

The GCC Is Getting Smarter. Is Security Keeping Up?

A Strategic White Paper on Cybersecurity, Governance, Risk & Compliance, Security Operations, and Agentic AI for Future-Ready GCCs



EXECUTIVE SUMMARY

India has emerged as one of the world's leading destinations for Global Capability Centers, with **2,100+ GCCs** and approximately **2.36 million professionals** supporting global enterprises. GCCs are increasingly responsible for high-value capabilities including AI, cloud, engineering, analytics, cybersecurity and enterprise operations.

This expansion is also increasing the volume and criticality of data, applications, identities and intellectual property managed from GCC environments. Cybersecurity therefore needs to move beyond traditional IT protection toward an integrated model covering **security governance, data governance, AI governance, risk management, compliance, assessment and continuous security operations**.

The global cost of cyber incidents further reinforces the need for proactive security. IBM reported a **USD 4.88 million** global average cost of a data breach in 2024, while the average cost in India reached **INR 195 million**. Organisations using AI and automation extensively in security were associated with an average **USD 2.2 million lower breach cost**.

Future-ready GCCs therefore need to embed security and governance into the GCC lifecycle from strategy and architecture through data, AI, operations and continuous monitoring.

Cybersecurity is no longer an IT function. For modern GCCs, it is a business, governance and resilience capability.

MARKET SNAPSHOT

2,100+

GCCs operating across India.

2.36 million

Professionals employed across India's GCC ecosystem.

\$4.88 million

Global average cost of a data breach in 2024.

₹ 195 million

Average cost of a data breach in India in 2024.

\$2.2 million

Average breach-cost difference associated with extensive AI and automation.

70%

Organisations reporting significant operational disruption following a breach.

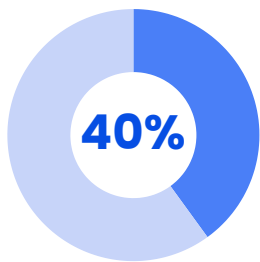
THE EVOLVING CYBERSECURITY & GCC LANDSCAPE

\$10.5 trillion

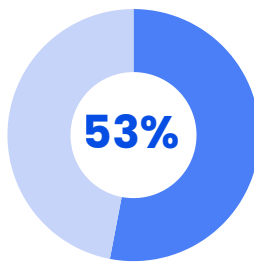
Estimated annual global cybercrime damage.

\$4.88 million

Global average cost of a data breach in 2024



Breaches in **IBM's 2024** study involving data distributed across multiple environments.



Organisations reporting a high level cybersecurity skills shortage in **IBM's 2024 study**.

Key Shift

Organisations are moving from perimeter-based protection toward:

✦ Zero Trust

✦ Cloud-native security

✦ Identity-centric security

✦ Continuous monitoring

✦ AI-powered detection

✦ Automated response

Key Observations

✦ GCCs are becoming critical owners of enterprise security capabilities.

✦ Cybersecurity is evolving from a centralized function into a distributed enterprise capability.

✦ AI and automation are reshaping how threats are detected, investigated and contained.

✦ AI, cloud, cybersecurity, engineering and analytics are becoming core GCC capabilities.

EMERGING CYBERSECURITY CHALLENGES

◆ Expanding cloud and hybrid infrastructure	◆ Third-party and supply-chain risks
◆ AI-powered cyber threats	◆ Increasing regulatory complexity
◆ Ransomware and identity attacks	◆ Cross-border data transfers
◆ AI and data security risks	◆ Shortage of cybersecurity talent

BUILDING A SECURE, GOVERNED & COMPLIANT GCC

A future-ready GCC requires governance across **security, data, AI, risk, and regulatory compliance**. Security Governance establishes the policies, accountability, and architecture needed to protect enterprise operations, covering cybersecurity strategy, security standards, identity and access, third-party security, and performance reporting.

