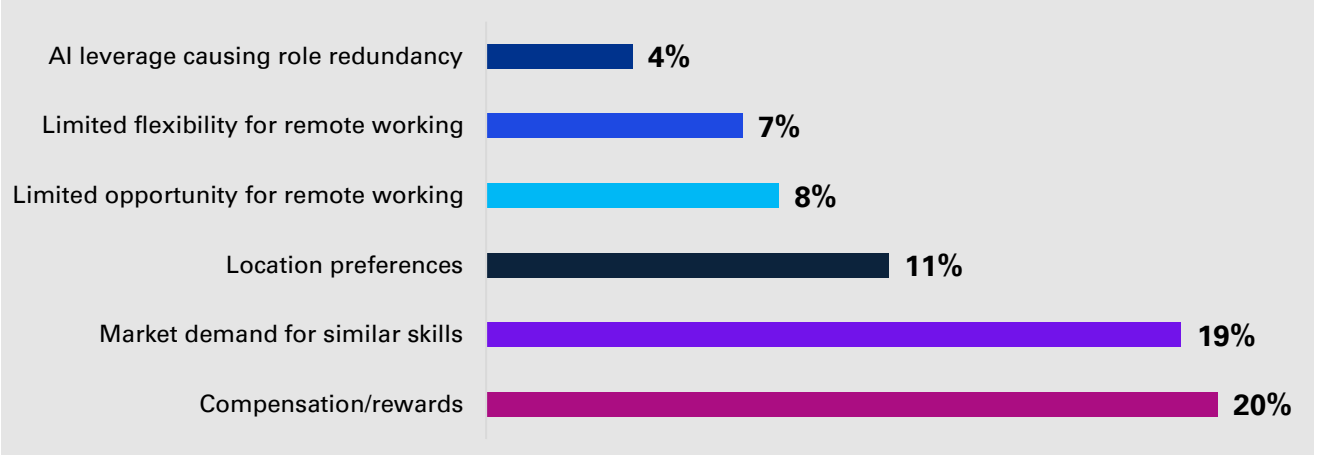


Figure 16: Top cyber GCC challenges for attracting and retaining cybersecurity talent

2.5 Key practices for nurturing fresh cybersecurity talent in cyber GCCs

Cyber GCCs are adopting a structured and multi-layered approach to onboard and integrate fresh talent, reflecting the growing need to build a sustainable cybersecurity talent pipeline at scale. The approach combines early exposure, formal training, and continuous skill development, enabling freshers to transition effectively into complex cybersecurity roles. Cyber GCCs believe in providing practical experience helping to upskill and integrate freshers.

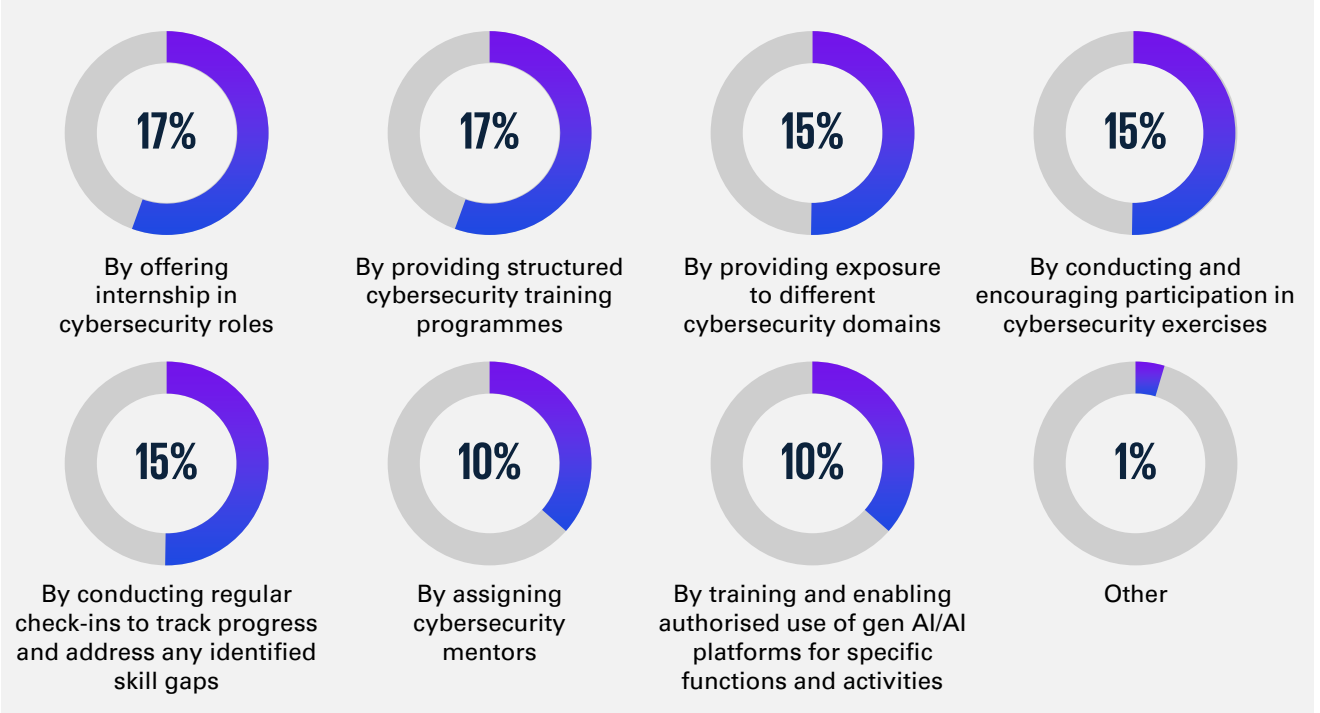


Figure 17: Preferred practices for freshers training and integration in cyber GCCs

Cyber GCC case studies 5

Security and compliance centre of excellence and analyst program: A leading energy sector GCC established a security and compliance Centre of Excellence (CoE), with fresher analyst talent, to govern a large risk and compliance function delivering over 3,000 annual security risk assessments. The CoE established and streamlined governance through KPI/KRI reporting, management dashboards, process standardisation, quality reviews, structured analyst training, and regular stakeholder governance forums. These efforts reduced resource allocation turnaround time from six weeks to two weeks, decreased Service Level Agreement(SLA) breaches by 70 per cent, improved first-time-right delivery by 60 per cent, strengthened audit readiness, and enhanced stakeholder experience through continuous monitoring and feedback-driven improvements.

2.6 Technology led cybersecurity delivery maturity in cyber GCCs

AI, cloud, advanced analytics, automation have been significantly utilised in delivering cybersecurity in an efficient and effective manner by various cyber GCCs. Technology quotient in cyber GCCs has seen a significant uptick since 2023, with AI leading the pack.

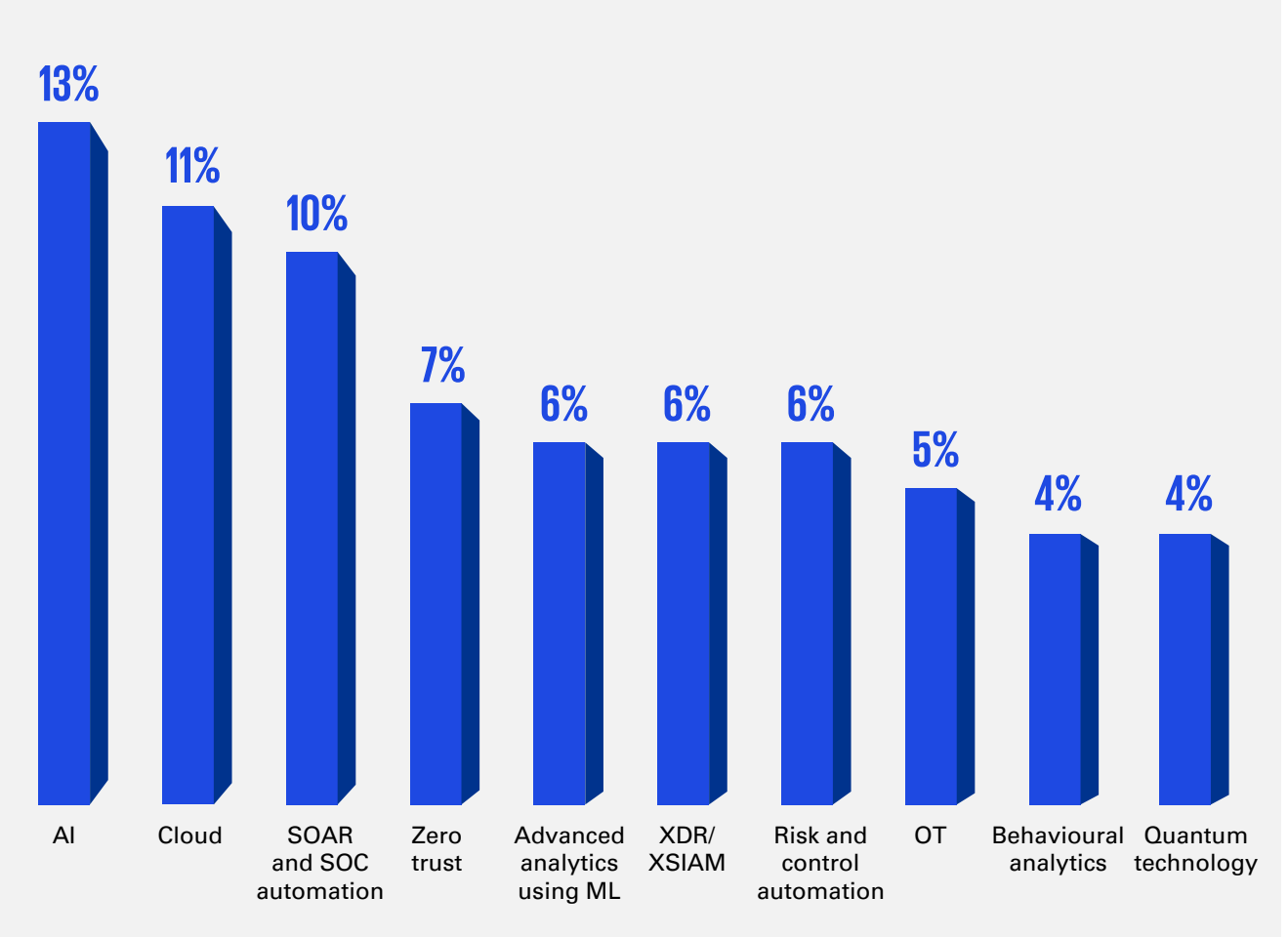


Figure 18: Technology led cybersecurity use cases

2.7 Key risk culture initiatives in cyber GCCs

Cyber GCCs emulate global organisations, following defence-in-depth approach, implement various initiatives to embed and sustain risk culture. AI powered cybersecurity learning and assistance has become one of the widely adopted risk culture initiatives.

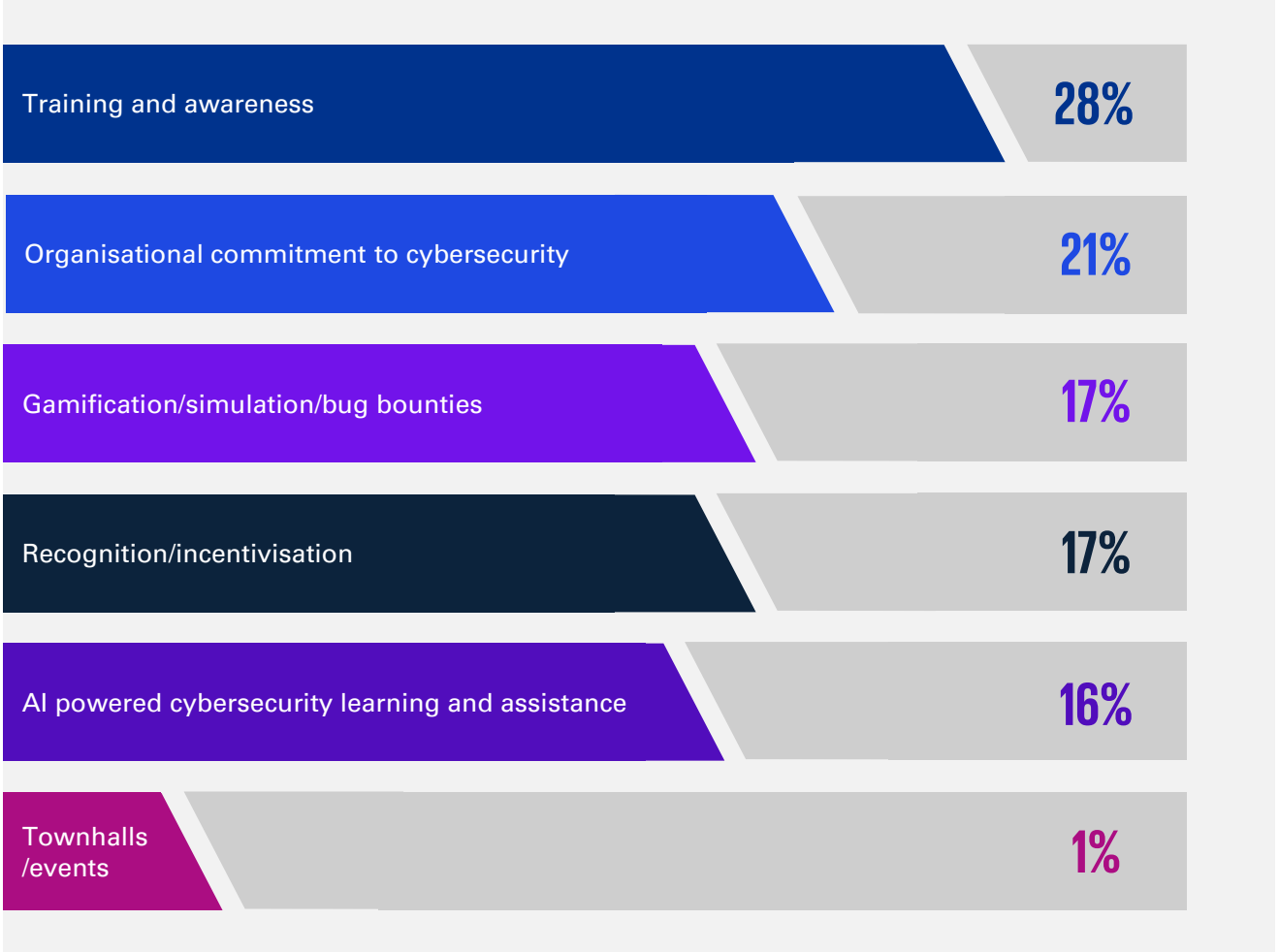


Figure 19: Risk culture initiatives

> ***As AI reshapes the cyber threat landscape, effective leadership in the GCC lies in using innovation to turn cybersecurity into a source of trust, resilience, and measurable value for customers and shareholders***
>
> ***- Rahul Goel, Chief Data Office Risk COE and Tech CCO India COE lead, Commonwealth Bank of Australia***


AI

3

AI and cybersecurity

Global Capability Centres (GCCs) in India are playing a vital role in enabling their global organisations to adopt AI across various business and enterprise functions. At the same time, AI adoption is introducing new attack surface, including AI model powered adversarial threats, shadow AI, third party AI risk, and AI regulatory compliance challenges.

Recent frontier and earlier AI models have surfaced cybersecurity as the top risk across governments, businesses, regulators and consumers. AI has made cybersecurity an existential business issue.

Global organisations and their cyber GCC leadership have received significant sponsorship in AI investments, global board appointed high-powered committee involvement and business and technology executive drive and prioritisation of AI security and AI for security functions.

Cyber GCCs are at the forefront of securing AI adoption while leveraging AI for strengthening cybersecurity, in terms of effectiveness and efficiency. Security of AI and AI for security are rapidly evolving cybersecurity functions across cyber GCCs, working with the ecosystem of global platforms and products and niche providers and continuously innovating and adapting to the fast-paced developments in AI and cybersecurity.

3.1 AI as a force multiplier for cybersecurity

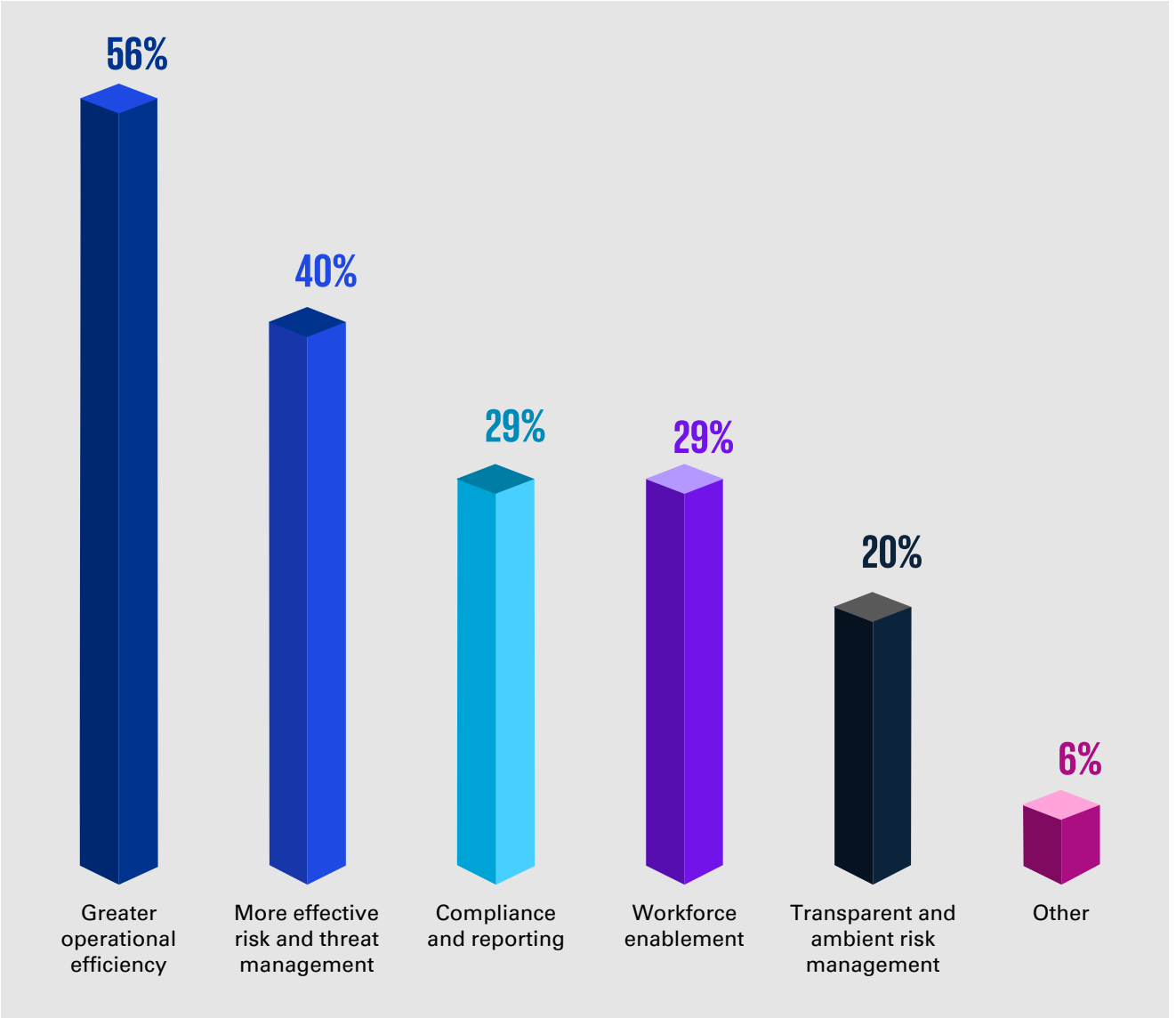


Figure 20: How AI adoption has benefitted cyber GCCs

AI adoption is significantly helping in more effective and efficient cybersecurity and digital risk management. A significant number of cyber GCCs have experienced about 10-40 per cent operational efficiencies in various cybersecurity activities, using AI. Also, across various cybersecurity functions, AI powered use cases for more effective vulnerability, threat, risk, control and security awareness management have been developed and implemented by various cyber GCCs.

