A 9.9 GROUP PUBLICATION
www.cisoforum.in
cisoforum-in

JANUARY 2026
SUPPLEMENT OF CIO&LEADER

CISOFORUM

Security For Growth And Governance

How AI Is Redefining the CISO Mandate in 2026

Amal Krishna, Executive Director and CISO at ONGC, on how AI risk, evolving data protection mandates, and fragmented governance are reshaping the CISO agenda. PG. 20

Next CISO Awards 2025. PG. 09

CISO Samman. PG. 16

CIO&LEADER studiotalks

CIO&LEADER STUDIOTALKS—
WHERE TECHNOLOGY MEETS THE SPOTLIGHT!

CIO&Leader proudly presents StudioTalks—a premium platform where India's most influential CIOs and CTOs take center stage. Captured with high-production aesthetics, sleek visuals, and dynamic backdrops, StudioTalks transforms leadership insights into an engaging cinematic experience, and brings India's most influential CIOs and CTOs into the spotlight.
This exclusive series explores visionary leadership, emerging technologies, and strategic transformation—all presented in a format that blends deep insights with the visual polish of a professional studio production.

WHY JOIN STUDIOTALKS?

Engage in powerful conversations that shape the future of enterprise IT.

Share your expertise in a high-impact, TV-style format.

Be featured among India's top technology leaders.

Be the voice of transformation. Be part of CIO&Leader StudioTalks.

SECURE YOUR SPOT NOW!

For more information
Jatinder Singh
Executive Editor - Enterprise Tech
jatinder.singh@9dot9.in, +919718154231

For Business Proposal
Hafeez Shaikh
National Sales Head, B2B Tech,
hafeez.shaikh@9dot9.in, +91 9833103611

Follow us: @CIOandLeader

The new talent equation

2026 MARKS an inflection point for Indian CISOs. As enterprises accelerate AI adoption, comply with the DPDP Rules 2025, and India's AI Governance Guidelines, and expand their digital footprint across sectors, cybersecurity is no longer just a technical function—it's a strategic imperative. Yet this transformation arrives amid an acute staffing crisis that threatens to outpace even the most well-resourced security teams.

The convergence of AI, regulation, tool proliferation, and an ever-expanding digital footprint is intensifying pressure on cybersecurity leaders. Teams now require expertise in prompt injection risks, model governance, and privacy-by-design—skills rarely found in traditional security hires. Compliance demands professionals who can interpret DPDP obligations through both legal and technical lenses while communicating risk effectively to boards. Security tool sprawl breeds operational fatigue without corresponding headcount growth, and the attack surface—fueled by cloud, IoT, and third-party ecosystems—continues to widen. Although CISOs urgently need AI risk analysts, privacy engineers, and cloud-native architects, talent scarcity and burnout severely constrain hiring.

CISOs must respond not by chasing headcount, but by re-imagining how talent creates value. Prioritize up-skilling existing staff in AI and regulatory domains, and automate tier-1 tasks responsibly to free capacity for strategic work. Embed compliance into product and engineering workflows—not just leave it to security teams. Most critically, move beyond siloed SOC expansion toward cross-functional "resilience pods" that integrate security into business velocity.

In this new era, staffing success will no longer be measured by team size—but by strategic alignment, adaptability, and the ability to enable secure innovation. For CISOs, talent is not a cost; it is the cornerstone of enterprise resilience. ■

"In this new era, staffing success will no longer be measured by team size—but by strategic alignment, adaptability, and the ability to enable secure innovation."

R. Giridhar
Group Editor, B2B Tech
r.giridhar@9dot9.in

CONTENTS JANUARY 2026

COVER STORY

20-23
How AI is redefining the CISO mandate in 2026

Amal Krishna, Executive Director and CISO at ONGC, explains how AI risks, evolving data protection, and fragmented governance are reshaping the CISO's agenda in 2026

Cover Design by:
Manish Kumar

Please Recycle This Magazine And Remove Inserts Before Recycling

NEWS & VIEWS

FEATURE

INSIGHTS

OPINION

INTERVIEW

CISOFORUM
Security For Growth And Governance
www.cisoforum.in

MANAGEMENT
Managing Director: **Dr Pramath Raj Sinha**
Printer & Publisher / CEO & Editorial Director (B2B Tech): **Vikas Gupta**
COO & Associate Publisher (B2B Tech): **Sachin Nandkishor Mhashilkar**

EDITORIAL
Group Editor: **R Giridhar**
Editor: **Jatinder Singh**
Senior Correspondent & Editorial Coordinator – CISO Forum: **Jagrati Rakheja**
Principal Correspondent: **Musharrat Shahin**

DESIGN
Creative Director: **Shokeen Saifi**
Assistant Manager - Graphic Designer: **Manish Kumar**

SALES & MARKETING
Senior Director - B2B Tech: **Vandana Chauhan**
Head - Brand & Strategy: **Rajiv Pathak**

National Sales Head - B2B Tech: **Hafeez Shaikh**
Reginal Sales Head - North: **Sourabh Dixit**
Senior Sales Manager - South: **Aanchal Gupta**

COMMUNITY ENGAGEMENT & DEVELOPMENT
Head - Databases: **Neelam Adhangale**
Senior Community Manager: **Vaishali Banerjee**
Senior Community Manager: **Reetu Pande**
Senior Community Manager: **Snehal Thosar**

OPERATIONS
General Manager - Events & Conferences: **Himanshu Kumar**
Senior Manager - Digital Operations: **Jagdish Bhainsora**
Manager - Events & Conferences: **Sampath Kumar**
Senior Producer: **Sunil Kumar**

PRODUCTION & LOGISTICS
Senior Manager - Operations: **Mahendra Kumar Singh**

For editorial queries write to:
editor@cioandleader.com

For sales/business queries write to:
responses@cioandleader.com

OFFICE ADDRESS
9.9 GROUP PVT. LTD.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published, Printed and Owned by 9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
Published and printed on their behalf by
Vikas Gupta. Published at 121, Patparganj,
Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091, India. Printed at G. H. Prints Private Limited, A-256 Okhla Industrial Area, Phase-I, New Delhi - 110020.

Editor: **Vikas Gupta**

Dr. Yusuf Hashmi joins Dell Technologies UAE as chief cybersecurity advisor

Dr. Yusuf Hashmi has joined **Dell Technologies UAE** as **Chief Cybersecurity Advisor,** bringing deep expertise in cyber resilience, security strategy, and transformation across enterprise and government sectors. In this role, he will advise CXOs and CISOs on modernising architectures, Zero Trust adoption, AI-enabled security operations, hybrid and multi-cloud protection, cyber recovery, and ransomware resilience, while driving executive engagement and cybersecurity thought leadership.

Sameer Ratolikar elevated to group head & CISO at HDFC Bank

Sameer Ratolikar has been elevated to **Group Head & Chief Information Security Officer** at **HDFC Bank,** marking a key milestone in his cybersecurity leadership journey. With over 27 years of experience, including more than a decade at HDFC Bank, he has led enterprise security strategy, cyber resilience, and regulatory compliance, reinforcing the bank's commitment to robust cyber governance.