Data Governance ensures enterprise and personal data is properly managed, protected, and controlled throughout its lifecycle through data classification, ownership and stewardship, access controls, privacy, retention, deletion, and cross-border data governance. It also establishes clear accountability and policies for secure, compliant data use.

AI Governance manages risks across AI models, data, automated decisions, and autonomous agents through risk assessment, responsible AI, model governance, data protection, human oversight, fairness, security, and Agentic AI controls. The **NIST AI Risk Management Framework** supports trustworthy AI risk management.

Risk & Compliance aligns business risks with regulatory, security, and operational requirements through risk assessment, compliance monitoring, third-party risk, audit readiness, and reporting. **Security Assessment** identifies vulnerabilities and measures security maturity through vulnerability testing, penetration testing, cloud and AI security assessments, and configuration reviews.

GLOBAL REGULATORY LANDSCAPE

GCCs operating across multiple countries may need to comply with different privacy, cybersecurity, sector-specific and data-transfer requirements.

Selected Regulatory Frameworks

European Union

- ◆ GDPR
- ◆ EU AI Act
- ◆ NIS2 Directive

India

- ◆ Digital Personal Data Protection Act, 2023
- ◆ DPDP Rules, 2025
- ◆ CERT-In cybersecurity directions

United States

- ◆ CCPA/CPRA
- ◆ Sector-specific regulations such as HIPAA and GLBA
- ◆ State-level privacy laws

China

- ◆ PIPL
- ◆ Data Security Law
- ◆ Cybersecurity Law

Brazil

- ◆ LGPD

United Kingdom

- ◆ UK GDPR
- ◆ Data Protection Act 2018

Singapore

- ◆ Personal Data Protection Act (PDPA)
- ◆ Cybersecurity Act

Australia

- ◆ Privacy Act
- ◆ Australian Privacy Principles

For multinational GCCs, compliance is not a one-time certification exercise. It is a continuous process of regulatory mapping, control implementation, monitoring and evidence management

Selected regulatory frameworks are for general reference only. Applicable requirements may vary based on jurisdiction, industry and business operations.

AGENTIC SOC, AGENTIC AI SECURITY & THE FUTURE OF CYBERSECURITY

Security Operations Center (SOC)

A SOC provides continuous visibility into the enterprise security environment and enables organisations to detect, investigate and respond to threats.

Core SOC Capabilities

◆ 24x7 Security Monitoring	◆ SIEM Management
◆ Threat Intelligence	◆ Threat Detection
◆ Incident Response	◆ Threat Hunting
◆ Digital Forensics	◆ Security Analytics

Agentic AI in Cybersecurity

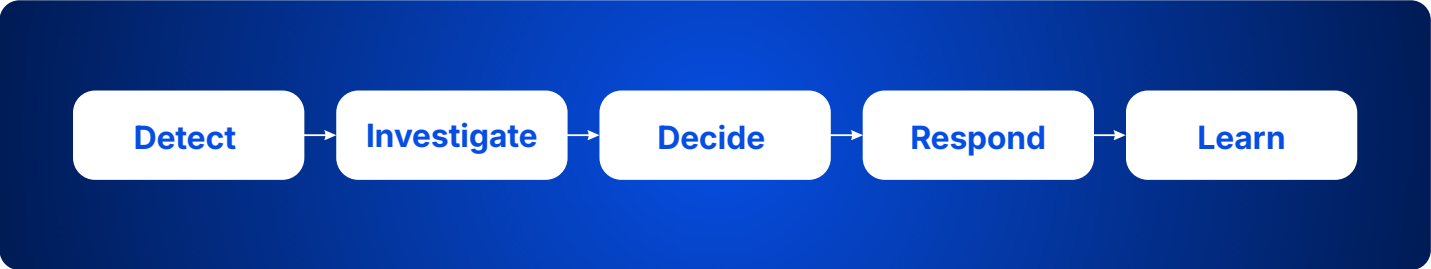
Agentic AI can move cybersecurity from human-led monitoring toward intelligent, semi-autonomous security operations.