AI quotient, AI skills and AI investments have been tapped into by cyber GCCs, in a strategic shift to use AI and other technologies to deal with AI powered cybersecurity risks and threats.

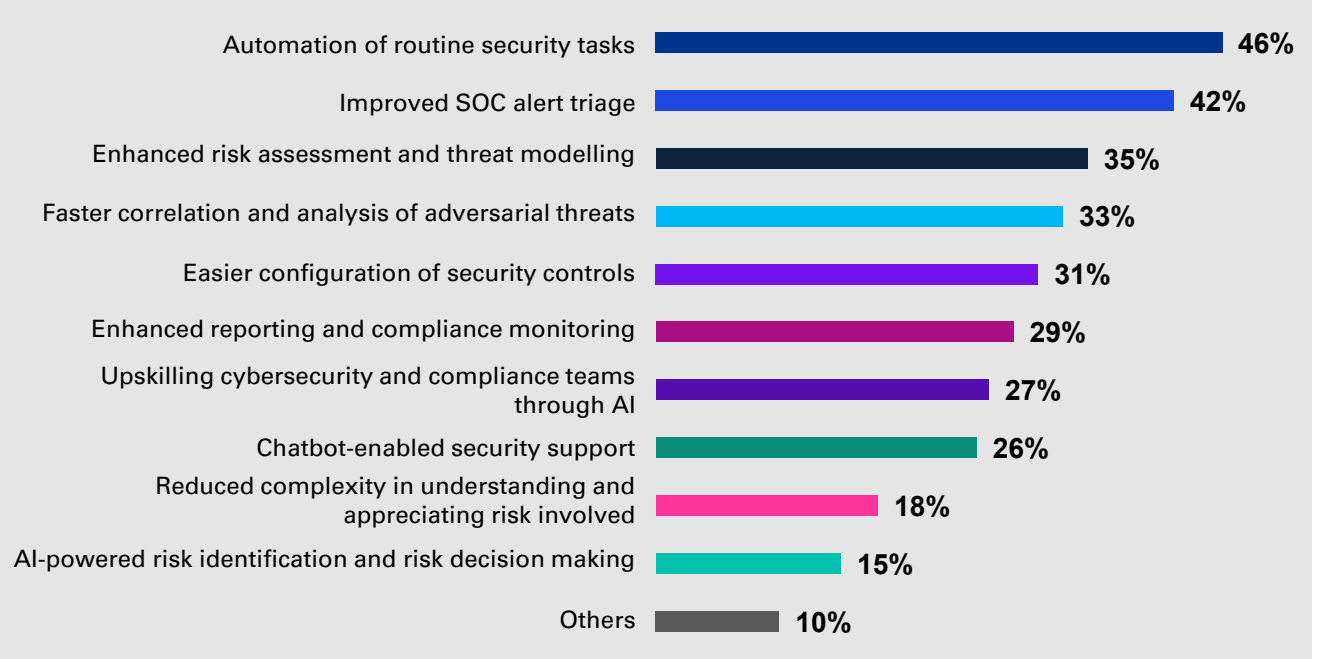


Figure 21: Cybersecurity activities, where AI adoption has most benefitted organisations

6 Cyber GCC case studies

AI led red teaming platform : A mature cyber GCC developed, an AI-powered command and control accelerator that enhances red team operations through automated attack path generation, command optimisation, malware signature analysis, troubleshooting assistance, and continuous learning. By combining generative AI, locally trained models, threat intelligence, and human expertise, the platform enabled faster and more effective adversarial simulations, reduced analysis effort, improved repeatability of testing, and strengthened the overall quality of offensive security assessments. The platform provided AI-assisted support across reconnaissance, exploitation, post-exploitation, detection evasion, and knowledge management activities, helping their global organisation scale advanced red teaming capabilities and improved cyber resilience.

AI-enabled application security testing: A leading GCC transformed its global application security programme by implementing an AI-powered testing framework that combines threat intelligence, attack surface management, AI-driven test case generation, automated vulnerability assessment, and human-led validation. The solution leveraged specialised AI agents to identify application context, executed security testing, prioritised risks, and generated detailed remediation guidance across web applications, APIs, and digital platforms. This resulted in improved testing coverage, reduced manual effort, accelerated vulnerability identification and remediation, and enhanced security governance through continuous monitoring, risk-based prioritisation, and executive reporting.

> *For GCCs Scaling AI adoption, robust AI security is no longer just a safeguard - it is a core business differentiator.*
>
> *- Shalini Pillay*
> *India Leader – Global Capability Centers, KPMG in India*

3.2 AI security challenges

As cyber GCCs scale AI, they are encountering an intense and fast paced set of security challenges, requiring iterative, continuous and targeted approaches to deal with the same.

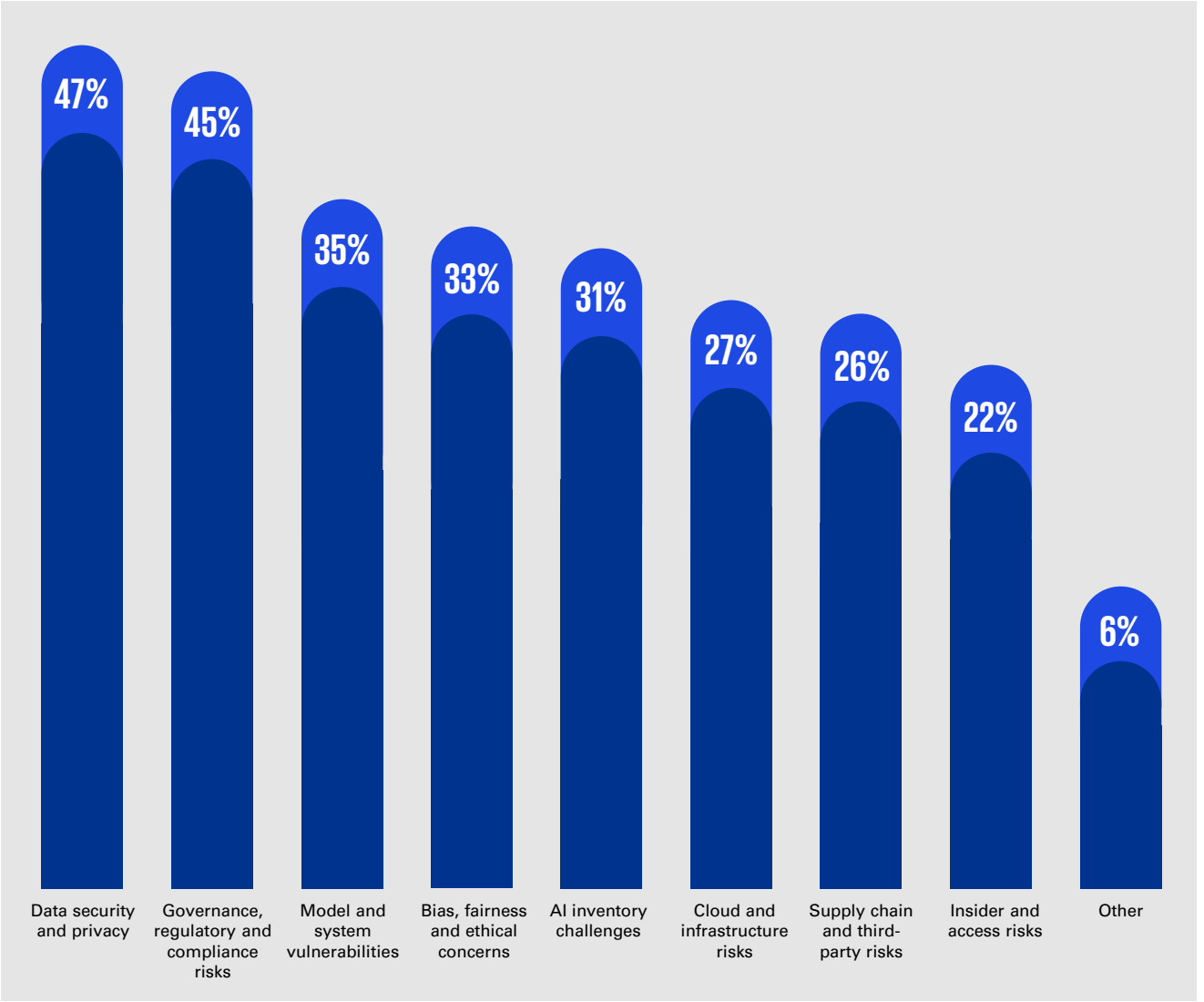


Figure 22: Key AI security challenges

AI inventory challenges (31 per cent) point to a foundational gap in secure AI adoption: limited visibility into the AI systems, models, datasets and dependencies being developed, deployed or consumed across the enterprise.

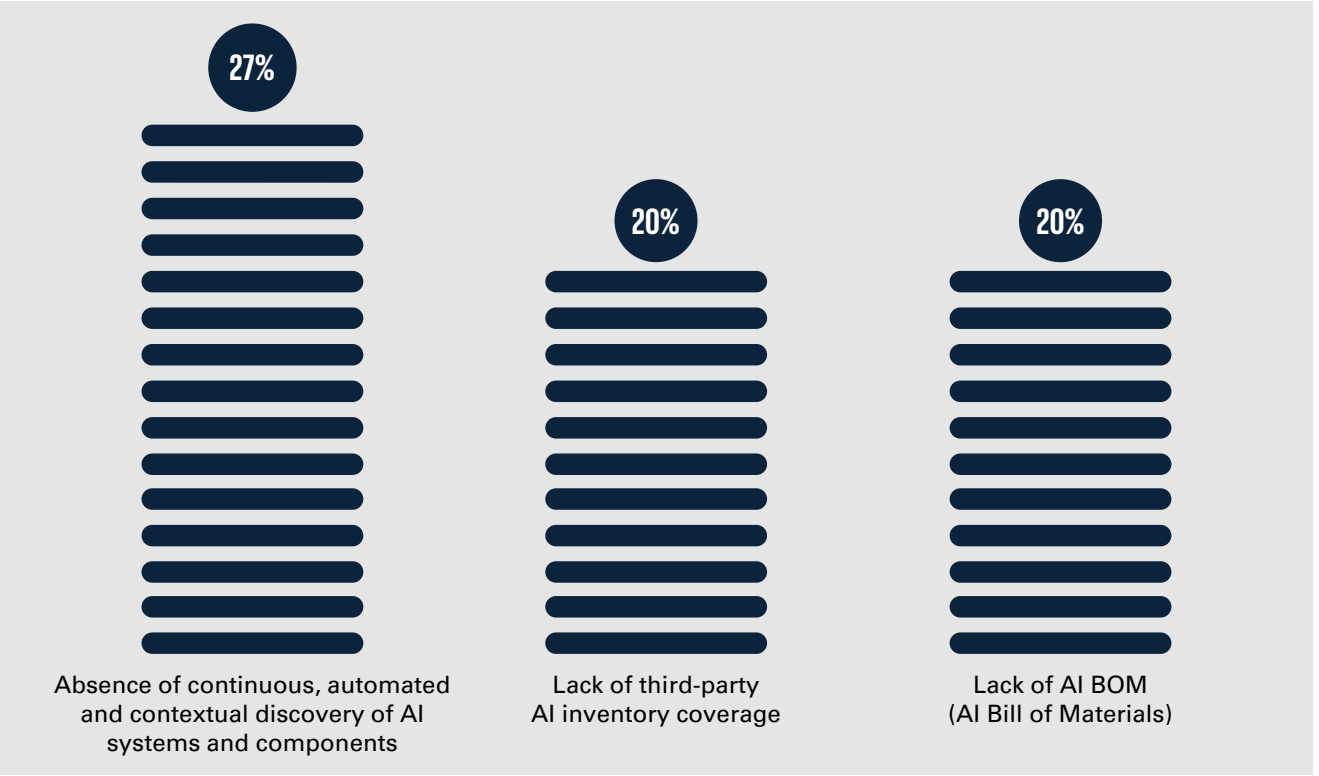


Figure 23: AI inventory challenges

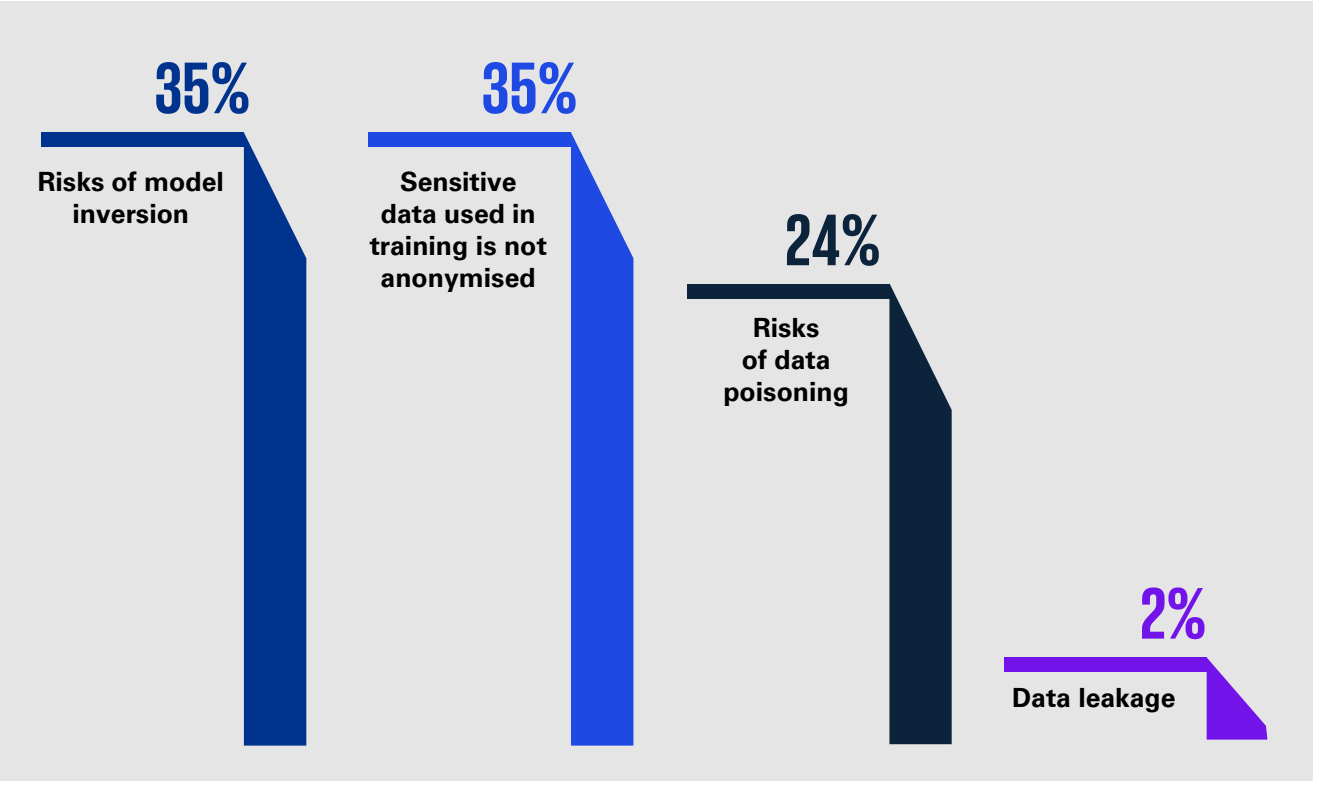


Figure 24: Data security and privacy challenges in AI adoption

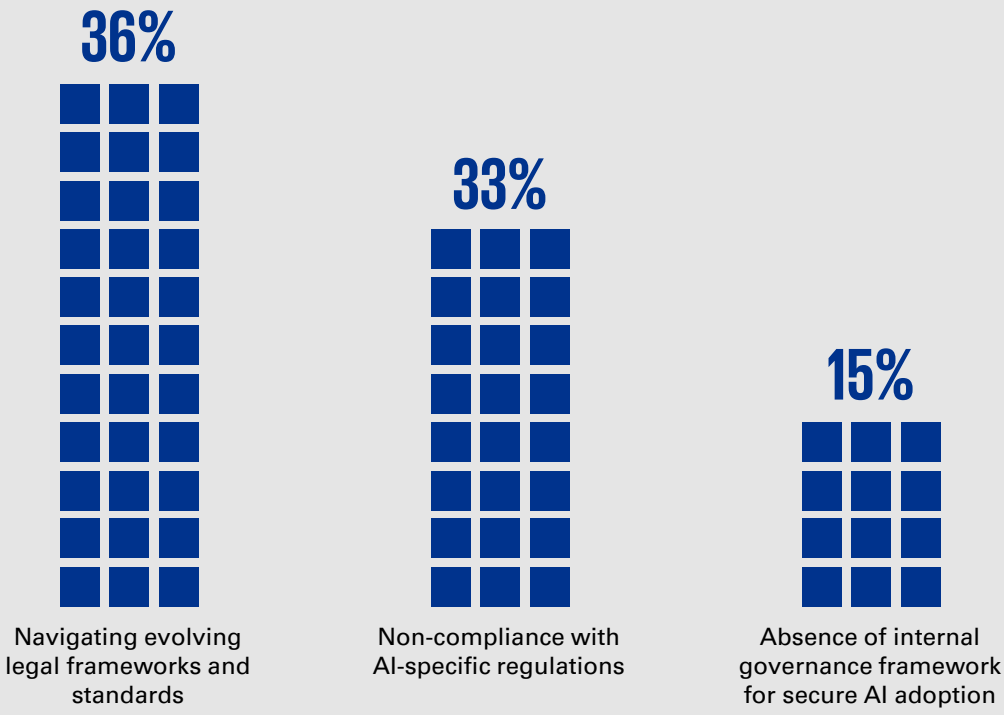


Figure 25: Governance, regulatory, compliance risks in AI adoption

Cyber GCC case studies 7

Red teaming and Penetration Testing (PT) of AI : A leading cyber GCC has set up a focused red teaming activity to identify compromise of AI-enabled recruitment through indirect prompt injection. An AI-powered voice interview platform was assessed to determine whether untrusted resume content could influence the interview process. The assessment identified that hidden instructions embedded within a candidate's resume were incorporated into the AI agent's context without adequate sanitisation or separation from trusted system instructions.

Consequently, the AI interviewer altered the intended workflow, skipped mandatory technical questions and advanced the candidate. The case demonstrated risks relating to recruitment workflow bypass, manipulation of AI-driven decisions, loss of interview integrity and potential progression of unsuitable candidates.

Unauthorised modification of AI agents and tools: An agentic AI platform was assessed from the perspective of a low-privileged, authenticated user. The red team identified weaknesses in API-level access controls that enabled modification of tools and system prompts belonging to another workspace or user.