V V Subba Raju joins iBASIS as CISO

V V Subba Raju has assumed the role of **Chief Information Security Officer** at **iBASIS,** strengthening its cybersecurity and risk leadership. He will lead enterprise-wide security strategy, architecture, and compliance. Previously at NTT DATA Business Solutions and CallHealth, he brings deep experience across global IT operations, cybersecurity, and enterprise risk management to support iBASIS's expanding digital footprint.

Rajkumar Punna joins Vistaar Financial Services as CISO

Rajkumar Punna has been promoted to **Chief Information Security Officer** at **Vistaar Financial Services,** marking a key leadership milestone. He will lead enterprise information security strategy, cyber resilience, governance, risk and compliance, and regulatory adherence. With prior leadership roles at Vistaar, Kinara Capital, NTT Ltd., and Manappuram Finance, he brings deep expertise across cybersecurity, cloud security, and IT operations.

Abhishek N. joins Avendus as group CISO

Abhishek N. has joined **Avendus as Group Chief Information Security Officer,** where he will lead enterprise-wide cybersecurity strategy, governance, risk management, and regulatory compliance. Previously at SBI Mutual Fund, Tata Technologies, and eClerx, he brings deep expertise across SOC operations, application and cloud security, DevSecOps, GRC, and board-level cyber risk management to strengthen Avendus' cyber resilience.

Anshuman Pund joins SBM Bank (India) as CISO

Anshuman Pund has joined **SBM Bank (India)** as **Chief Information Security Officer,** leading enterprise information security, cyber risk, compliance, and security operations. Previously CISO at Suryoday Small Finance Bank, and with roles at NPCI, Tech Mahindra, and IDBI Intech, he brings deep expertise across banking, payments, governance, SOC operations, and large-scale security transformation to strengthen the bank's cyber resilience.

Pavankumar Shukla takes over as head of information security & DPO at IDfy

Pavankumar Shukla has joined **IDfy** as **Head of Information Security & Data Protection Officer,** leading security, privacy, and compliance strategy. With nearly two decades of experience, including leadership roles at Delhivery, TIFIN, and LTI, he brings deep expertise across cybersecurity, GRC, data privacy, and enterprise risk to strengthen IDfy's digital trust and identity intelligence platform.

Shivaji Manwadkar promoted to chief security officer at SBFC Finance

Shivaji Manwadkar has been promoted to **Chief Security Officer** at **SBFC Finance,** reflecting the organisation's focus on strengthening security leadership. In this role, he will oversee enterprise security strategy, regulatory compliance, and cyber and operational frameworks. With experience across SBFC Finance, HDFC Bank, and earlier IT roles, he brings strong domain expertise to support the company's digital growth.

Ransomware recovery climbs — but AI-driven attacks are redefining cyber risk

Confidence in recovery from ransomware exploits is rising, but AI-driven attacks and supply chain risks are exposing dangerous gaps in real cyber resilience.

By **CISO Forum** | editor@cisoforum.com

AS 2026 approaches, a new tension is shaping the global cybersecurity landscape: organizations are more confident than ever in their ability to recover from ransomware, yet they face a rising wave of sophisticated, AI-powered attacks that threaten to outpace their preparedness. The OpenText Cybersecurity 2025 Global Ransomware Survey highlights this paradox, revealing a digital world where optimism and vulnerability now coexist uneasily.

Confidence vs. reality

The survey finds that 95% of organizations believe they can recover from ransomware, a dramatic vote of confidence. Yet reality tells a different story—only 15% of attacked organizations recovered their data entirely, and 2% recovered none at all. This gap signals that strong sentiment may not be matched by true resilience, particularly as threat actors adopt advanced AI-driven techniques.

"Resilience isn't just about recovery—it's about anticipating and adapting to threats."

AI widens the threat surface

AI boosts productivity but heightens cyber risk. While 88% allow GenAI, fewer than half have policies. 52% report AI-driven attacks, 44% deepfakes, leaving organizations—especially SMBs—unprepared amid rapid innovation.

Supply chain attacks surge

Beyond AI, the report flags vendor-driven risks: two in five faced ransomware last year; 25% via suppliers. Over 45% paid ransoms, 30% spent $250,000+, revealing cyber extortion's high cost globally.

Cybersecurity becomes a board priority

Ransomware has shifted from technical risk to boardroom priority. 71% of leaders rank it top-three threat. Companies respond with cloud security, backups, and training, signaling resilience as a strategic priority.

The road ahead

Ransomware in 2025 is evolving, not just escalating. While organizations feel prepared, AI-powered attacks are faster and deceptive. Cybersecurity resilience demands balancing innovation with governance, anticipating threats before they strike. ■

Why AI agents demand a new approach to identity security

AI agents expose identity blind spots, forcing enterprises to replace static privileges with continuous, risk-aware identity security.

By **CISO Forum** | editor@cisoforum.com

THE EXPONENTIAL rise of artificial intelligence agents is fundamentally reshaping enterprise security paradigms. As organizations embrace AI-driven automation, a critical vulnerability emerges: non-human identities (NHIs) now operate with superhuman speed and privileged access across systems, creating unprecedented security challenges that traditional identity management frameworks cannot address.

The standing privilege problem

According to IDC projections, the identity security market will nearly double from $29 billion in 2025 to $56 billion by 2029, reflecting the urgency with which enterprises must adapt. This growth is driven by the proliferation of AI agents, service accounts, and machine identities that dynamically access sensitive data, applications, and compute resources across distributed cloud environments.

"When AI agents operate autonomously with these permanent access rights, organizations face continuous exposure."

The fundamental issue lies in legacy access models built on static policies and standing privileges that persist despite changing threats. When autonomous AI agents retain permanent access, organizations face continuous exposure, enabling lateral movement, data exfiltration, or malicious actions before security teams can intervene.

Moving to continuous ildentity

CrowdStrike's recent acquisition of SGNL signals a strategic shift toward "Continuous Identity," where access is dynamically granted or revoked based on real-time risk. By eliminating standing privileges and continuously evaluating identity, device posture, and behavior, this model redefines access security.

For Indian CISOs driving digital transformation, the message is clear: identity security must move beyond static roles and periodic reviews to continuous, risk-aware authorization. As agentic workforces grow, every AI agent becomes a privileged identity needing protection.

The way forward requires integrating identity threat detection and response with privileged access management, enabling just-in-time access, continuous evaluation, and real-time threat intelligence across hybrid environments. ■

AI-powered cyberattacks will mimic humans in 2026—and your security might not notice

AI-driven cyber attacks will bypass traditional detection and force a shift to cognitive security defenses.

By **CISO Forum** | editor@cisoforum.com

CYBERSECURITY FIRM Seqrite has issued a stark warning: 2026 will usher in an era of "cognitive threats"—sophisticated cyberattacks that use artificial intelligence to mimic human behavior with alarming accuracy.