Key Use Cases

◆ Automated threat detection	◆ Incident investigation
◆ Vulnerability prioritization	◆ Automated response
◆ Compliance monitoring	◆ Security workflow orchestration
◆ Threat intelligence analysis	◆ Predictive risk analysis

Agentic Security Model

Human oversight remains important for high-impact security decisions, particularly where automated actions could affect critical systems or sensitive data.



Future Cybersecurity Outlook — 2026–2030

Key Trends & Capabilities

◆ AI-native Security Operations	◆ Agentic SOC
◆ Zero Trust Architecture	◆ Continuous Compliance
◆ Cloud-Native Security	◆ Identity-Centric Security
◆ AI Security & Model Protection	◆ Data-Centric Security
◆ Automated Risk Management	◆ Privacy-Enhancing Technologies

Key Message

The next generation of cybersecurity will combine human expertise, intelligent automation and continuous governance to create adaptive and resilient security operations.

FROM GOVERNANCE TO EXECUTION

How SNS Square Supports Secure GCCs

SNS Square helps enterprises translate cybersecurity strategy, governance and risk management into scalable operational capabilities.

Cybersecurity Strategy & Advisory

- ◆ Cybersecurity Roadmap
- ◆ Security Architecture
- ◆ Security Governance
- ◆ Cyber Resilience Strategy

Governance, Risk & Compliance

- ◆ GRC Advisory
- ◆ Regulatory Mapping
- ◆ Compliance Readiness
- ◆ Risk Assessments

Data & AI Governance

- ◆ Data Governance Frameworks
- ◆ Data Privacy & Protection
- ◆ AI Governance
- ◆ AI Risk Assessment

Security Assessment

- ◆ Vulnerability Assessment
- ◆ Penetration Testing
- ◆ Cloud Security Assessment
- ◆ AI Security Assessment

Security Operations

- ◆ 24x7 SOC
- ◆ SIEM
- ◆ Threat Intelligence
- ◆ Incident Response

Agentic AI Security

- ◆ AI-powered Threat Detection
- ◆ Automated Incident Response
- ◆ Compliance Automation
- ◆ Security Workflow Orchestration

INDUSTRY PERSPECTIVE: ALBERTSONS GCC, INDIA

Albertsons' expansion of its capabilities in India reflects the broader trend of global enterprises leveraging India to build technology, digital and enterprise capabilities.

Key Observations

- ◆ Access to India's technology and digital talent ecosystem.
- ◆ Growing focus on AI, cloud and digital engineering capabilities.
- ◆ Ability to support global business operations through a scalable GCC model.
- ◆ Increasing importance of cybersecurity and governance as GCC responsibilities expand.



Key Industry Insight

The emergence of enterprise GCCs in India demonstrates how global organisations are moving beyond traditional delivery models toward strategic technology and capability centres. As these centres gain greater ownership of data, AI and critical business processes, cybersecurity and governance become foundational capabilities rather than supporting functions.

Conclusion

Global Capability Centres are becoming strategic engines for enterprise technology, innovation, data and AI. This transformation creates significant opportunities, but also introduces new cybersecurity, privacy, regulatory and operational risks.

A future-ready GCC must therefore move beyond traditional cybersecurity toward an integrated model encompassing:

Security Governance | Data Governance | AI Governance | Risk & Compliance | Regulatory Intelligence | Security Assessment | SOC | Agentic AI

Organisations that embed these capabilities into the GCC lifecycle can strengthen resilience, improve regulatory readiness, protect critical data and accelerate secure digital transformation.

Connect With Us

Whether you are establishing a new GCC, strengthening cybersecurity governance, managing regulatory requirements or accelerating AI-led transformation, SNS Square can help build the capabilities required for secure and sustainable growth.

Visit us at www.snssquare.com
or write to us at info@snssquare.com