The altered system prompt subsequently caused the AI agent to invoke a modified tool, resulting in execution of unauthorised commands within the host environment and disclosure of command output. The case highlighted how inadequate authorisation, workspace isolation and tool-execution controls could enable cross-user compromise and broader server-level impact..

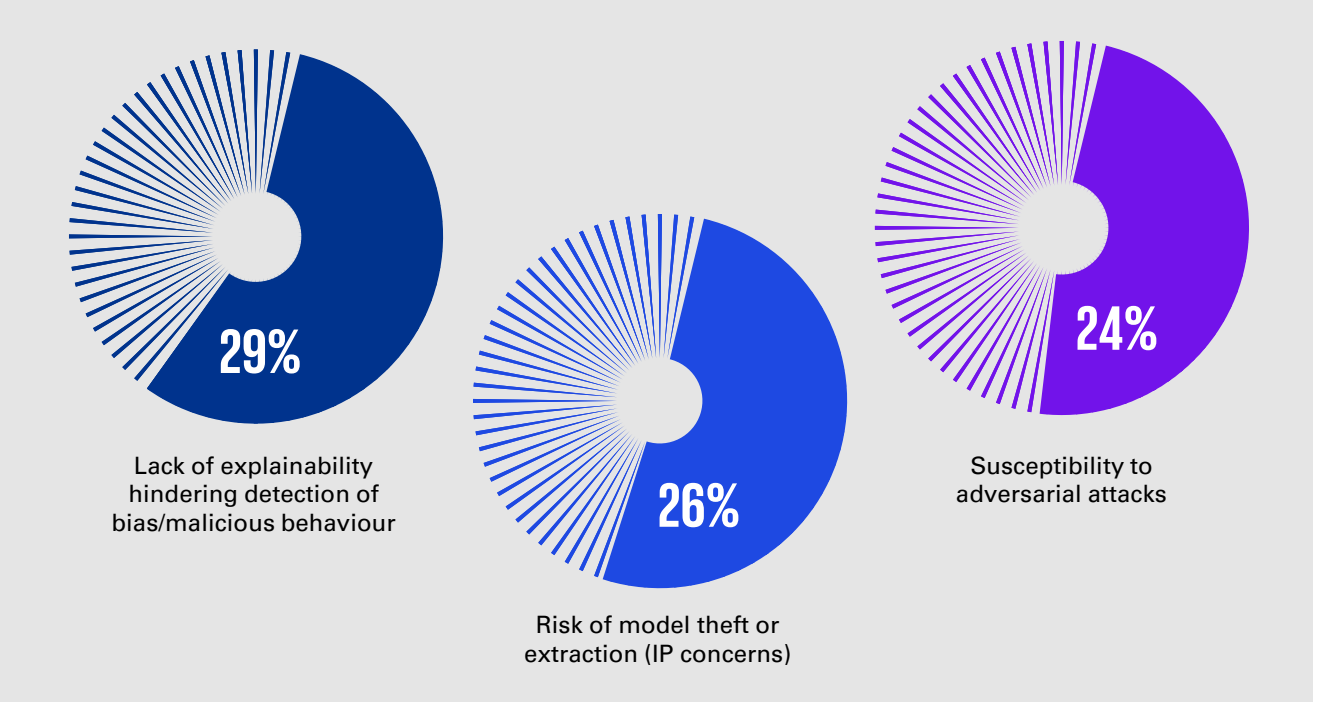


Figure 26: AI model and system vulnerabilities

3.3 Third party AI risks

Software supply chain security and third-party AI risks (25 per cent) reflect the extent to which AI adoption depends on external libraries, pre-trained models, platforms and service providers. The main concerns are:

- **Risks from third-party AI tools or services (23 per cent)**
  These relate to the security, transparency and control maturity of externally provided AI solutions.
- **Malicious code/backdoors in open-source libraries or pre-trained models (18 per cent)**
  Open-source components and pre-trained assets may introduce hidden vulnerabilities or unverified dependencies.

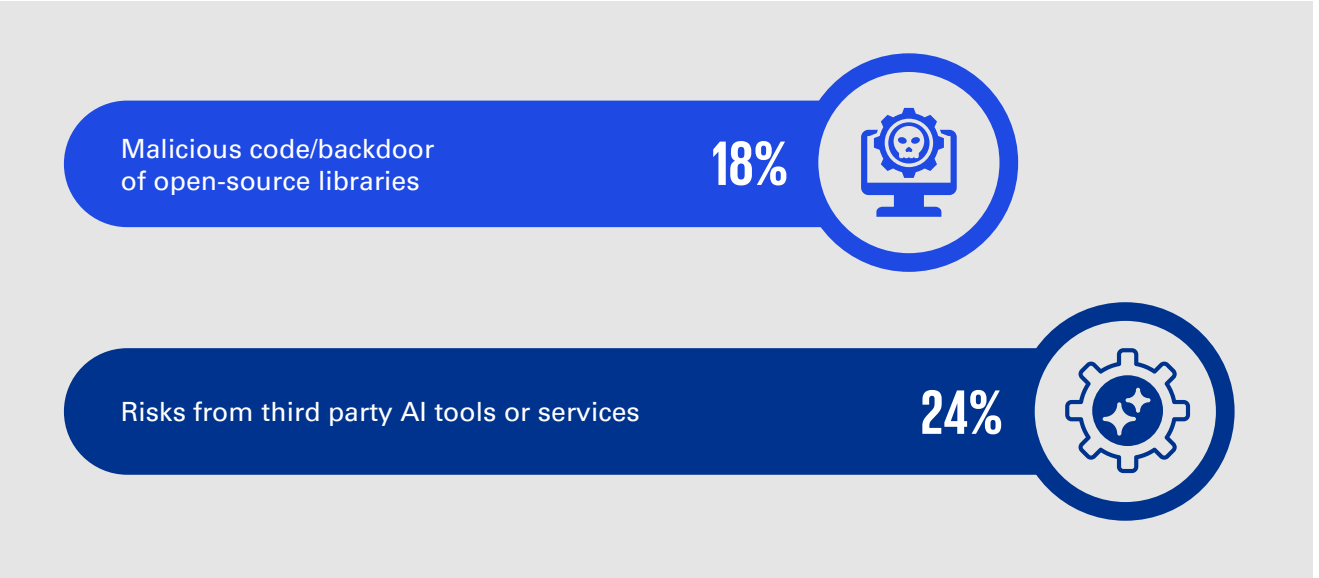


Figure 27: Percentage of software supply chain security and third-party AI risks

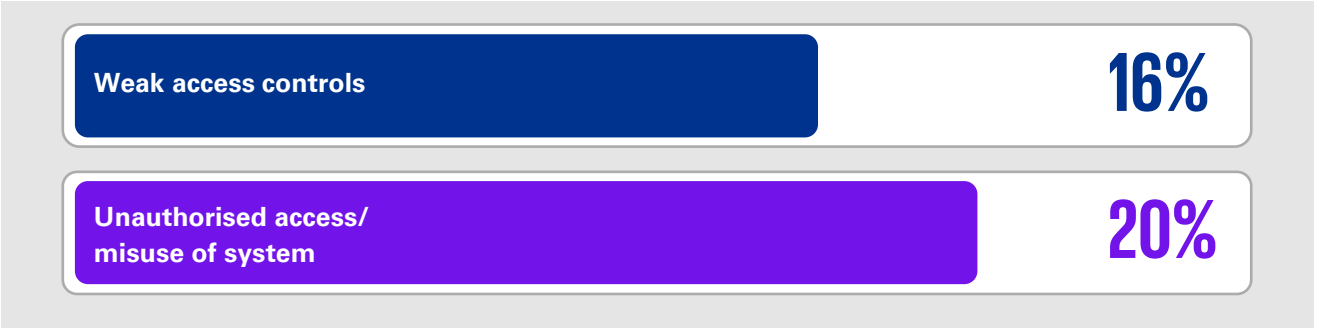


Figure 28: Insider and access risk

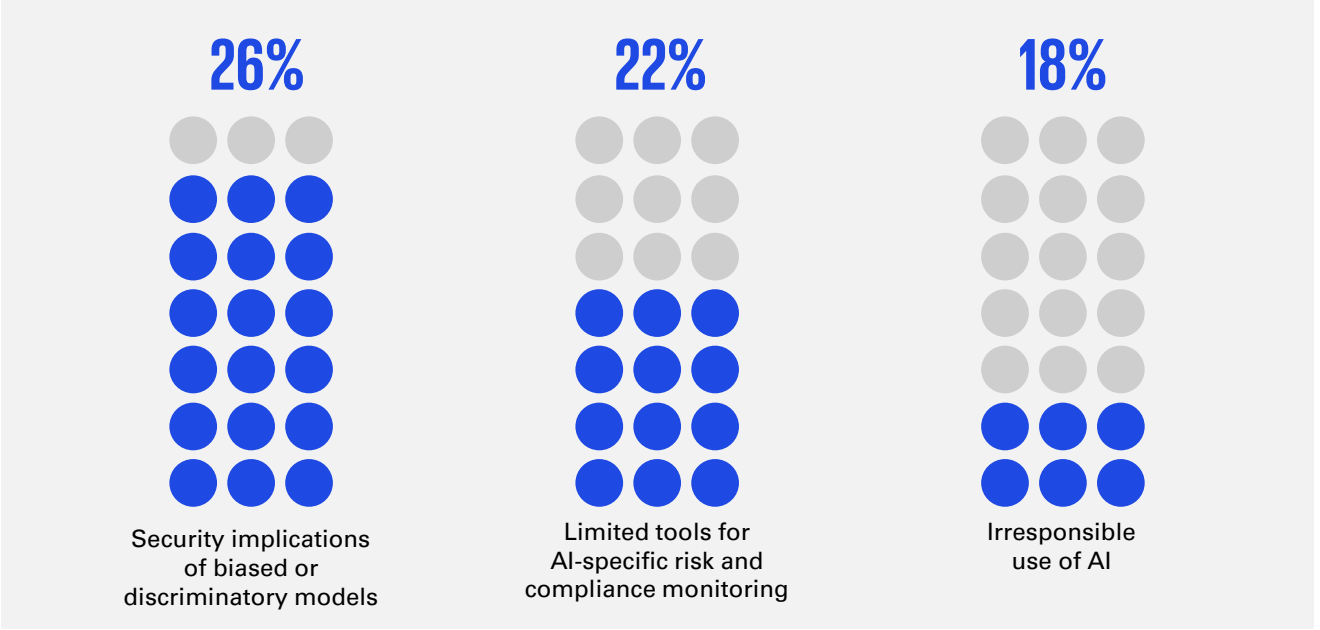


Figure 29: Bias, fairness and ethical concerns

Cyber GCC case studies 8

Security of AI: A leading cyber GCC had performed an assessment including end to end AI governance, security, and resilience to evaluate the maturity of their global AI ecosystem across internal platforms and their client-facing services.

The assessment benchmarked capabilities against leading frameworks such as NIST AI RMF, ISO 42001, and MITRE ATLAS, providing a comprehensive view of AI governance, security, risk management, and operational readiness.

The assessment scope included their global organisation's AI operating model across three dimensions—'trusted and responsible AI, secure AI and respond AI'—covering governance, security controls, privacy, resilience, monitoring, and incident response capabilities and the underlying AI architecture, technology stack, and control environment to identify gaps and improvement opportunities.

To validate control effectiveness, cyber GCC conducted AI red team assessments on select AI applications, simulating advanced adversarial attacks including prompt injection, jailbreaks, model extraction, inversion, data poisoning, and multi-stage attack scenarios. Post assessment, cyber GCC developed a prioritised roadmap to strengthen AI governance, enhance security resilience, reduce regulatory and operational risks, and enable secure, responsible, and scalable AI adoption across the enterprise.

3.4 AI security risk management

Cyber GCCs have been exploring and implementing various activities to manage AI security risks. Given the dynamic evolution of AI itself, AI security is evolving rapidly and cyber GCCs along with global and local startup ecosystem have been helping their global organisations in refining and refreshing their AI security management approach.

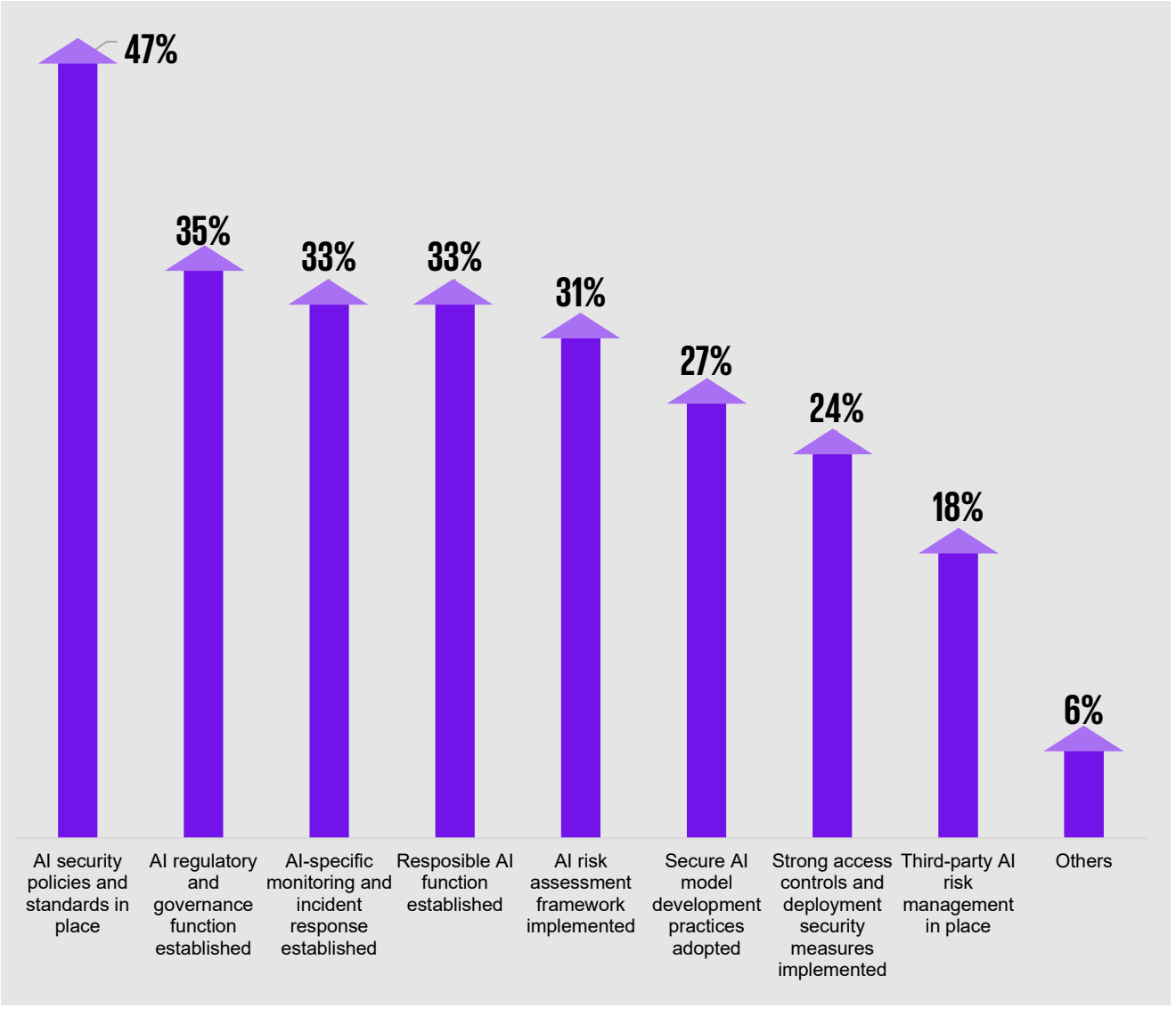


Figure 30: Key activities for managing AI security risks

In response to above noted challenges, organisations are putting in place a more structured set of controls to secure AI adoption and support regulatory compliance.

3.5. Managing third-party AI security risk

Third-party AI security risk management is emerging, with a clear progression towards more structured and continuous oversight.