According to Seqrite's India Cyber Threat Report 2026, prepared by researchers at India's largest malware analysis facility, these AI-augmented attacks represent a fundamental shift from traditional malware-based threats. The new generation of cyberattacks will combine intelligence with automation, creating threats that can think, adapt, and deceive in ways never seen before.

"2026 will usher in an era of 'cognitive threats'—sophisticated cyberattacks that use artificial intelligence to mimic human behavior."

Hyper-personalized phishing takes center stage

The most concerning development involves AI-generated digital twins that replicate writing, speech, and video, bypassing human and automated defenses and rendering traditional phishing obsolete. The threat extends to mobile banking, where AI-driven malware autonomously fills credentials, defeats biometrics, and executes fraud.

AI becomes both weapon and target

State-backed and criminal groups will deploy AI across attacks, from vulnerability discovery to real-time malware evolution, evading detection and mimicking other groups. Alarmingly, attackers will target AI itself, poisoning training data to trigger misclassifications and convert enterprise AI platforms into data-theft tools.

Defense requires new thinking

Seqrite urges organizations to move from reactive security to cognitive resilience, prioritizing AI-driven predictive intelligence, faster patching, Zero Trust, AI model integrity validation, and assume-breach frameworks to outpace advanced adversaries. ■

NextCISO 2025: Identifying India's next generation of cybersecurity leaders

NextCISO 2025 applies a scientifically grounded, jury-governed evaluation framework—spanning psychometric testing, referee feedback, and expert interviews—to recognise emerging leaders in cybersecurity.

NextCISO Winners Devarshi Jana, First America | **Edward Antony,** Integra Software Services | **Avanik Jain,** Vedanta (STL Digital) | **Anand Kumbhani,** ICICI Securities | **Akash Gajre,** Mahindra Finance | **Bhushan Hukeri,** Rapid Circle | **Arun Thanga Pandiyan Rajendran,** Scienaptic Systems | **Balasundaran Ranjan,** Quest Global Engineering Services being felicitated by **Arun Gantayat,** Kaspersky & **Jaydeep Singh,** Kaspersky

THE 7th edition of the NextCISO awards commenced in August 2025 with a call for applications. Prospective applicants, aspiring to become Chief Information Security Officers (CISOs) were invited to self-nominate themselves for the award selection process through a series of social media posts, print advertisements and emails.

In the first stage, all award aspirants had to complete the NextCISO application form—and provide detailed personal and professional information, including education, work history, and technical skills. By mid-September 2025, when the applications closed, there were 151 aspirantswho had registered for the process.

All applicants had to nominate supervisors and referees who could support their application for the award. The NextCISO team obtained more than 140 confidential evaluations and recommendations from referees.

In the second stage, applicants took two psychometric tests: Personality Profile test and Emotional Quotient test. The tests were administered online by France-based Central Test International. Every applicant who completed the tests received a free copy of the detailed assessment reports for personal reference and self-development.

As in past years, the NextCISO awards program draws on the knowledge and support of the CISO community.Twenty-one senior executives who comprise the jury of the NextCISO2025 awards, collectively represent many decades of experience in IT, cybersecurity and corporate management. The jury panel members discussed and decided on the award winner selection process—and conducted detailed interviews of shortlisted applicants. The jury also approved the final list of award winners.

A total of 46 applicants who passed scrutiny were interviewed and evaluated by two senior CISOs.The scores assigned to all candidates in every stage of the selection process were input into a proprietary scoring model that assigns carefully calibrated weights to various factors. The output of scoring model is used to create the final list of award recipients.

The final list of 24 NextCISO2025 award recipients, was reviewed and approved by the jury. The award presentation ceremony was held on 21 November 2025 at Athiva Resort & Spa, Khandala,where each winner was felicitated with a trophy and certificate of recognition.

NextCISO Winners Vinay Raymagiya, Godrej Industries | **Raghav Grandhi,** Spandana Sphoorty Financial | **Sonu Vashist,** Crystal Crop Protection | **Paramanand Shinde,** Sanghvi Movers | **Sachin Chopade,** Jio Platforms | **Vinod R,** Sutherland being felicitated by **Anand Jethalia,** Microsoft

To ensure that the selection of the NextCISO awardees is completely fair and unbiased, no member of the CISO Forum editorial team was involved in the selection or elimination of candidates, nor are editors and staff of the CISO Forum a part of the jury panel.

Psychometric tests

All applicants for the NextCISO awards take two psychometric evaluations—a personality test and an emotional quotient test. These tests are administered by Paris-based Central Test. The results of the tests are factored into the total evaluation of the candidate. All candidates who take the psychometric evaluations receive personalized reports that can be used for self-development.

The Central Test Personality Inventory for Professionals (CTPI-R) test provides an assessment of work-related personality traits that play a crucial role in performance. According to the test designers, CTPI-R conforms to the standards of scientific validation set out by the International Test Commission, and the American Psychological Association.

The workplace competencies are defined as "clusters of knowledge, skills and attitudes that are predictive of superior performance in a given job". According to Central Test, the competency scores in the CTPI-R are not a 'direct assessment' of competencies but an 'assessment of proximity' of the test taker to the profile of others who have demonstrated a high level of that specific competency.

NextCISO Winners **Koushik Dutta,** Tech Mahindra | **Kulbhushan Upadhyay,** TCIL | **Mahesh Toshniwal,** Jindal Steel | **Nitin Kumar Chauhan,** Tanla Platforms | **Kamal Kant Gupta,** Luminar Technology Services | **Kabilan RK,** Tamilnad Mercantile Bank | **Radhika Natarajan,** BHEL Electronics Division | **Kaushik Das,** Star Cement being felicitated by **Joshua Kathiravan,** Claroty

NextCISO 2025 jury members Dinesh Shrimali, Tata Steel | **Pawan Chawla,** Tata AIA Life Insurance | **Yusuf Hashmi,** AMS International UAE | **Pradipta Patro,** KEC International | **Divan Raimagia,** Adaan Green Energy | **Satyavrat Mishra,** Godrej Industries | **Himachal Jothinarasimhan,** Ashok Leyland | **Ninad Varadkar,** Edelweiss Financial Services feliciated by **Vikas Gupta,** 9.9 Group

The assumption behind this method of evaluation is that people with similar profiles will be more likely to exhibit similar abilities. As the scores are derived from an assessment of proximity to an ideal profile, they give an indication of the extent to which the candidate is psychologically inclined towards high performance on a specific competency. The score on each dimension of competency also provides an indication of the extent to which the person is trainable on each competency.

The Emotional Quotient test, assesses the ability to perceive, understand and manage one's own emotions and those of others. This is an essential leadership requirement in current times.

The test participants are evaluated across 19 parameters covering intra-personal and inter-personal emotional attributes. The test also evaluates Leadership Suitability Fit on five dimensions—adaptability, leadership, personal development, self-assertion and self-awareness.

Workplace competencies

According to Central Test, the CTPI-R test has been standardized on a large international group of working managerial professionals. The test uses a continuous scale of 0 to 100% to deduce 24 competencies that are relevant in the workplace. The conclusions are based on statistical studies and theoretical models.

The overall analysis of scores of all NextCISO applicants across 24 groups of workplace competencies (Decision Making, Perspective Taking, Networking, Innovation & Creativity, strategic Planning, Stress Management, Quality Orientation, Sense of Duty etc.) indicates that Winner group scored higher on Innovation & Creativity and Stress Management, but low on Quality Orientation and Sense of Duty.

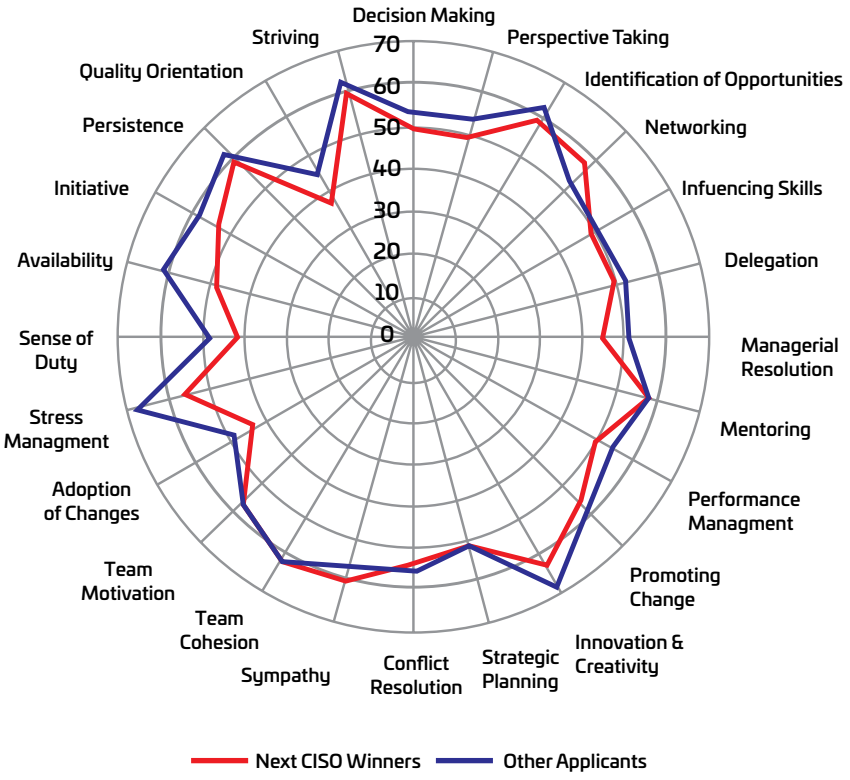
Personality profile

The CTPI-R test provides an assessment of work-related personality traits that play a crucial role in performance. The test measures work personality across 19 dimensions. These dimensions are organized into two groups: People Management and Change Management.

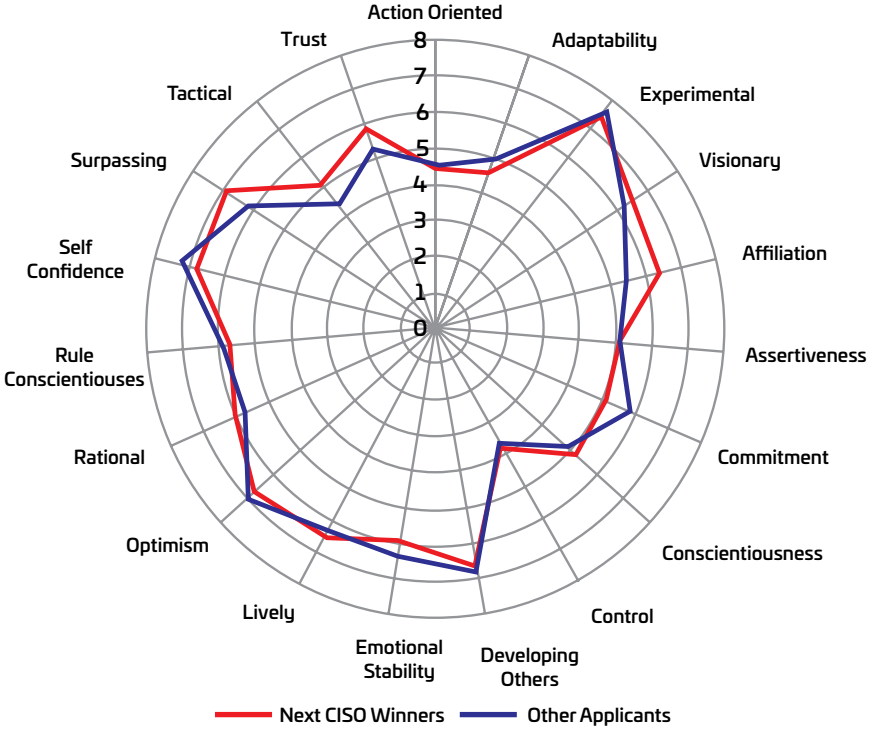
The test results are reported on a scale of 0 to 10, with 0 implying a low level and 10 implying a high level of conformance to the behavioural characteristic.

Both the NextCISO winner group and the other applicant groups registered relatively lower scores on Control and Tactical dimensions. A clear divergence between the two groups emerged across selected behavioural factors, particularly Affiliation, Commitment, Surpassing, and Tactical attributes, where the winner group displayeda distinct profile compared to other applicants, indicating differentiated motivational and executional orientations.

Workplace competetencies



Personality profile



Emotional skills

The Emotional Quotient test assesses the ability to perceive, understand and manage one's own emotions and those of others. The participants are measured across 15 parameters, organized into two groups (intra-personal and inter-personal).

While both NextCISO winner and other applicant groups exhibit similar emotional skills, the winner group scored high on Resilience but low on Tactfulness and Empathy. However, Other applicants scored higher on dimensions like Self Regard and Flexibility.