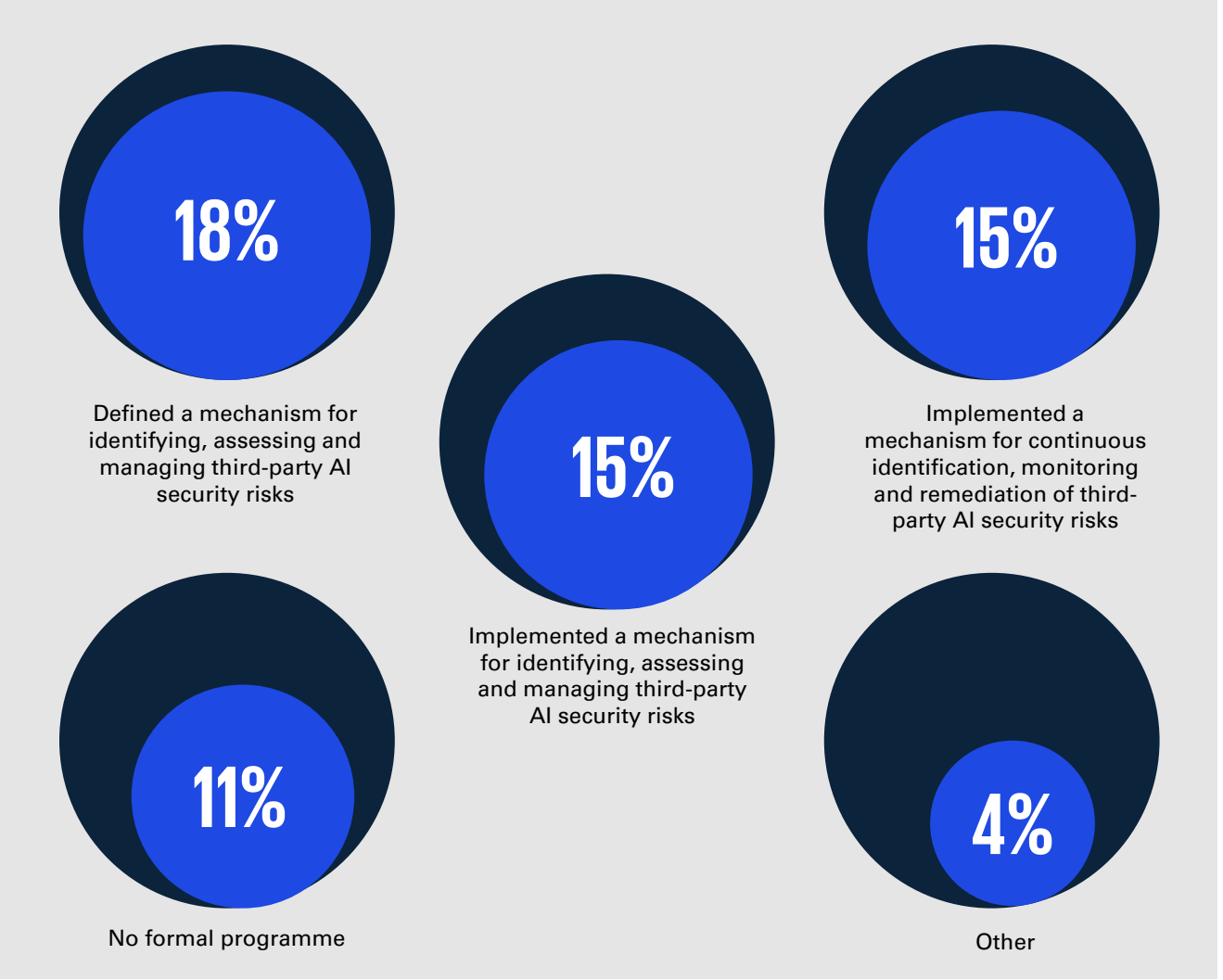
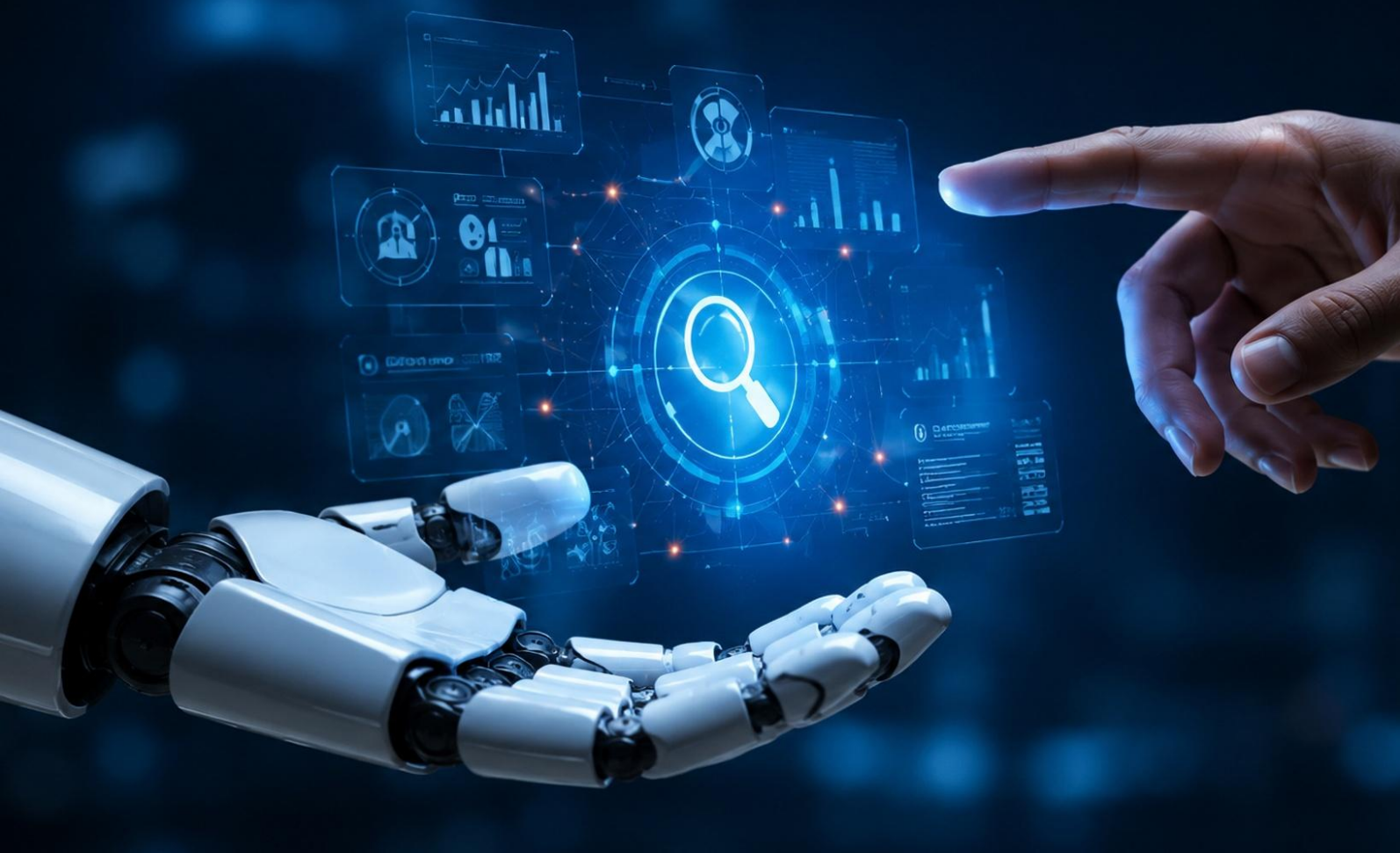


Figure 31: Maturity of third-party AI security risk management

> **As Global Capability Centres accelerate their AI transformation, securing AI has emerged as the defining priority, not just a compliance checkbox, but a genuine competitive differentiator. Organisations that embed security and governance into their AI foundations from day one are the ones earning lasting trust from customers, regulators, and partners alike.**
>
> ***- Vijay Kumar Puttaswamy, Head - Enterprise Governance, Risk, Resilience & Assurance, Atlassian***

4

Cybersecurity Research and Development (R&D) and innovation



Cyber GCCs are increasingly contributing to cybersecurity innovation, product and platform development, and long-term cybersecurity strategy. As global organisations modernise business operating models and expand the use of AI, automation, advanced analytics, and emerging technologies, cyber GCCs are taking on a focused role in securing the innovation and delivering cybersecurity solutions, right from ideation, engineering, and development.

4.1 Promoting a culture of innovation within cybersecurity GCCs

AI investments, AI skill demand, and AI quotient have significantly helped in promoting, achieving and sustaining innovation across various cybersecurity domains. Cyber GCCs are empowering their teams with AI training and assistance in a concerted effort to strengthen R&D and innovation in cybersecurity.

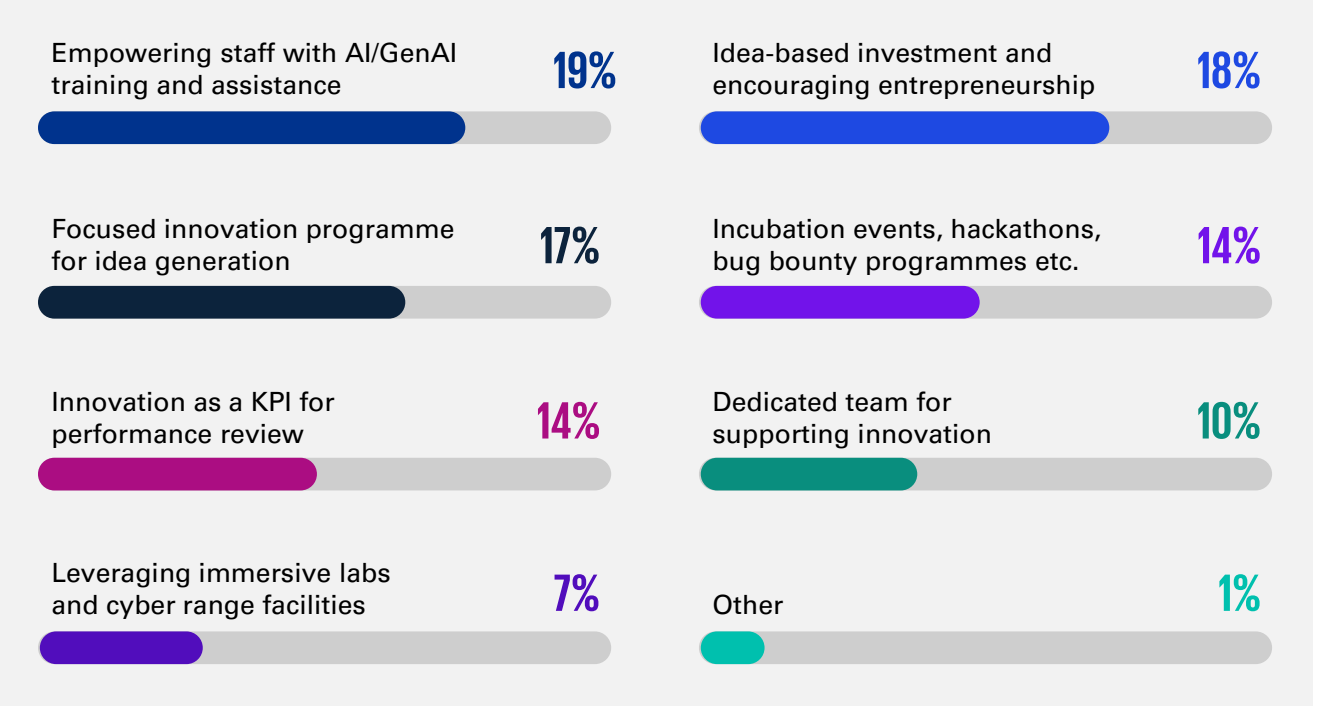


Figure 32: Key initiatives to promote culture of cybersecurity innovation

Cyber GCC case studies 9

eGRC transformation: A leading oil and gas GCC modernised its global enterprise risk and governance ecosystem through the implementation of eGRC platform modules, enabling a unified approach to risk, compliance, and third-party risk management. The program included migration of legacy risk data, configuration of risk and control self-assessments (RCSA), implementation of key risk and control indicators, policy and exception management, smart assessments, risk and third-party workspaces, executive dashboards, and CMDB enrichment.

The initiative streamlined risk management processes, reduced manual effort through automation, enhanced data quality and integrity with the eGRC platform module as a single source of truth, accelerated third-party onboarding, enabled automated control testing, and strengthened enterprise-wide risk visibility and governance.

Priority domains for cybersecurity innovation

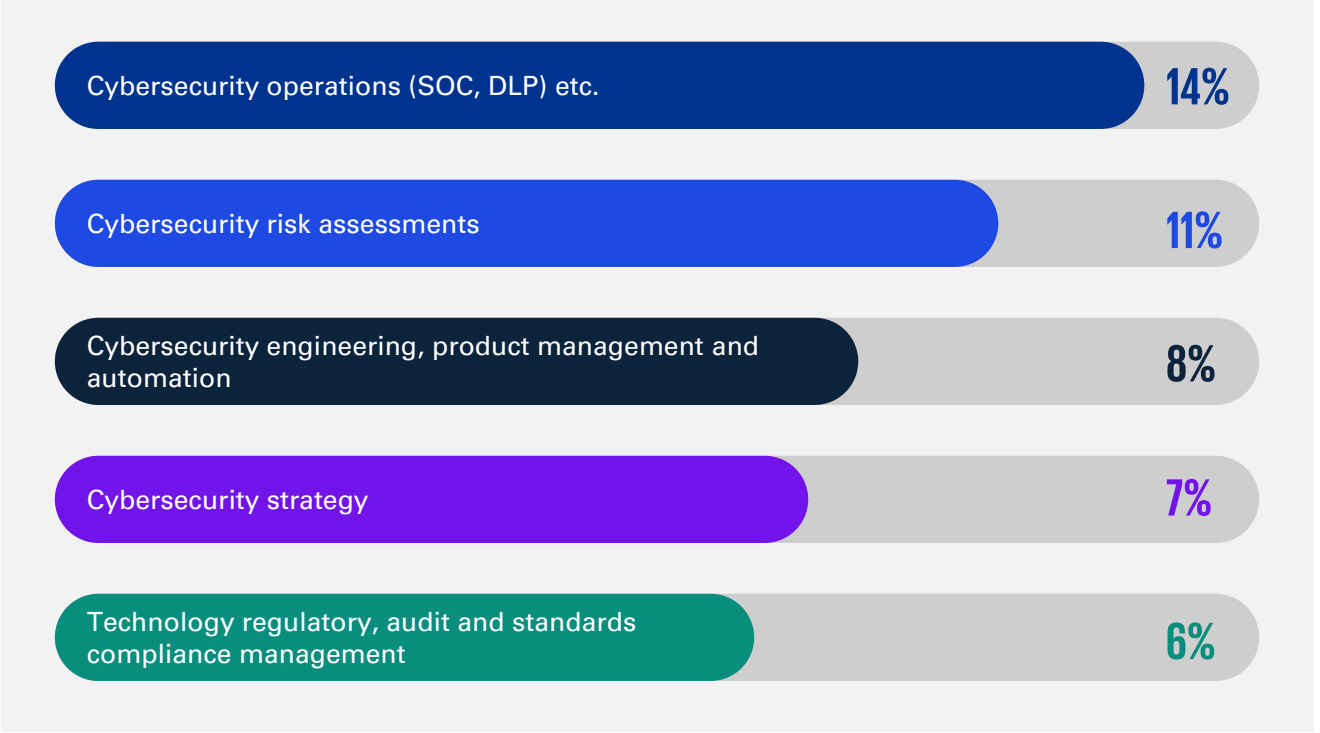


Figure 33: Top five domains for cybersecurity innovation

In addition to the above, cyber GCCs also have invested in innovation across cloud security, third party risk management, cyber resilience and cybersecurity governance.

4.2. Cyber GCC adoption of dedicated cybersecurity R&D labs

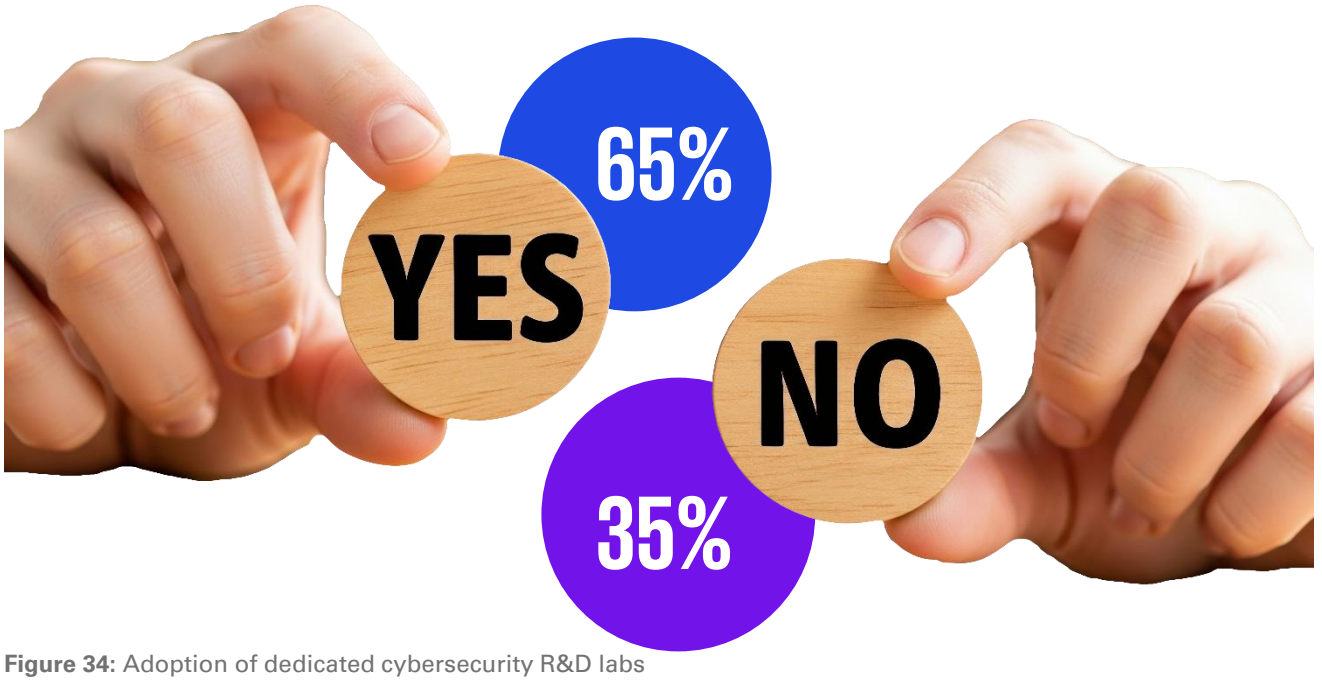


Figure 34: Adoption of dedicated cybersecurity R&D labs

Cyber GCCs that do not operate cybersecurity R&D labs, are observed to perform cybersecurity engineering, research and development and innovation embedded within cybersecurity platforms, engineering and automation and cybersecurity operations functions

4.3.Trends in Cybersecurity R&D Investment

Cyber GCCs are empowering their teams with AI training and assistance in a concerted effort to strengthen R&D and innovation in cybersecurity. 67 per cent of cyber GCCs have increased their R&D spend.

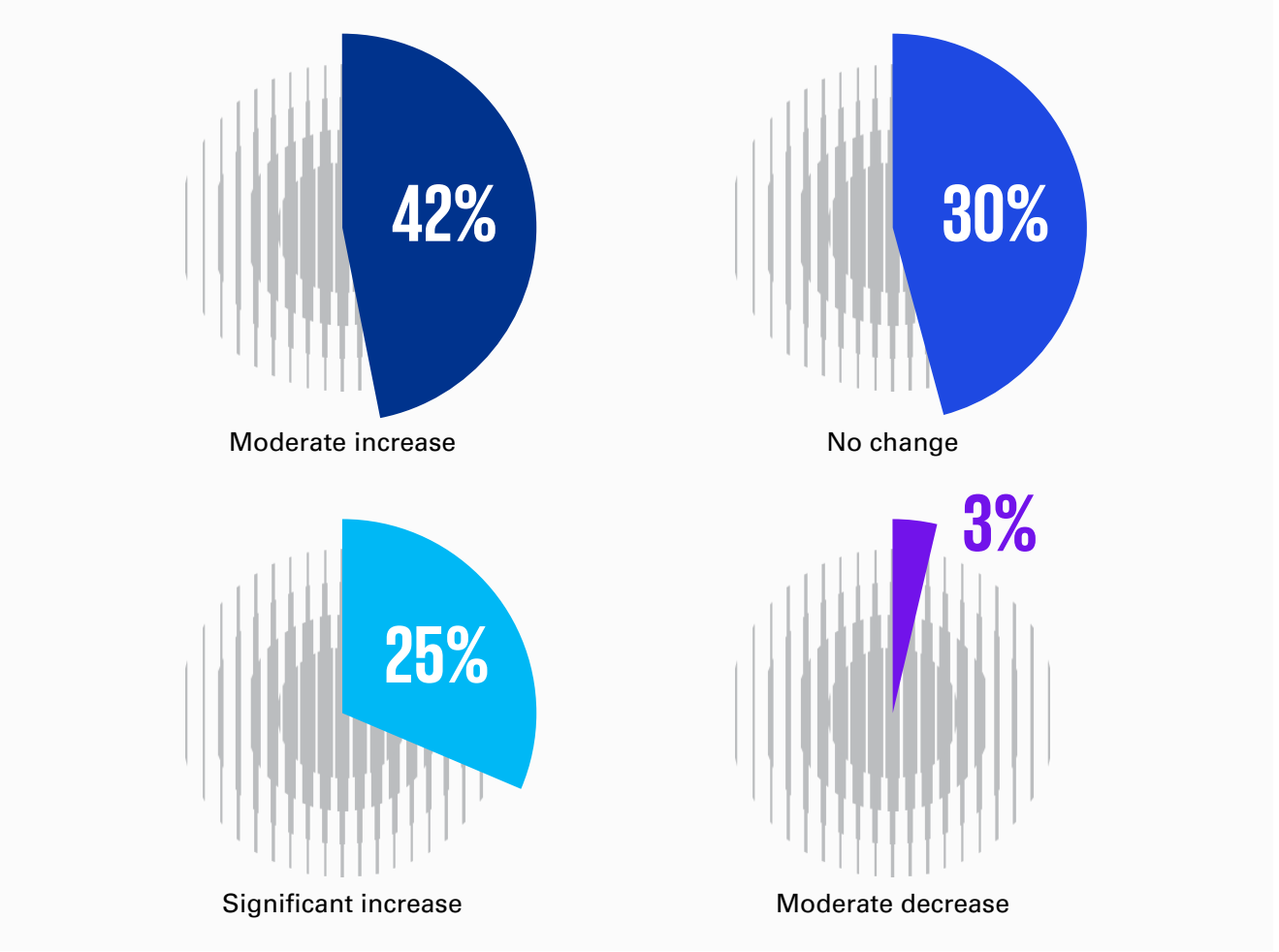


Figure 35: Cybersecurity R&D investment trends in cyber GCCs

> ***Cyber threat profile has significantly evolved and GCCs have emerged as strong force in manging this dynamic risk through constant innovation, AI powered operations and driving thought leadership.***
>
> ***- Atul Gupta, Leader Consulting Markets – GCC and Managed Services, KPMG in India***

4.4 Future trends shaping the strategic positioning of cyber GCCs

Cyber GCC leadership has identified specific trends that will shape the strategic positioning of cyber GCCs in the next three to five years. They also earmarked focused priorities in-line with the key trends.