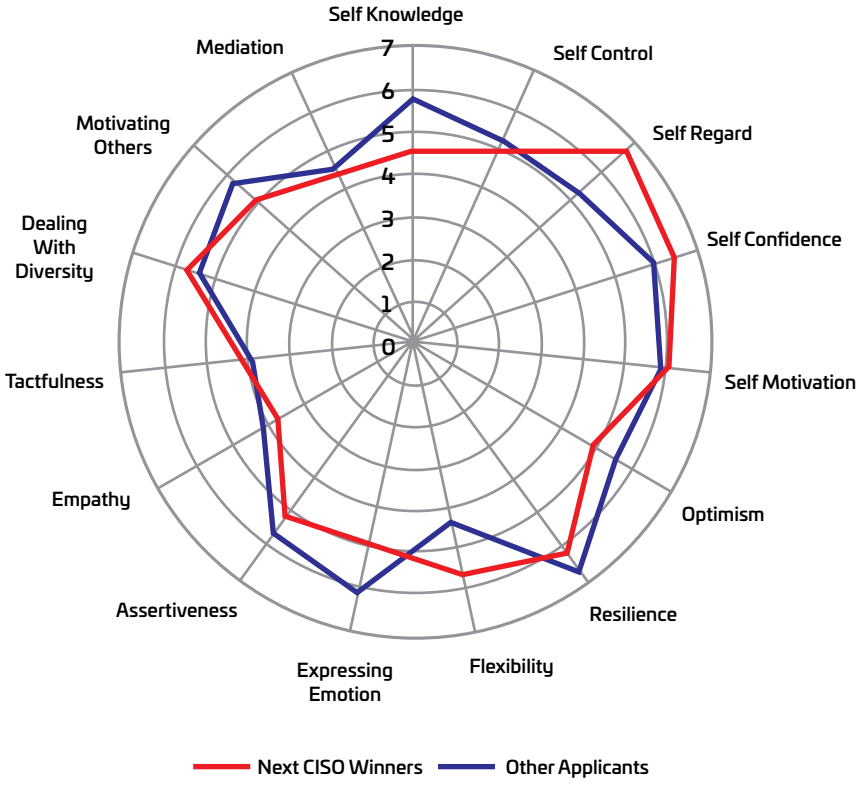
"NextCISO 2025 applies a grounded, jury-governed evaluation framework—spanning psychometric testing, referee feedback, and expert interviews—to recognise emerging leaders in cybersecurity."

Leadership suitability fit

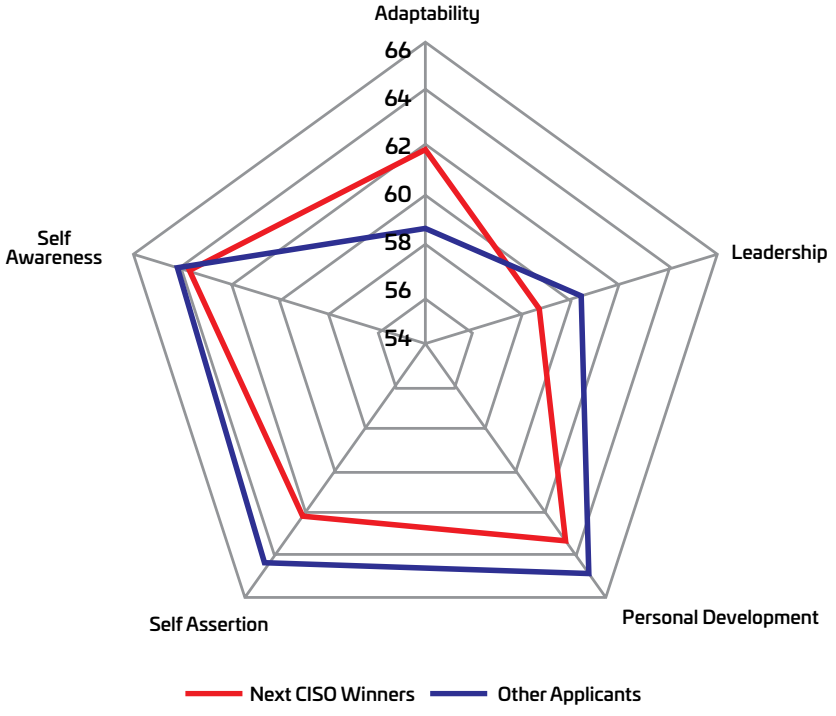
Leadership Suitability Fit evaluates applicants on five dimensions—adaptability, leadership, personal development, self-assertion and self-awareness.

The NextCISO winners did a little better than other applicants across all dimensions, there was a noticeable difference on the Adaptability factor, and very little difference on self-awareness. Winner group exhibited higherscore on Self Assertion and Personal Development. ■

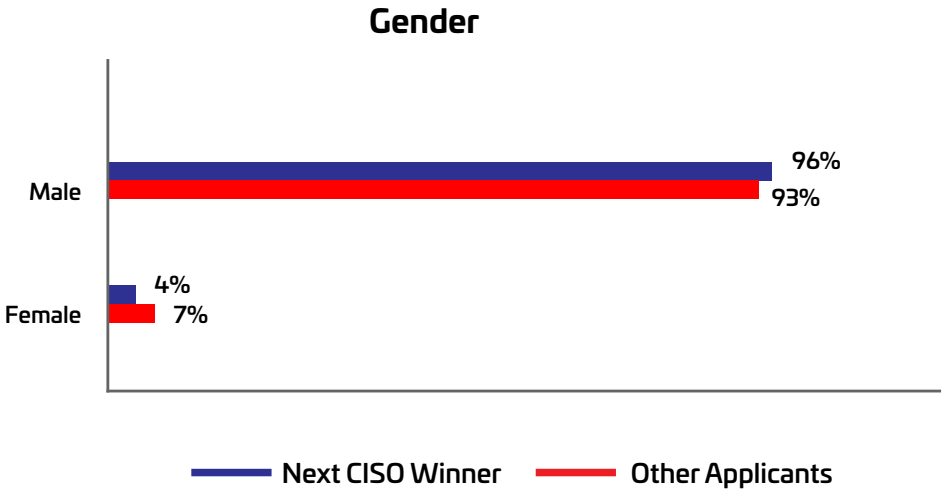
Emotional skills



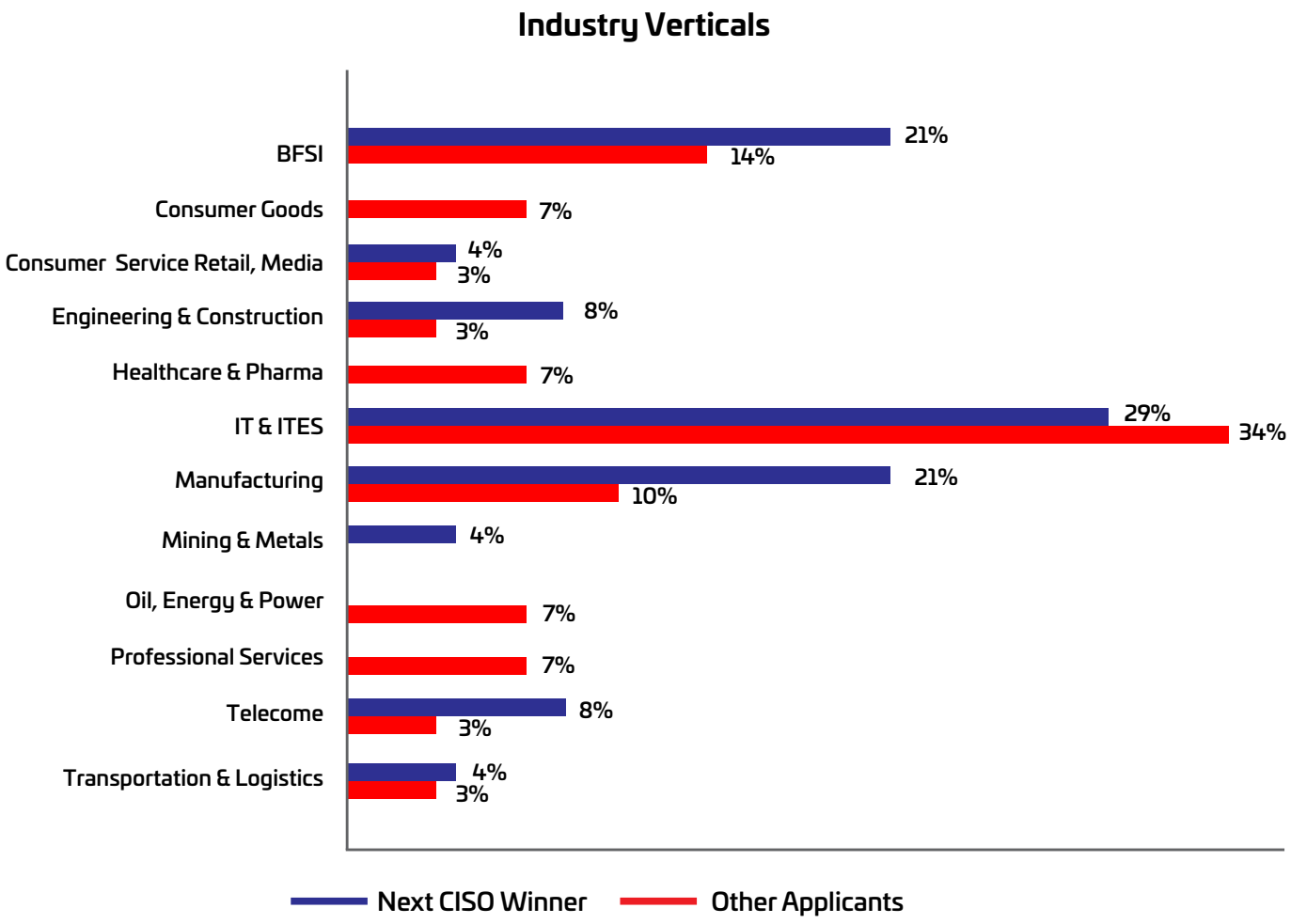
Leadership Suitability Fit



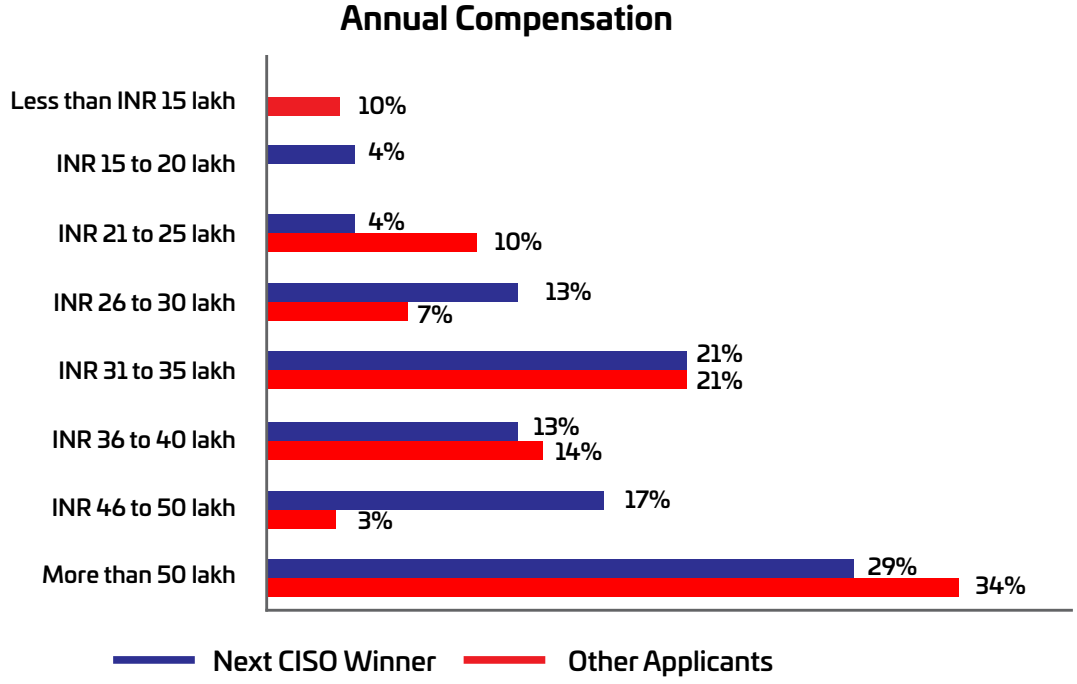
Only 4% of Next CISO winners are female



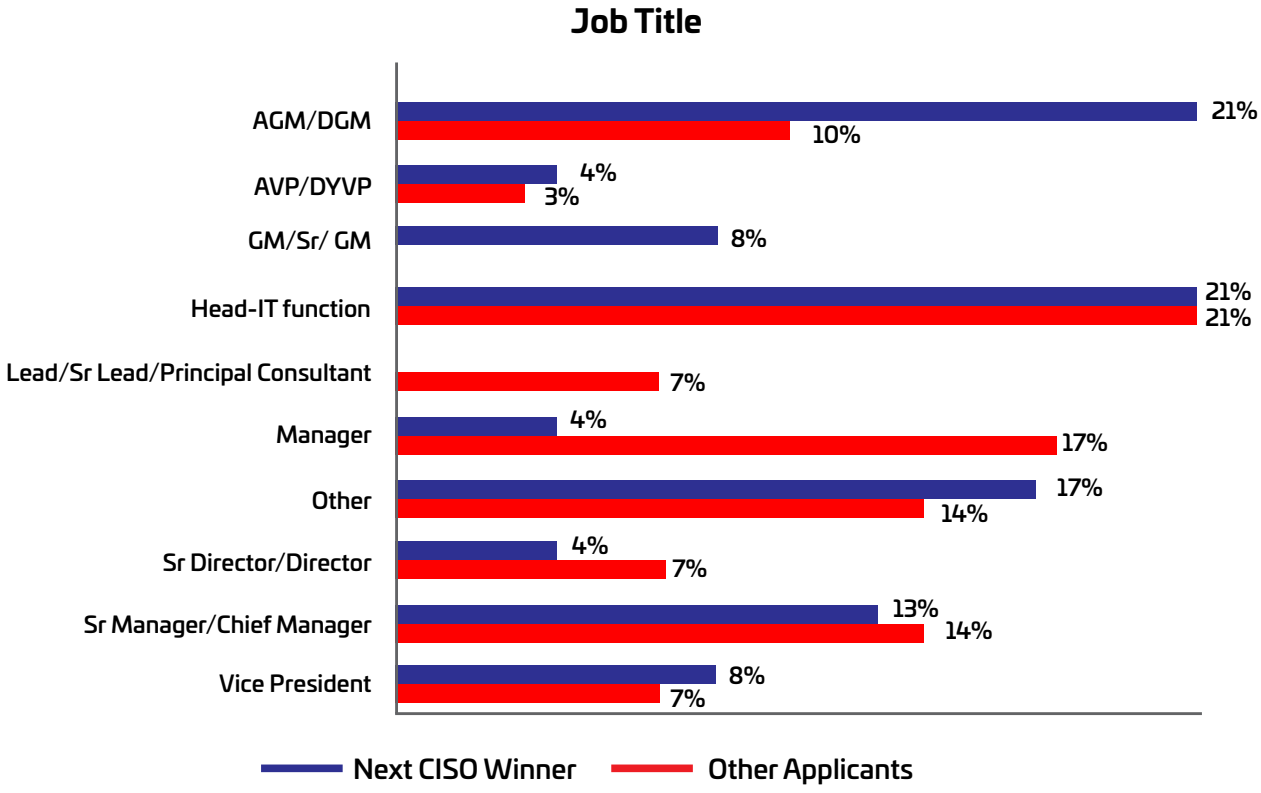
71% of the winners are from the service industry, BFSI and manufacturing