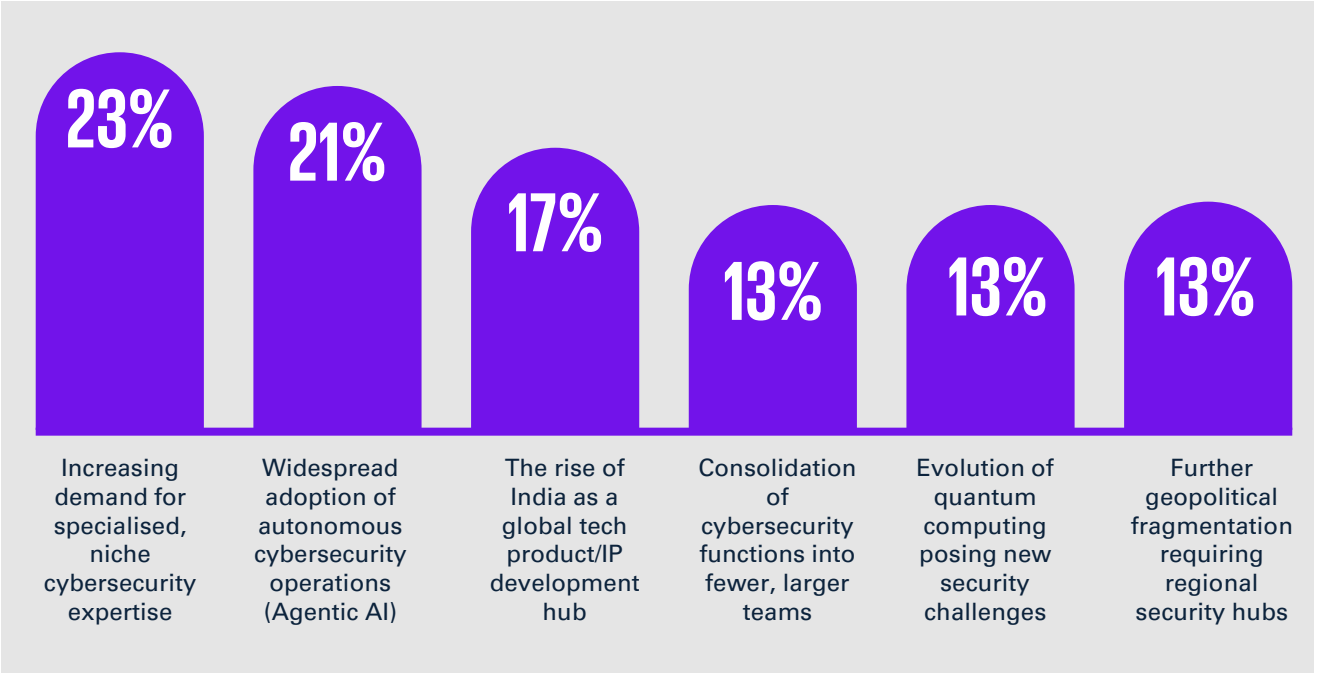


Figure 36: Future trends shaping the strategic positioning of cyber GCCs

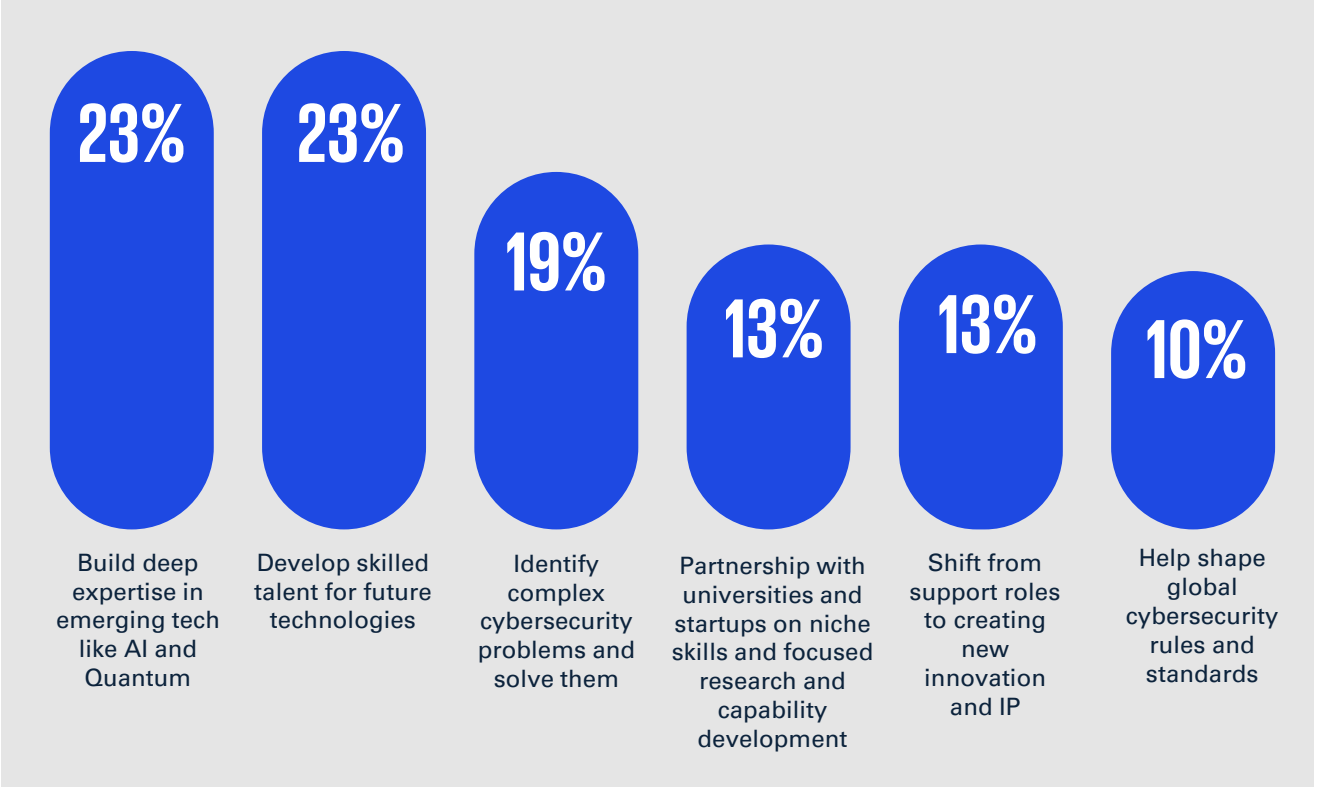


Figure 37: Cyber GCC leadership priorities for the next 3-5 years

COEs across various existing and emerging cybersecurity domains are being setup or expanded by the cyber GCCs

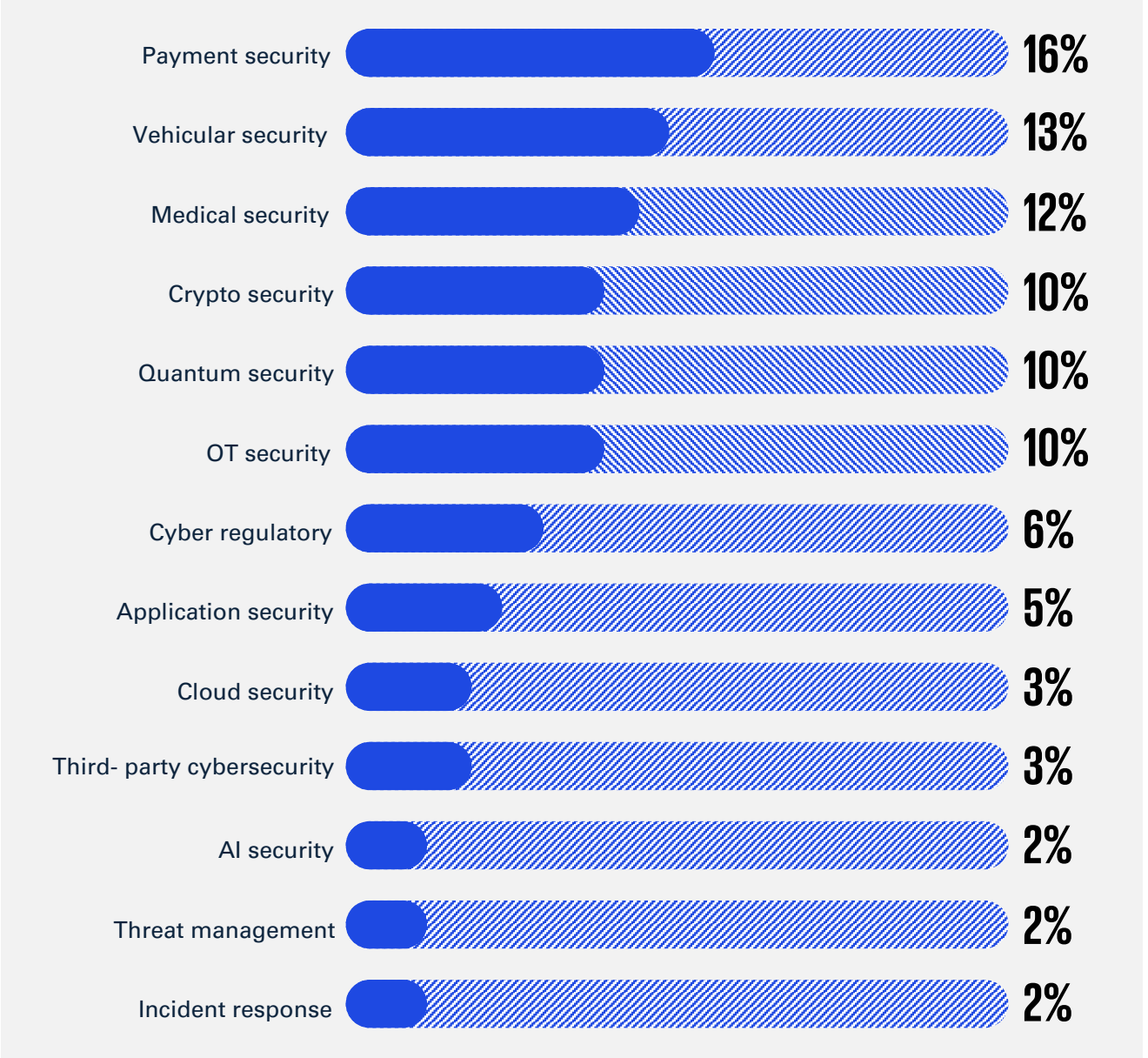


Figure 38: Cybersecurity COEs set-up by cyber GCCs

Cybersecurity is now a strategic advantage and business enabler for large organisations helping in their AI journey. GCCs are at the forefront of enabling this value proposition.

- Anish Mitra
Partner, Cyber Security and Technology, KPMG in India


5
Cybersecurity resilience

5.1 Top cybersecurity challenges

Cyber GCC leadership continues to operate in a highly dynamic and inter-connected risk environment, where traditional priorities such as regulatory compliance and third-party risk management remain prominent, while new-age challenges driven by AI adoption, digital transformation, and ecosystem dependencies are rapidly reshaping the threat landscape.

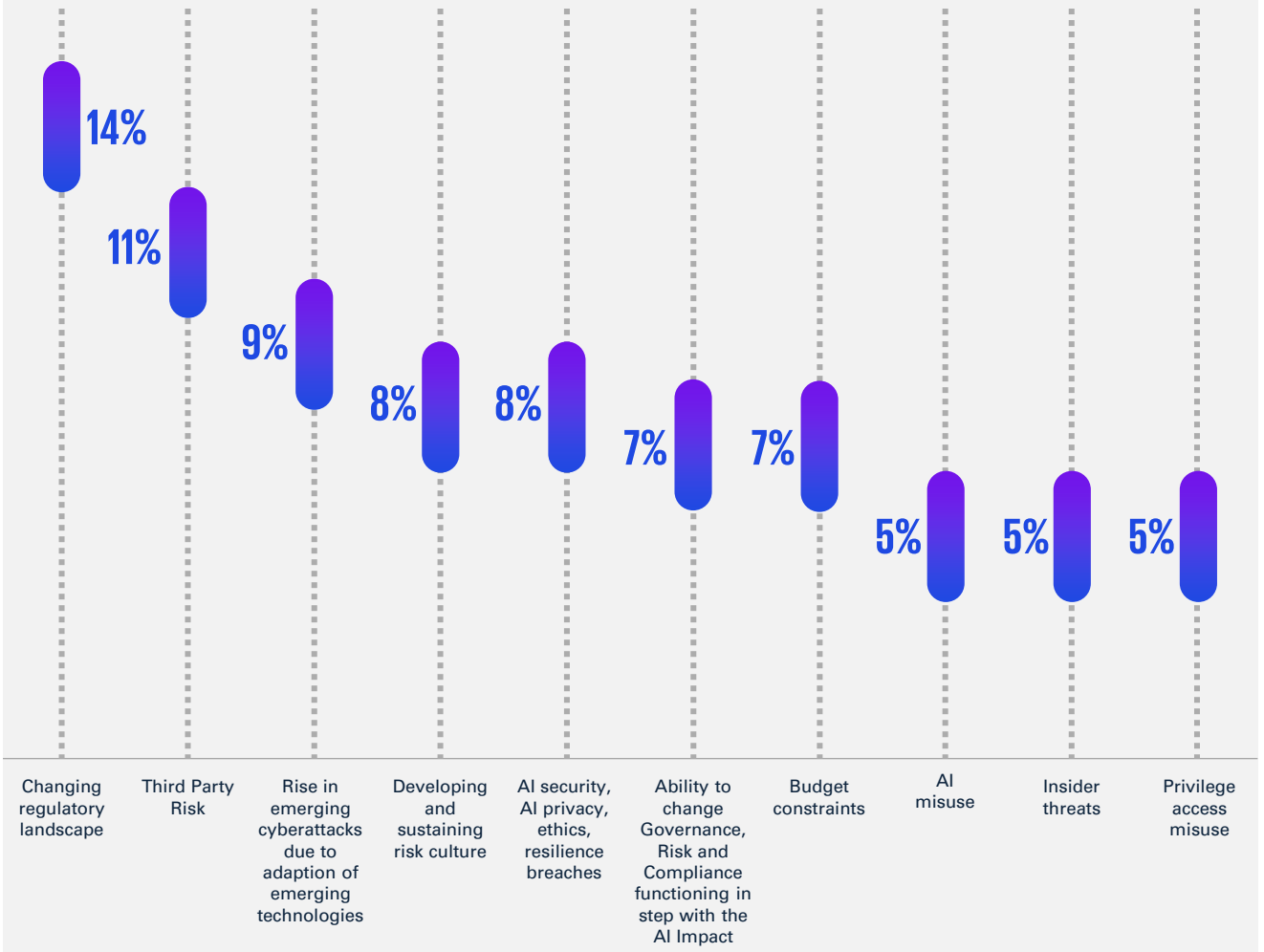


Figure 39: The top ten challenges faced by cyber GCC leadership

While established challenges continue to demand focus, 2026 marks a clear inflection point with the emergence of AI-related risks including AI security, privacy, ethics, and misuse as a distinct and growing area of concern. At the same time, budget constraints, talent gaps, and evolving governance expectations are adding pressure on cyber GCC leadership to balance innovation with risk mitigation, particularly as cyber GCCs take on a larger and global role in managing cybersecurity.

The evolution indicates a shift from building foundational cybersecurity capabilities to managing complexity at scale, with cyber GCCs increasingly expected to address emerging technology risks while sustaining governance and compliance maturity. This underscores the transition of cybersecurity from a control-centric function to a strategic, resilience-driven discipline, tightly aligned with business and technology transformation agenda.

5.2 Top cybersecurity threats and preparedness level

AI security threats have entered the top ten cybersecurity threats cyber GCC leadership is dealing with. Prompt injection, model theft, data poisoning, deepfakes etc. have become prevalent in organisations with significant AI adoption.

Multiple top cybersecurity threats from the previous edition of this report continue to be posing significant challenges for the cyber GCCs, while their preparedness in dealing with these threats has matured considerably.

Supply chain security threats, OT security threats, ransomware etc. have become more sophisticated, while organisations are still working on either standing up focused programmes and infrastructure to deal with these better or yet to initiate.