58% of the winners receive an annual compensation exceeding INR 35 lakhs



42% of those selected are senior managers (Head - IT, AGM and DGM)



CISO Samman 2025: Celebrating leadership at the frontlines of cybersecurity

CISO Samman recognises seasoned CISOs who have built resilient, trusted, and future-ready security ecosystems for India's most critical enterprises and digital infrastructure.

The selection committee members are:

Brijesh Datta
Executive Vice President and CISO, Jio Platforms

Dr Durga Prasad Dube
Executive Vice President, Reliance Industries Limited

Rajesh Thapar
Chief Information Security Officer, National Stock Exchange

Sameer Ratolikar
Group Head & CISO, HDFC Bank

Dr. Sandeep K. Shukla
Director, International Institute of Information Technology Hyderabad

Sunil Varkey
Cybersecurity Consultant

Uday Deshpande,
Chief Information Security Officer, Larsen & Toubro

THE CISO The CISO Samman is an initiative to honor distinguished Chief Information Security Officers (CISOs) in Indian enterprises to recognize their substantial contributions to the profession of cybersecurity, and their role in community initiatives to strengthen IT security in organizations. Unlike traditional awards, the CISO Samman is not about conferring accolades but paying tribute to experienced CISOs.

The CISO Samman process uses a jury driven nomination system to ensure that the selection of honorees is based on merit. An initial list of prospective nominees is prepared for consideration by the committee. The preliminary criteria include at least 20 years of professional experience, with at least 3 years served in a CISO role. For Public Sector Unit (PSU) nominees, the jury has the option to relax this criterion and consider IT and risk management experience prior to the current role. All nominees must currently serve as CISOs in India. Retired individuals, those in non-CISO roles, past CISO Samman honorees, or CISOs based outside India are not eligible for consideration.

CISO Samman 2025 recipient **Murlidhar Nambiar,** Group Chief Information Security Officer, State Bank of India being felicitated by **Sachin Mhashilkar** & **Jatinder Singh**.

CISO Samman 2025 recipient **Jacxine Fernandez,** Vice President – Information Security, ICT Governance & Revenue Management, Bangalore International being felicitated by **R. Giridhar.**

The jury evaluates nominees based on their professional experience and achievements, demonstrated leadership in cybersecurity, strategic impact on their organizations, and contributions to the cybersecurity community (including mentoring, education, participation in expert panels and advisory committees, etc.).

The jury for the CISO Samman 2025 comprised of eminent CISOs, past CISO Samman honorees, and-renowned cybersecurity experts who bring their extensive expertise, experience and insights to the selection process.

CISO Samman 2025 recipient **Agnelo D'Souza**, Chief Information Security Officer, Adani Airport Holdings being felicitated by R**ajesh Thapar,** Chief Information Security Officer, National Stock Exchange of India & **Uday Deshpande,** Chief Information Security Officer, Larsen & Toubro

Agnelo D'Souza

Chief Information Security Officer, Adani Airport Holdings

Agnelo D'Souza is a distinguished cybersecurity leader with over two decades of experience driving large-scale security transformations across critical sectors. As the CISO of Adani Airport Holdings, he leads the cybersecurity strategy for one of India's most complex and high-availability infrastructure ecosystems, ensuring resilience across airport operations, passenger systems, and digital platforms.

Before joining Adani Airports, Agnelo spent 20 years with Kotak Mahindra Bank, where he played a pivotal role in building one of the most robust banking security frameworks in the country—balancing innovation with compliance and customer trust. Known for his visionary approach to data protection, risk governance, and incident response, he has consistently championed proactive defense and cultural awareness around cybersecurity. His leadership continues to shape the evolving landscape of digital trust in India's critical infrastructure ecosystem.

Jacxine Fernandez

Vice President – Information Security, ICT Governance & Revenue Management, Bangalore International Airport

Jacxine Fernandez is an accomplished cybersecurity and risk management leader with a distinguished global career spanning the Middle East, Africa, and India. As Vice President at Bangalore International Airport, he is the strategic force behind enterprise-wide cybersecurity, ICT governance, and revenue management for one of India's busiest and most critical aviation hubs. He has led the transformation of security operations into a modern MDR-driven program, implemented a comprehensive multi-year cybersecurity roadmap, and strengthened IT-OT-IoT security across more than 15,000 stakeholders, ensuring resilience in a high-stakes, mission-critical environment.

Previously, as Group CISO at Adani and during senior leadership roles at Zain Group and Airtel Africa, he established integrated security frameworks, pioneered cloud-first transitions, and unified cybersecurity governance across diverse geographies. A visionary, process-driven leader with proven capability in crisis management, business continuity, and technology governance, he exemplifies excellence in securing complex digital ecosystems and empowering business-aligned cybersecurity transformation.

CISO Samman 2025 recipient **Lucius Lobo,** Chief Information Security Officer, Tech Mahindra being felicitated by R**ajesh Thapar,** Chief Information Security Officer, National Stock Exchange of India & **Uday Deshpande,** Chief Information Security Officer, Larsen & Toubro

Lucius Lobo

Chief Information Security Officer, Tech Mahindra

Lucius Lobo is a pioneering cybersecurity leader who has shaped one of India's most advanced enterprise security programs at Tech Mahindra. As CISO, he leads global information security, business continuity, and data protection, ensuring cyber resilience across a multinational digital services ecosystem. He previously co-founded Tech Mahindra's cybersecurity practice, scaling it to serve 110+ global enterprises across 25 countries with advisory, integration, assurance, and managed security services — earning recognition in Gartner's global Market Guide for security consulting.