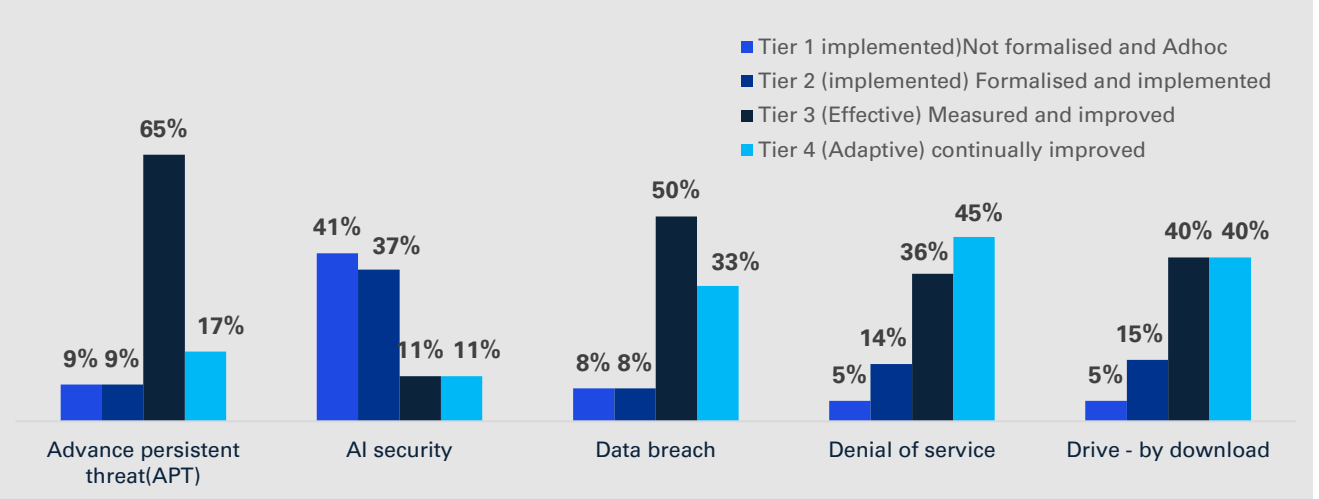


Figure 40 a: Top five cybersecurity threats with their preparedness level

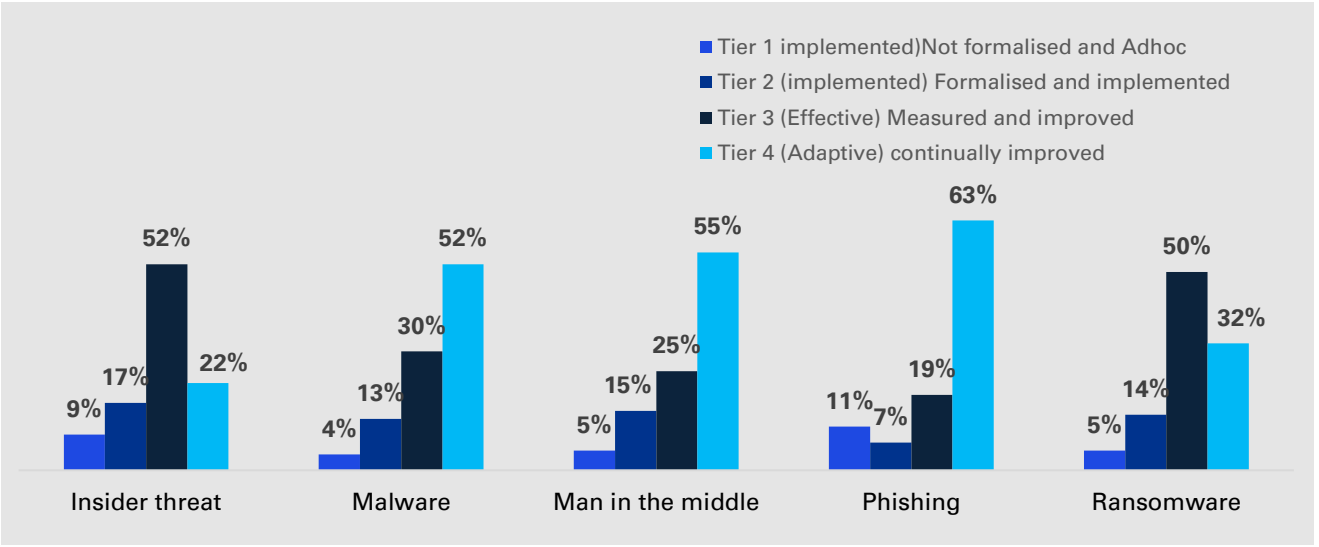


Figure 40 b: Remainder of the top ten cybersecurity threats with their preparedness level

The findings indicate a bifurcation in cybersecurity maturity, where cyber GCCs are progressing towards adaptive resilience for operational threats, while strategic and evolving risk areas like AI Governance, AI risk and AI Privacy are yet to mature. Closing this gap will require organisations to accelerate the transition from control implementation to continuous optimisation driven by advanced analytics, integrated risk frameworks, and AI-enabled security capabilities.

5.3 Top cybersecurity risks

The top ten cybersecurity risks reported to the global boards included not only the ones prominent since 2023 such as cyber regulatory risk, end point security risk, cloud security risk, etc. but also a few new cybersecurity risks.

AI misuse has entered the top cybersecurity risks tracked by global boards. This is significant considering heightened AI adoption and investments and highlights the growing importance and concern of AI misuse. Boards and executive are invested in secure AI adoption.

Geopolitical conflicts and expanding AI infrastructure have brought critical infrastructure and system risk to the top of the chart. Data centre security, telecom security, network security etc. have gained significant attention in the recent months.

Third party cybersecurity risk continues to feature in the top ten cybersecurity risks and with growing third-party AI and data, this will require more technology and AI driven strategy to deal with.

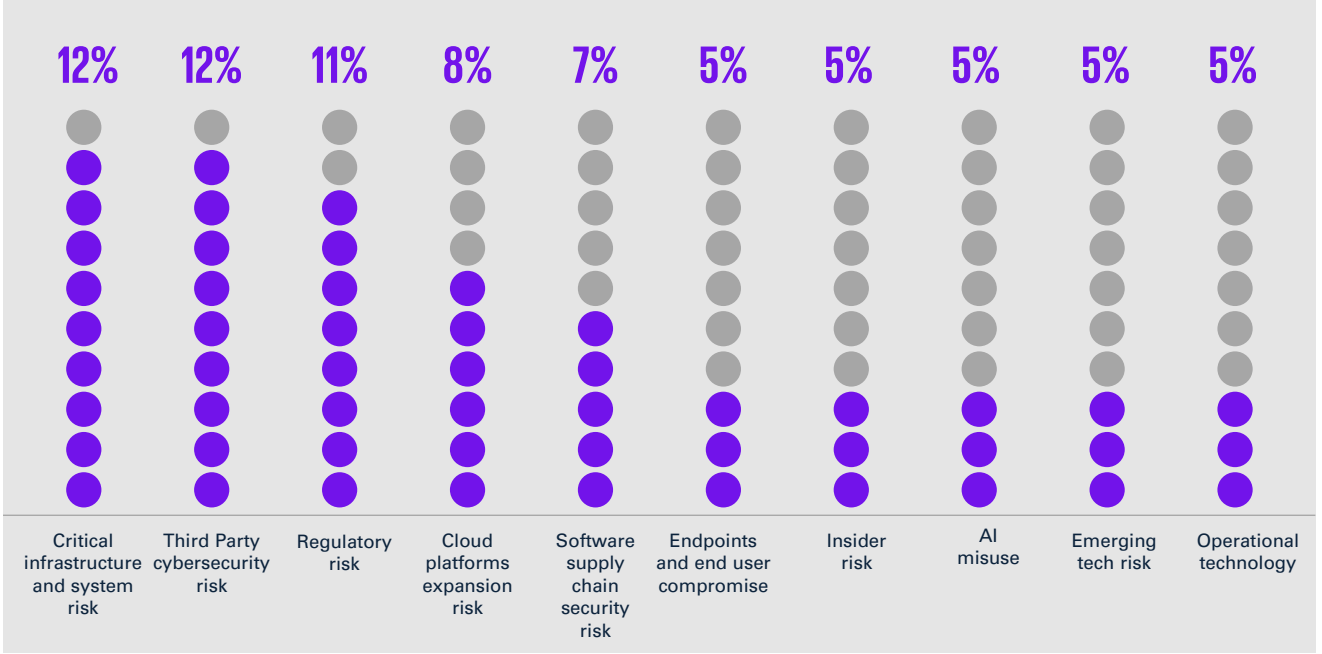


Figure 41: Top ten cybersecurity risks tracked by global boards

Cyber GCC case studies 10

AI-powered third-party cyber risk management: A global investment bank GCC has leveraged its in-house AI platform to automate several key third-party cyber risk management activities, including the evaluation of third-party questionnaire responses and supporting evidence, generation of targeted follow-up questions for vendors, and first-level quality assurance of assessment deliverables.

The initiative has delivered measurable benefits, including a 20 per cent reduction in assessment costs and a 15 per cent increase in throughput, while improving consistency and efficiency across the review process. Building on these results, the organisation is now expanding AI adoption to additional use cases such as automated report generation, risk intelligence prioritisation, and contract clause review, demonstrating how AI can enhance both the scale and effectiveness of cyber risk management programs.

5.3 Security challenges faced by organisation during cloud adoption

Cloud adoption has expanded multifold and also the cloud security challenges. Cyber GCCs have been playing a significant role in identifying, reporting and managing key cloud security challenges to their global organisations.

Cloud security has become a very distinct and niche cybersecurity function requiring significant skill, technical depth and innovative approaches to deal with ever emerging cloud security challenges.

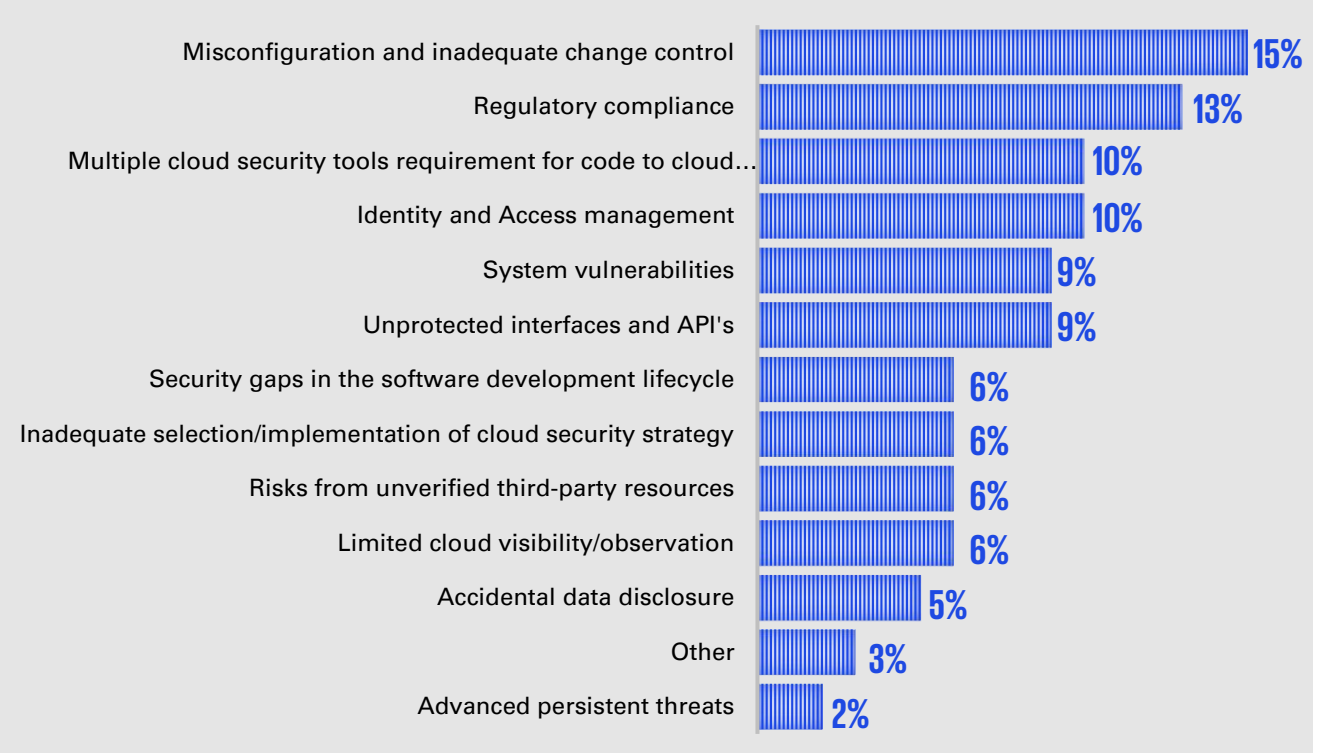


Figure 42: Top security challenges associated with cloud adoption

Cyber GCC case studies 11

Findings to Remediation Programme: A Global FinTech GCC had to deal with millions of open (CNAPP) findings across a multi-account global cloud estate. Remediation was ad hoc, unowned and their engineering team had no defensible basis for deciding what to fix first. Four levers were used - pattern-based remediation, asset identity de-duplication, re-validation of true external (internet) exposure, and AI-driven exception management - to arrive at a prioritised, owner-mapped remediation backlog.
This has helped the global organisation achieve measurable cloud risk reduction outcomes including reduction of bulk of findings within 3-4 months, tracking of exploitable, externally reachable risk instead of raw severity count and governed, time-bound exceptions stopping the backlog regrowing unseen.

12 Cyber GCC case studies

Cloud security audit evidence extraction: A leading global cloud provider had to deal with their customer challenges in identifying and extracting specific audit evidences from their cloud environment. 'Compliance manager' utility was developed to address this challenge and help the 3LOD functions to accurately capture required audit evidences.

This has helped the global cloud provider as well as their end customers reduce audit fatigue and repetitive evidence request, manual and error prone evidence collection etc.

Cybersecurity emerges as a strategic lever for cloud adoption with distinct advantages highlighted below, by the survey. Most organisations consider cloud adoption to provide for improved resilience, while security and cost savings also have been key factors.

Interestingly, about 2 per cent of organisations have chosen to move out of cloud, indicating a reverse migration from cloud.

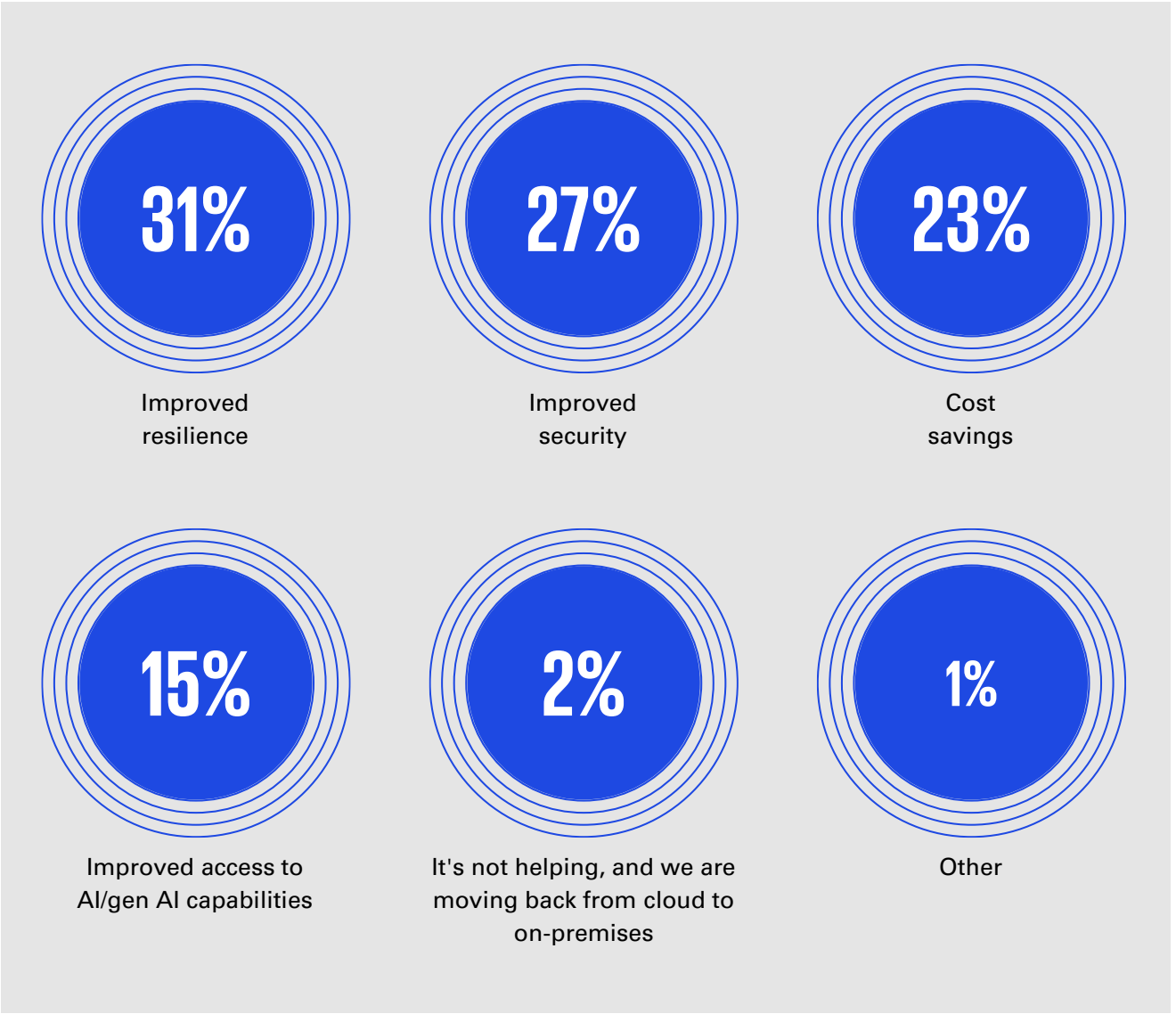


Figure 43: How cloud migration has benefited from cybersecurity standpoint

Key challenges in securing OT systems and networks

OT security is evolving across sectors with increasing OT adoption. While oil and gas, power, utilities sectors have seen OT security use cases mature significantly, they also have experienced OT security risks and challenges.

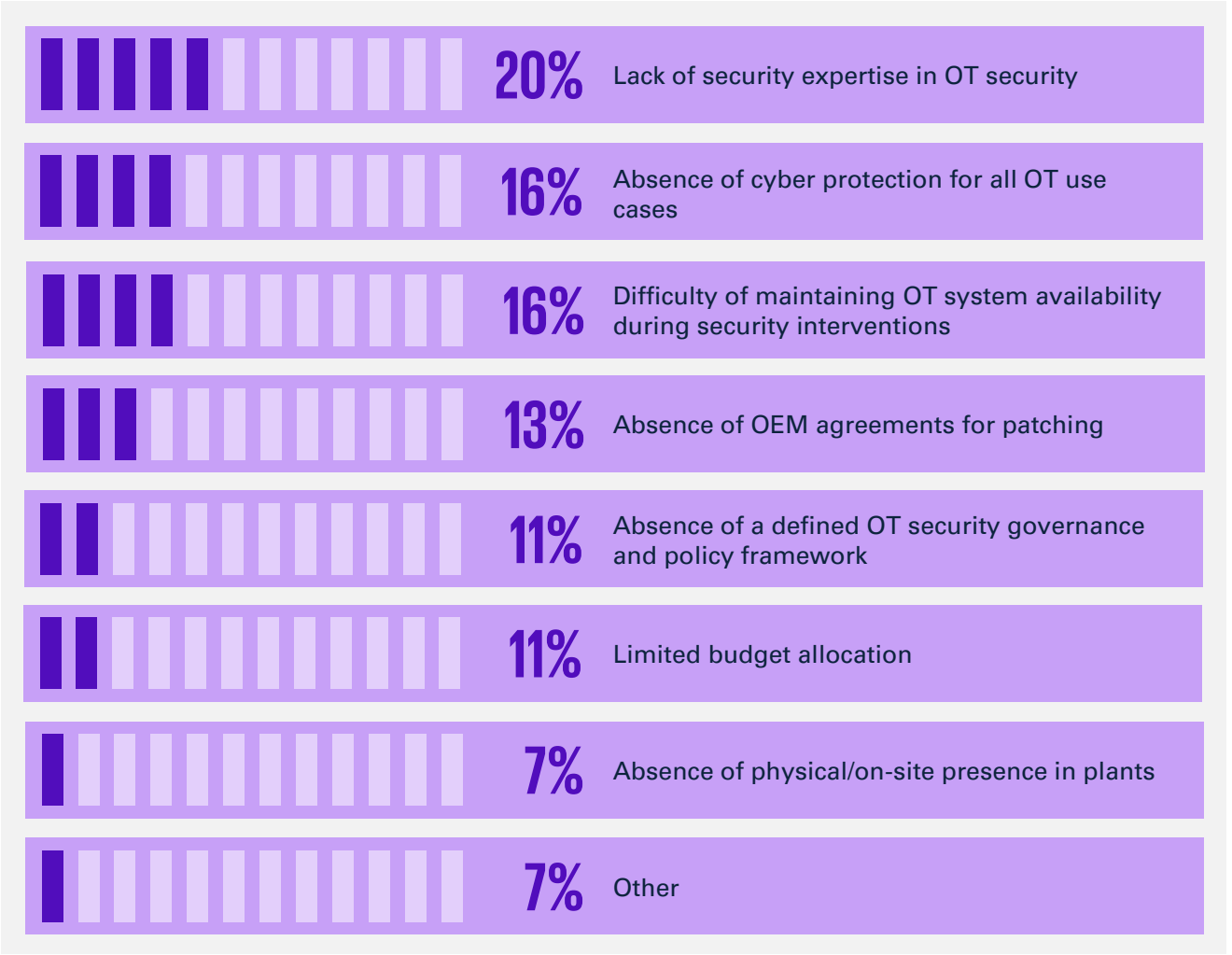


Figure 44: Top OT security challenges

The findings suggest that while OT security is gaining strategic attention, its adoption remains uneven across sectors, with non-OT-heavy industries yet to fully engage, and OT-dependent organisations grappling with foundational capability gaps.

As IT and OT environments continue to converge, there is a growing need to build specialised talent, formalise governance frameworks, and enable security controls that are non-disruptive to operations. This reinforces the role of cyber GCCs in scaling OT security expertise and supporting their global organisations in managing complex, safety-critical environments with resilience and precision.

5.4 OT reference architecture for IT/OT convergence

Operational Technology (OT) systems are increasingly converging with IT systems to enable more smarter and more efficient systems with real-time and seamless data flow, effective decision making and enhanced ability for targeted maintenance, and real-time visibility. A robust OT reference architecture ensures secure integration while maintaining reliability and safety.

Cyber GCCs have helped their global organisations in integrating OT and IT environments. Various cyber GCCs have put in place programmes for OT security, aligned IT/OT reference architecture with ISA 62443, and are assessing and managing OT security risks to critical systems. However, many organisations are yet to either initiate or mature their OT security programmes, while some of the global organisations have started leveraging cyber GCCs for the same.

Many organisations are still maturing their IT/OT integration strategies, with varying levels of alignment to recognised security frameworks. The distribution below highlights how prepared enterprises are in defining a unified IT/OT reference architecture.

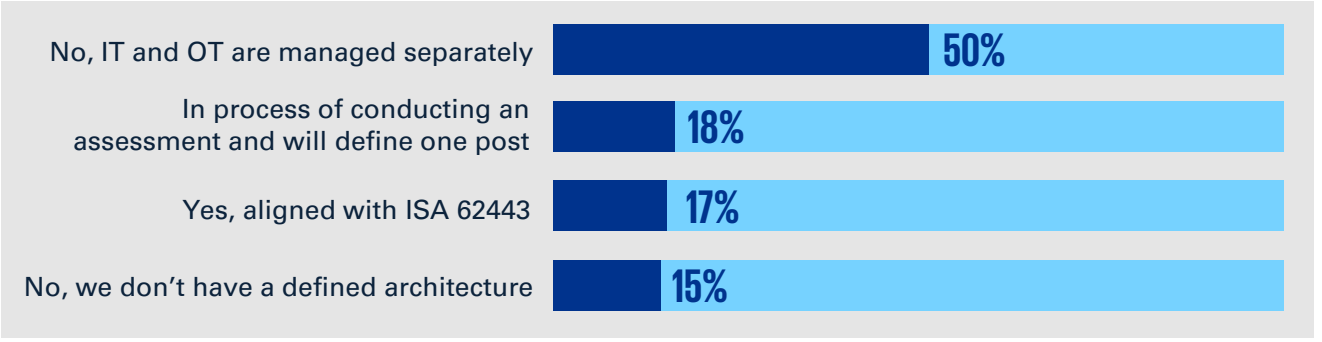


Figure 45: IT and OT convergence management

Cyber GCC case studies 13

OT cybersecurity transformation: A leading global energy major GCC helped its global organisation in assessing and strengthening the cybersecurity posture of its critical OT environments across thermal generation plants, renewable energy facilities, substations, and manufacturing operations. The programme included OT network architecture reviews, IT/OT convergence assessments, vulnerability assessments, configuration reviews, access control evaluation, and governance framework development.

By identifying critical vulnerabilities, segmentation gaps, legacy system risks, and operational security weaknesses, the cyber GCC enabled the global organisation to standardise cybersecurity practices across sites, improved compliance with industry guidelines, enhanced resilience against cyber threats, and established a roadmap for long-term OT security governance and risk reduction.

Key benefits:

1. Enhanced visibility into OT cybersecurity risks across diverse operational environments
2. Identification of critical vulnerabilities, network segmentation weaknesses, and IT-to-OT attack paths
3. Standardisation of OT security practices and controls across generation, transmission, distribution, and manufacturing facilities
4. Improved compliance with critical infrastructure security requirements and industry leading practices
5. Development of a prioritised remediation roadmap and governance framework to strengthen cyber resilience
6. Increased maturity of the organisation's OT cybersecurity programme, enabling proactive risk management across critical operational assets.

5.5 External shocks: geopolitical and systemic risk

Events such as geopolitical conflicts, trade restrictions, supply chain disruptions, and shifting alliances are contributing to heightened cyber threats, regulatory fragmentation, and operational disruptions.

Geopolitical uncertainty is increasingly shaping the global cybersecurity landscape, introducing non-traditional risk drivers that extend beyond technology into economic, regulatory, and supply chain domains.

In this evolving environment, cyber GCCs are playing a critical role in absorbing and managing the downstream impact of geopolitical shocks, enabling global organisations to sustain operations, strengthen resilience, and adapt to rapidly changing risk conditions.

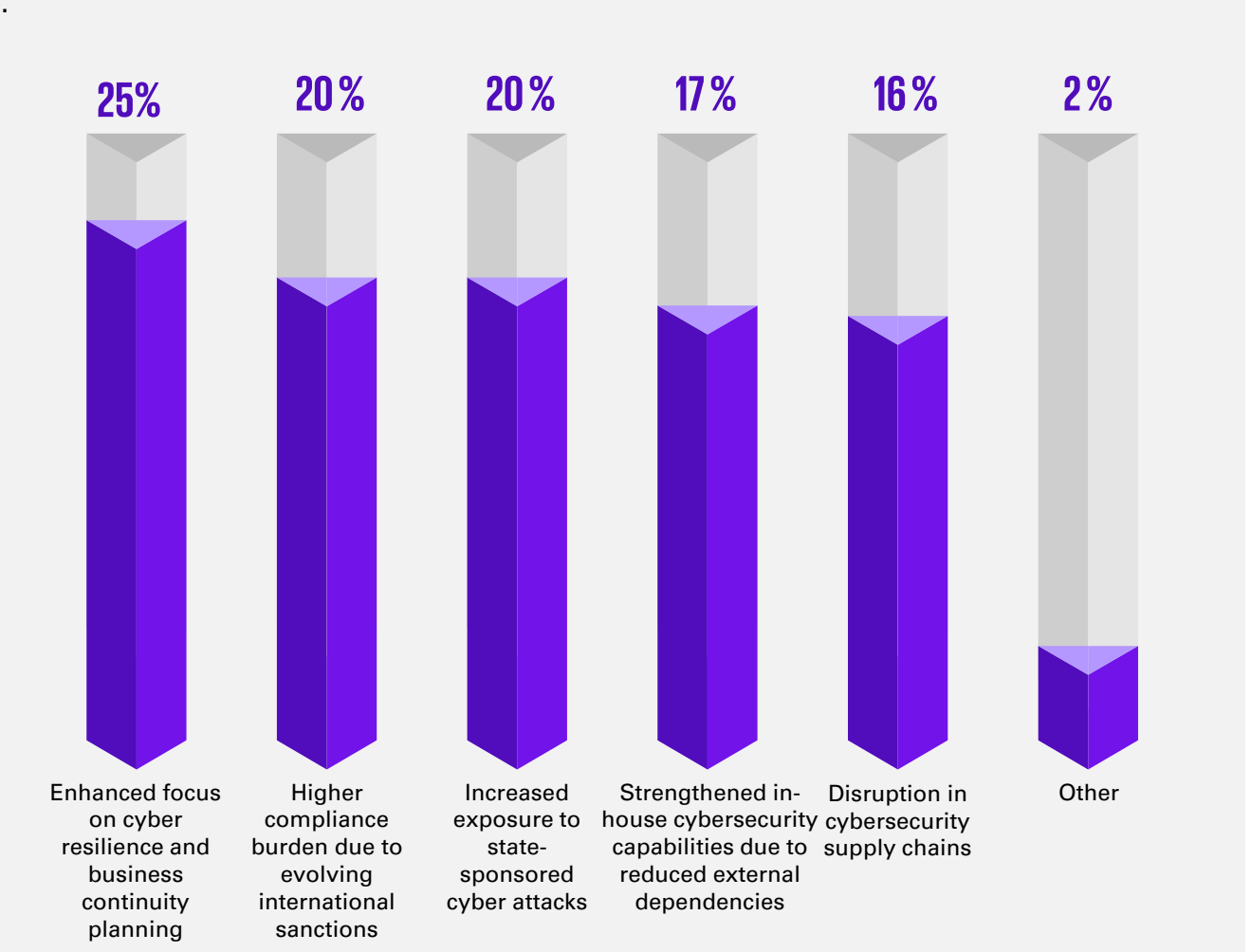


Figure 46: Impact of geopolitical events

The impact of geopolitical developments is both broad-based and multi-dimensional, affecting how organisations prioritise resilience, security investments, and operational strategies.

The findings indicate that cybersecurity is no longer isolated from geopolitical dynamics. Instead, organisations are increasingly required to embed geopolitical risk into their cyber resilience strategies, with a strong emphasis on continuity planning, regulatory adaptability, and threat anticipation.

There is a clear shift towards resilience-led cybersecurity, where organisations are preparing for systemic disruptions driven by external shocks, rather than isolated cyber incidents. This elevates the role of cyber GCCs as strategic enablers of global resilience and stability.

Cyber GCC role in dealing with geopolitical impact

In response to geopolitical disruptions, Cyber GCCs are implementing targeted strategies to strengthen internal capabilities, reduce external dependencies, and enhance operational control. The response strategies indicate a transition towards self-sufficient and resilient cybersecurity operating models, with Cyber GCCs at the core of this transformation. The focus on internal capability building, vendor diversification, and regulatory alignment highlights a strategic shift from efficiency-driven globalisation to resilience-driven localisation.

Cyber GCCs are evolving into critical resilience hubs, enabling organisations to navigate geopolitical volatility through stronger internal controls, localised capabilities, and adaptive operating models, ultimately supporting sustained business continuity in an uncertain global environment.

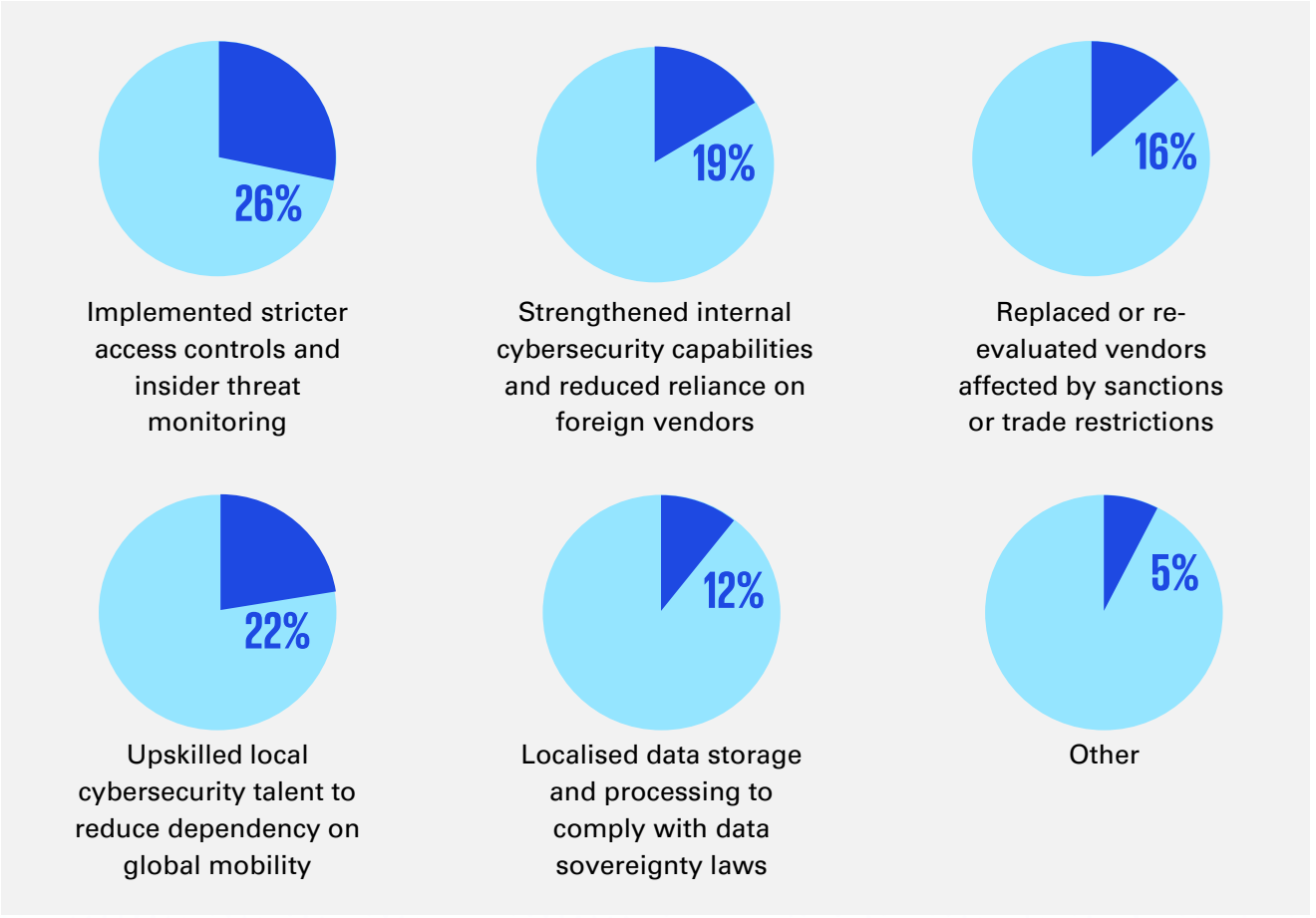


Figure 47: Strategies implemented to deal with the impact

5.6 Cryptographic resilience

The rapid advancement of quantum computing is introducing a fundamental shift in the cryptographic risk landscape, requiring organisations to reassess the long-term viability of existing encryption mechanisms. As data with long-term sensitivity becomes vulnerable to future decryption capabilities, cryptographic resilience is emerging as a critical pillar of enterprise security, encompassing visibility into cryptographic assets, readiness for Post-Quantum Cryptography (PQC), and the ability to adapt through crypto agility. Cyber GCCs are increasingly supporting global organisations in initiating PQC readiness programmes, although maturity levels vary significantly across the ecosystem.

Cryptographic inventory and PQC alignment:

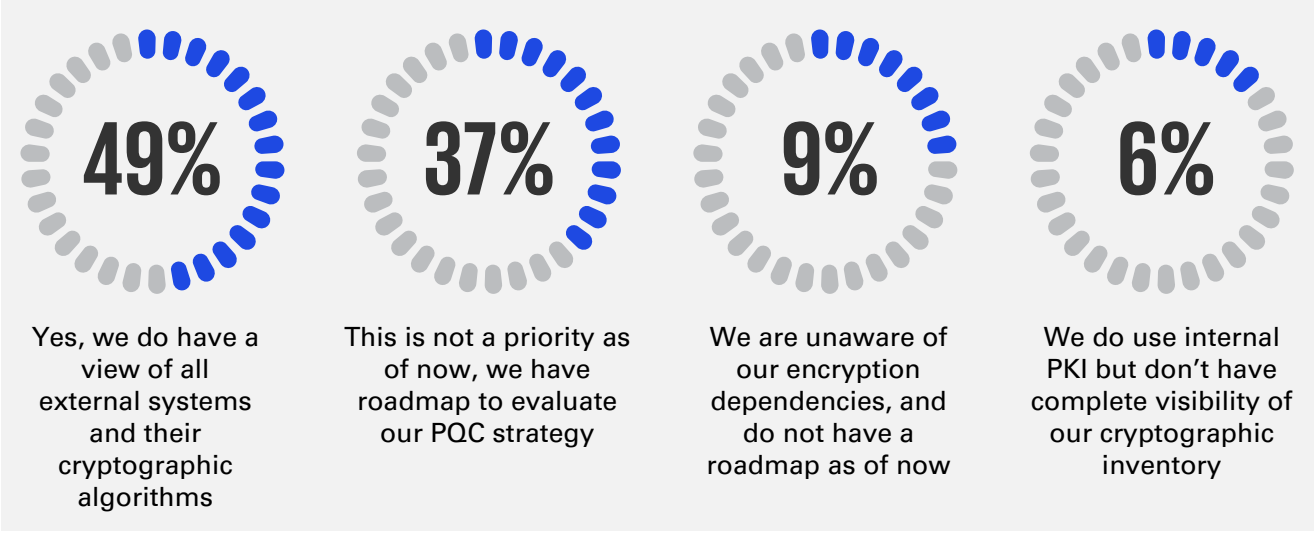


Figure 48: Organisations having cryptographic inventory, aligning with PQC guidelines

The data suggests that while baseline cryptographic visibility is improving, a large proportion of organisations are still in the early stages of translating awareness into actionable PQC strategies.

Organisations are acknowledging the importance of cryptographic inventory as a prerequisite, but PQC readiness remains deferred rather than actively executed, exposing potential long-term risk. This reinforces the need for cyber GCCs to drive enterprise-wide cryptographic discovery, risk mapping, and prioritised transition planning.

Quantum threat assessment and PQC migration readiness

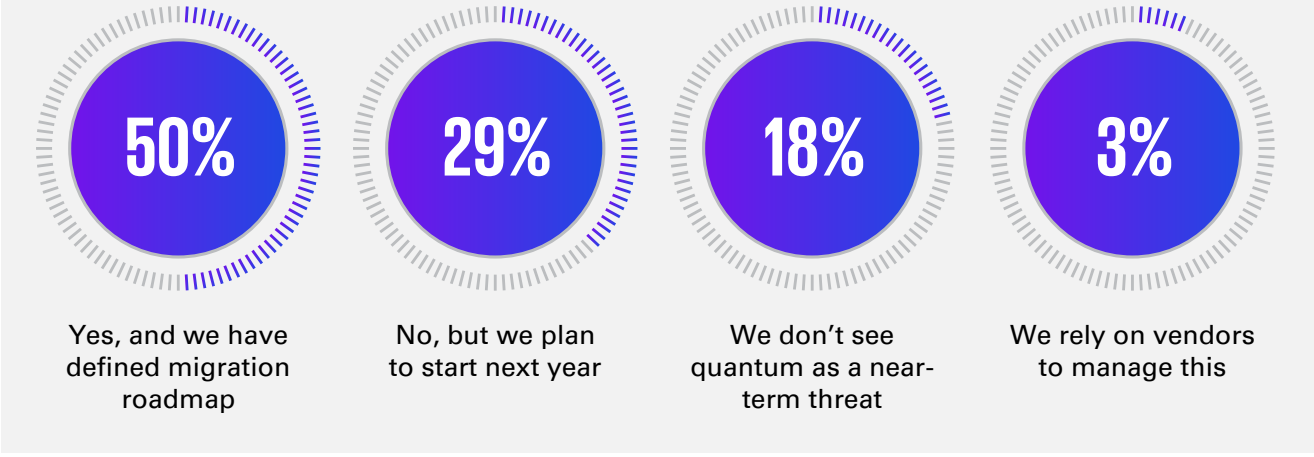


Figure 49: Quantum threat assessment and PQC migration readiness

As quantum risk transitions from theoretical to practical, organisations will need to accelerate from planning to execution, focusing on defining migration roadmaps, enhancing crypto agility, and reducing dependency on external vendors. Cyber GCCs are well-positioned to centralise and scale PQC initiatives, enabling consistent and coordinated enterprise-wide transformation.

Cyber GCC case studies 14

Post Quantum Cryptography (PQC) assessment:

A leading global banking GCC conducted a Post-Quantum Cryptography (PQC) assessment to help the bank understand its exposure to future quantum-computing risks and the potential impact on long-term encrypted data. The assessment scope included cryptographic landscape, PKI environment, and existing PQC initiatives against regulatory expectations, NIST PQC standards, and industry leading practices.

In addition, the following activities were performed to identify gaps and establish a roadmap for future PQC adoption

1. PQC readiness assessment – from the perspective of availability of a crypto inventory, PKI infrastructure and certificate related aspects
2. HSM configuration audit with regards to FIPS 140-2 and 140-3
3. Decentralised cryptographic audit for the overall cryptography and public key infrastructure (PKI) control environment to guide future PQC adoption.

5.7 Software Supply Chain Security (SSCS)

Software supply chain security risk has emerged as a critical focal area for global organisations, driven by increasing reliance on third-party software, open-source components, and cloud-delivered services.

Cyber GCCs are playing an important role in operationalising SSCS programmes, moving beyond policy definition to execution, monitoring, and integration with enterprise security operations. However, the maturity of these programmes varies significantly, reflecting a transition phase from foundational setup to scaled, end-to-end supply chain security risk management.

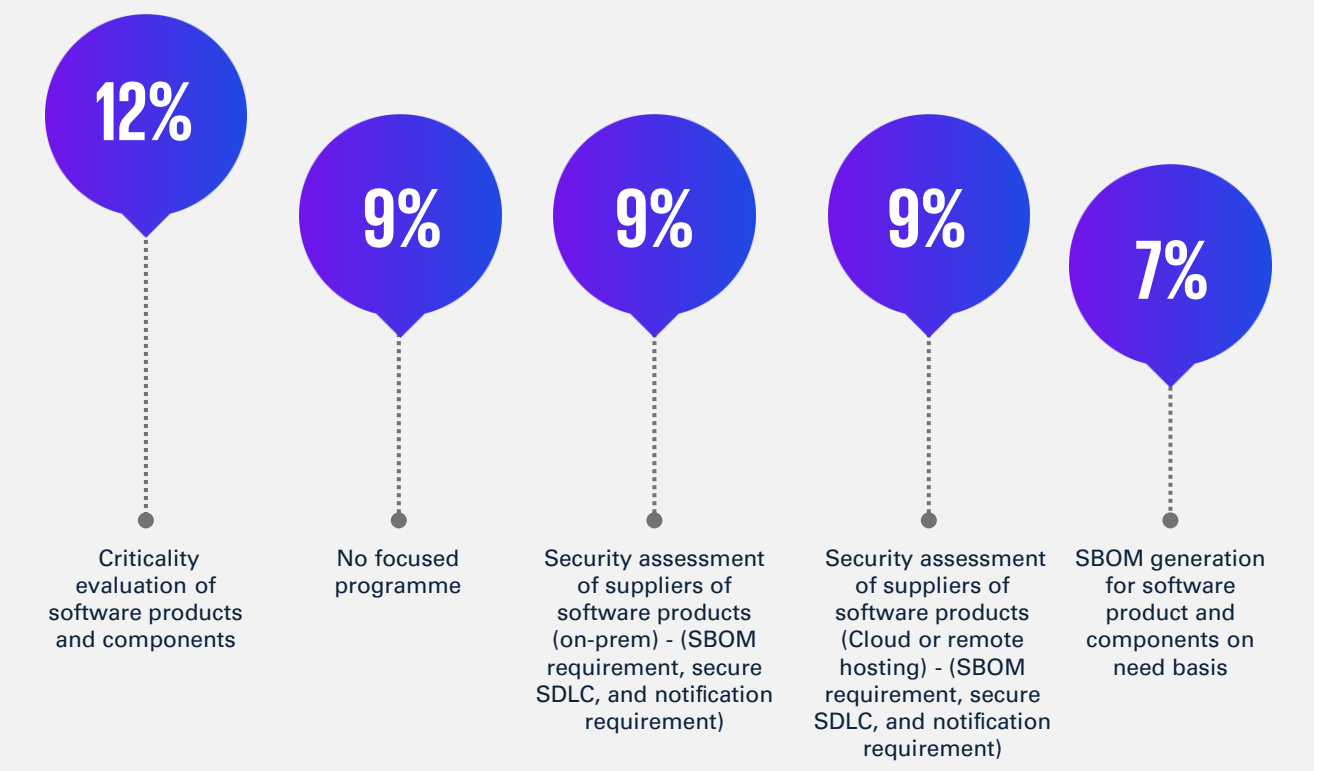


Figure 50 a: Top five activities of cyber GCC in managing software supply chain security risk

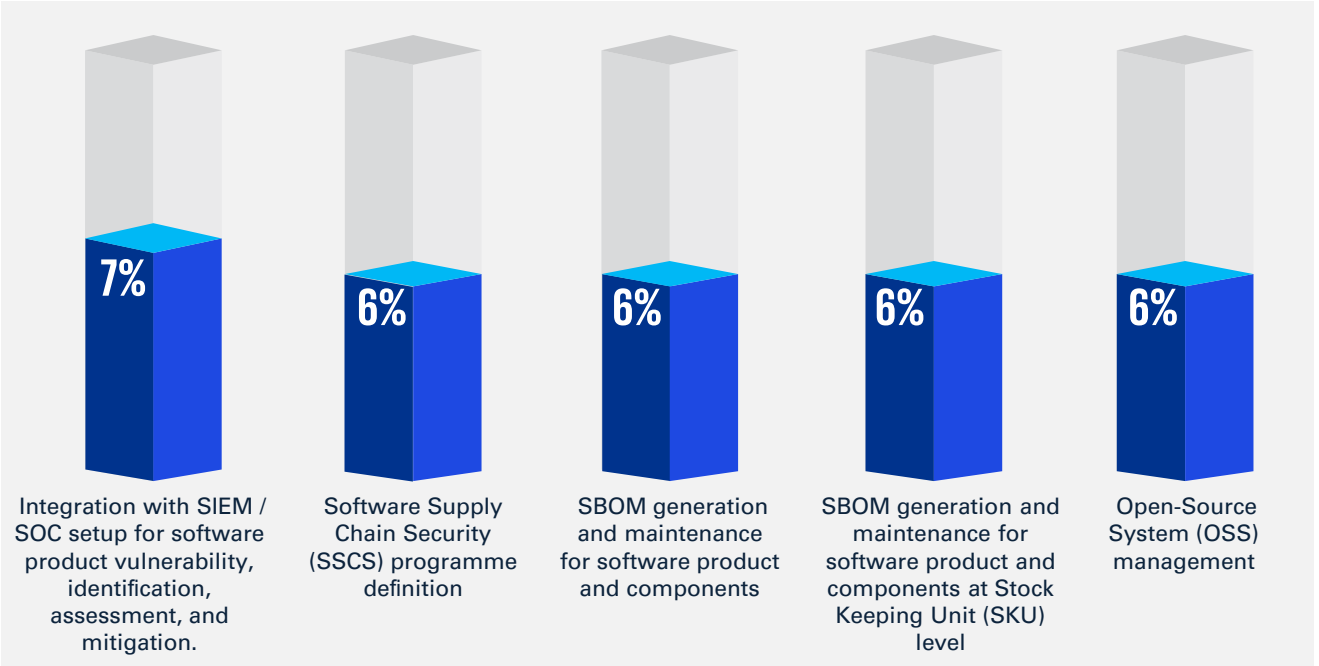


Figure 50b: Remainder of the key activities of cyber GCC in managing software supply chain security risk

Shift from programme definition to operational execution: The data highlights a clear shift from defining SSCS programmes to executing and embedding them within enterprise security operations. While foundational gaps still exist, particularly among organisations without structured programmes, the broader trend reflects increasing maturity in managing supplier security risk, software components, and vulnerabilities across the lifecycle.

Software supply chain security is evolving into a multi-layered discipline, requiring integration across procurement, development, security operations, and governance functions.

Cyber GCCs are emerging as central orchestrators of SSCS, enabling organisations to scale visibility, strengthen vendor assurance, and operationalise risk management across increasingly complex and distributed software ecosystems.

Cyber GCC case studies 15

Strengthening software supply chain security through continuous SBOM monitoring: A global telecommunications GCC enhanced its software supply chain security framework to address emerging risks associated with third-party Software-as-a-Service(SaaS) and Commercial Off-The-Shelf(COTS) applications. As part of this initiative, the organisation mandated that vendors provide Software Bills of Materials (SBOMs) for all relevant solutions. These SBOMs are ingested into an in-house platform that continuously monitors software components for newly disclosed high-severity and exploitable vulnerabilities. When critical vulnerabilities are identified, they are automatically prioritised for impact assessment and remediation engagement with the respective third parties.

This approach has enabled the organisation to improve visibility into the composition and security posture of external software assets, strengthen resilience against software supply chain attacks, and proactively manage vulnerabilities that could affect business-critical SaaS and COTS environments.

5.8 Cyber risk reporting

As cyber risk continues to gain prominence at the board level, organisations are increasingly focusing on strengthening risk culture and enhancing the way cybersecurity insights are communicated to leadership. Effective resilience today is not only driven by controls and capabilities, but also by the ability to translate cyber risk into business-relevant insights, enabling informed decision-making. In parallel, organisations are advancing towards integrated and collaborative operating models, with cyber GCCs playing a pivotal role in enabling centralised visibility, coordinated response, and intelligence-led operations.

Figure 51: Cybersecurity risk reporting to the board/committee/leadership/key stakeholders

5.9 Cyber fusion centres

Various global organisations have setup cyber fusion centres, bringing cybersecurity, fraud, law enforcement, legal, regulatory, AI, real-time intelligence and data management capabilities to fuse contextual insights from various data sources.

The primary objective of these centres is to provide a coordinated, effective and efficient response to specific intelligence inputs requiring actions from cross functional teams.

Cyber GCCs have been the go-to destination for operating these centres, providing next-generation capabilities and delivering faster incident response, overall better cybersecurity outcomes, cyber threat prevention in a proactive and coordinated manner. Cyber fusion centres are emerging as a key enabler of integrated cybersecurity operations, bringing together threat intelligence, detection, response, automation, and analytics into a unified operating model.

The adoption of cyber fusion centres signals a fundamental shift in cybersecurity operating models, from fragmented, function-specific approaches to integrated, intelligence-led ecosystems.

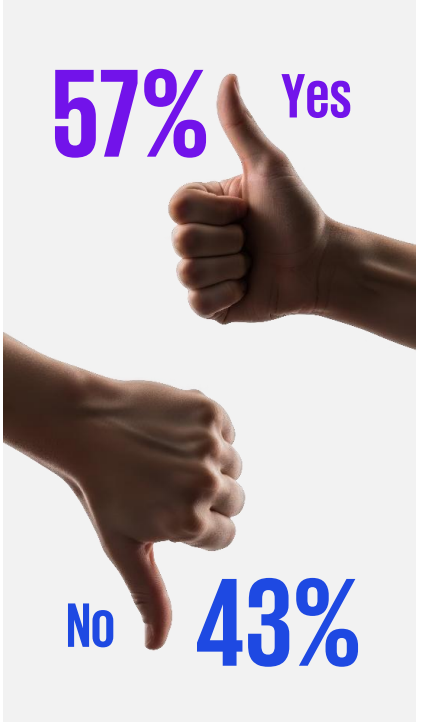


Figure 52: Cyber GCCs with cyber fusion centre

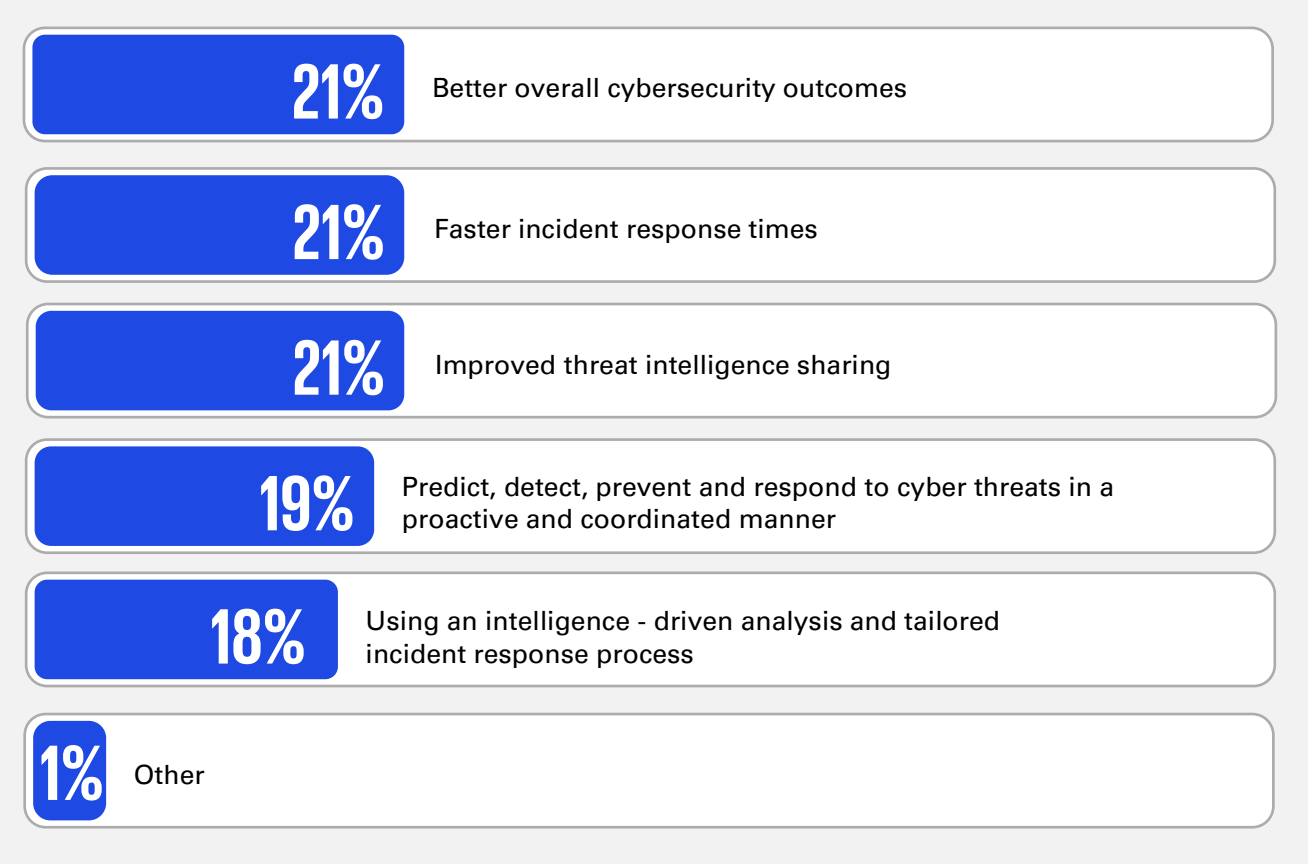


Figure 53: Benefits from setup of cyber fusion centres

Apart from these, cyber GCCs are also focusing on faster response for India specific incidents or investigations.

Methodology

The premise of this report is based on sources of information, meetings and brainstorming sessions undertaken by KPMG in India and DSCI and industry leaders between 2025 and 2026. Information used for comparison amongst the years 2026, 2023, 2020 and 2018 within this report is sourced from previous editions of Secure in India.

Survey

The insights published in this report are primarily based on the response received from the 'Secure in India' survey rolled out to Global Capability Centres (GCCs) in India. Respondents of this survey are GCC leaders, Chief Information Security Officers, Chief Technology Officers, their equivalent or their delegated designates involved in leadership and management functions of global cybersecurity delivery.

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

- Automotive
- Banking
- Construction materials
- Consumer goods
- Energy
- Electronics
- Financial services
- Fintech
- Food and beverage
- Healthcare
- Industrial Engineering
- Insurance
- Investment management
- Life Sciences
- Manufacturing
- Payments
- Retail
- Technology
- Telecommunication
- Transport and travel

Meetings with industry leaders

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

Secondary research

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

Content review

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

Acknowledgements

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

Our special thanks to the advisory panel for their strategic direction, right from conceptualisation to the launch of the report. Our thanks to all the KPMG in India Partners, Directors and colleagues who assisted in survey formulation and completion. We acknowledge the efforts put in by the following team members for publication of this report.

KPMG in India

- Aahana Panigrahi
- Aabha Chandane
- Abhishek Dashora
- Abhishek Kastala
- Aditya Nepalia
- Alka Baranwal
- Annapurna Alladi
- Anil KV
- Anil Singh
- Anish Mitra
- Anupama Atluri
- Apprajit Shrivastava
- Arun Choudhary
- Chhavi Jha
- Harsh Punatar
- Kaushal Yadav
- Krishna K Burugula
- Mallika Chandra
- Namrata Mehta
- Nandhika Praveen
- Nisha Fernandez
- Nishank Hiremath
- Pooja Patel
- Prajakta Talpade
- Pranav Kathale
- Rohan Satish
- Sabi ul Haque Naimi
- Saritha Naga Rana
- Shaleen Sehgal
- Shanu Rajput
- Shreyashi Sengupta
- Sonali Gupta
- Srija Purimetla
- Srijit Menon
- Sriramoju Chaitanya
- Tarini Chandrakar
- Venkatesh R

DSCI

- Vinayak Godse
- Amit Kr Ghosh
- Prasad Deore
- Samriddh Hada

About KPMG 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, Calicut, Chandigarh, Chennai, Delhi, Gandhinagar, Gurugram, Hyderabad, Jaipur, Kochi, Kolkata, Mumbai, Noida, Pune, Raipur, Trivandrum, Vadodara and Vijayawada.

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

About DSCI

Data Security Council of India (DSCI), set up by Nasscom, is a not-for-profit industry body and think tank on data protection, cyber security, and critical technologies in India. DSCI is committed to making cyberspace safe, secure, and privacy-assured, and to advancing critical technologies vital for national security through policy advocacy, thought leadership, capacity building, and outreach initiatives. DSCI engages with the government, regulators, defence, law enforcement agencies, embassies, industry members, and academia to position India as a leader in the global digital ecosystem.

For more information, visit: www.dsci.in

KPMG in India contacts:

Akhilesh Tuteja
Head - Clients and Markets
E: atuteja@kpmg.com

Hemant Jhajhria
National Head of Consulting
E: hemantj@kpmg.com

Gautam Bhattacharya
Head of Technology Consulting
E: gautamb@kpmg.com

Srinivas Potharaju
Partner and Head,
Cyber Security & Technology
E: srinivasbp@kpmg.com

Shalini Pillay
Partner and Head GCC
E: shalinipillay@kpmg.com

DSCI contacts:

Prasad Deore
Vice President, Data Security
Council of India (DSCI)
E: prasad.deore@dsci.in

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/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.

Printed in India. (TL_0826_AC_PT_VR)