As a respected industry voice, he has contributed to national security initiatives through public-private collaborations, served on the World Economic Forum's Internet Security Council, and supported policy and skills development efforts under the NASSCOM-DSCI initiative.

A passionate cybersecurity evangelist, he has authored StaySafe Cyber Citizen and runs the award-winning blog "Lucius on Security." Known for his entrepreneurial mindset and commitment to social impact, he continues to inspire the next generation of security talent and leaders.

Murlidhar Nambiar

Group Chief Information Security Officer, State Bank of India

Murlidhar Nambiar is a distinguished cybersecurity leader and the Group CISO of State Bank of India, India's largest financial institution. With a mandate spanning 45 crore customers, 22,000+ branches, 60,000+ ATMs, 15 group companies, and multiple international offices, he leads SBI's enterprise-wide cyber defense, threat intelligence, security engineering, emerging tech security, and red-team operations.

A proven architect of high-trust security environments, Murli has led cybersecurity efforts for the Reserve Bank of India (via ReBIT), Investcorp, ICICI Bank, Reliance Capital, Mashreq Bank Dubai, and global insurance and financial services businesses. His expertise includes building cybersecurity functions from the ground up, driving secure digital transformation, embedding resilience across critical systems, and aligning security with business strategy.

Recognized for hands-on leadership and structured execution, he has authored security frameworks and citizen-awareness content, developed SOCs, strengthened national cyber posture, and mentored next-generation talent—making him one of India's most respected financial-sector security leaders.■

How AI Is Redefining the CISO Mandate in 2026

Amal Krishna, Executive Director and CISO at ONGC, explains how AI risks, evolving data protection, and fragmented governance are reshaping the CISO's agenda in 2026

By **Jagrati Rakheja**
jagrati.rakheja@9dot9.in

AS INDIA'S Digital Personal Data Protection Act reshapes the regulatory landscape, CISOs are being pushed to rethink their role not as compliance custodians, but as architects of trust in an AI-driven enterprise. In a recent conversation with Jagrati Rakheja, Amal Krishna, Executive Director and Chief Information Security Officer at ONGC, explores how data protection, AI adoption, and governance models are colliding in ways many organizations remain unprepared for.

Krishna offers a clear-eyed perspective on why DPDP demands a distinct operational approach, why AI governance falters when disconnected from business decision-making, and how zero trust must evolve to address non-human identities. As autonomous systems expand and attackers increasingly weaponize AI, he argues that the future-ready CISO will be defined not by obstruction, but by the ability to enable secure, scalable innovation with confidence. Excerpts from the interview.

"The future CISO will not be defined by what they block, but by how securely they enable the business to scale."

CISO Forum: How does India's DPDP Act force CISOs to rethink data security, identity, and accountability as core business enablers, rather than treating them as compliance-driven controls?

AMAL KRISHNA: In my view, the DPDP Act essentially introduces another critical data dimension, or a distinct data classification, that security leaders must protect. However, managing DPDP-specific requirements such as consent, purpose limitation, and lawful processing demands a separate and focused approach. This is why a dedicated Data Protection Officer is necessary and, in my opinion, this role should remain distinct from the CISO. There are several nuances involved. For example, decisions around whether new content or applications involve personal data under DPDP must be discussed with business teams, and those decisions should be business-led.

The DPO can then work closely with the CISO to determine the appropriate level of security controls for such data. The CISO's responsibility remains broader, focused on securing the outer layer and end-to-end protection of all data leaving the organization, regardless of classification. Narrowing the CISO's role to DPDP alone risks role dilution and potential conflicts in accountability.

CISO Forum: As organizations look toward 2026, which emerging technology presents the most underestimated or least prepared-for security risk, and why should security leaders be paying closer attention to it now?

AMAL KRISHNA: As AI adoption accelerates across enterprises, the security risks associated with it have become the most pressing and, in many cases, the least understood. AI is increasingly being used to strengthen security operations, but the same capabilities are also being exploited by attackers to bypass controls, automate attacks, and scale threats. This dual-use nature makes AI fundamentally different from earlier technology shifts.

That is why AI must be implemented with a secure-by-design mindset, where security controls, governance, and accountability are embedded from the very beginning, rather than layered on later. As AI evolves through newer forms, including generative models and discussions around AGI and eventually ASI, the risks multiply. One of the most serious concerns is hallucination. If AI-driven security systems generate inaccurate or misleading outputs, the consequences can be severe. This is precisely why AI governance cannot exist in isolation. It must be tightly integrated with business context, risk management, and human oversight to be effective.

CISO Forum: Is AI governance breaking down in real-world enterprise environments, and what are organizations getting wrong in its execution today?

AMAL KRISHNA: AI governance fails the moment it is treated as a standalone security or compliance exercise. When governance is designed in isolation, disconnected from how the business actually uses AI, it becomes either ineffective or obstructive. In contrast, effective AI governance requires deep collaboration across functions. The CISO or the leader overseeing AI risk from a cybersecurity perspective must work closely with business owners, technology teams, and legal and compliance stakeholders.

Structures such as a digital or AI governance council are critical because they create a shared decision-making framework. In such forums, business priorities, innovation goals, and risk considerations are discussed together, not in silos. This collaborative approach ensures that AI initiatives move forward at speed while remaining secure, compliant, and accountable. When governance is embedded into business workflows, rather than imposed from outside, it becomes an enabler of trust rather than a barrier to progress.

"DPDP adds a new data dimension, not a new owner. The CISO's mandate must remain enterprise-wide, not regulation-bound."

CISO Forum: As AI systems gain the ability to act autonomously, how must CISOs redesign identity, privilege, and trust frameworks to securely govern non-human actors across the enterprise?

AMAL KRISHNA: For years, zero trust has largely been interpreted through a human lens, focusing on controlling how users access systems and data. AI fundamentally changes that assumption. Today, machines, applications, and autonomous agents are constantly communicating with one another, often at a scale and speed far beyond human interaction. These non-human actors must now be treated as identities in their own right.

This means applying zero trust principles rigorously to machines by enforcing least privilege, time-bound access, and highly specific contextual controls such as location, workload identity, and purpose. Access should be granted only for a defined task and revoked immediately after completion. Strong identity validation and

continuous monitoring are essential to prevent impersonation or misuse. Without this shift, AI-driven environments risk creating invisible trust gaps that attackers can easily exploit.

"AI governance fails the moment it is designed in isolation from real business decision-making."

CISO Forum: As attackers increasingly use AI to scale speed and sophistication, where do you see today's security architectures breaking first?
AMAL KRISHNA: The reality is that security in the age of AI has become a continuous cat-and-mouse game. There is security for AI, security within AI, and insecurity created by AI itself, and all three evolve simultaneously. Every powerful technology has both constructive and destructive potential, and AI amplifies this duality far more than previous innovations because of its pervasive reach across systems, data, and decision-making processes.

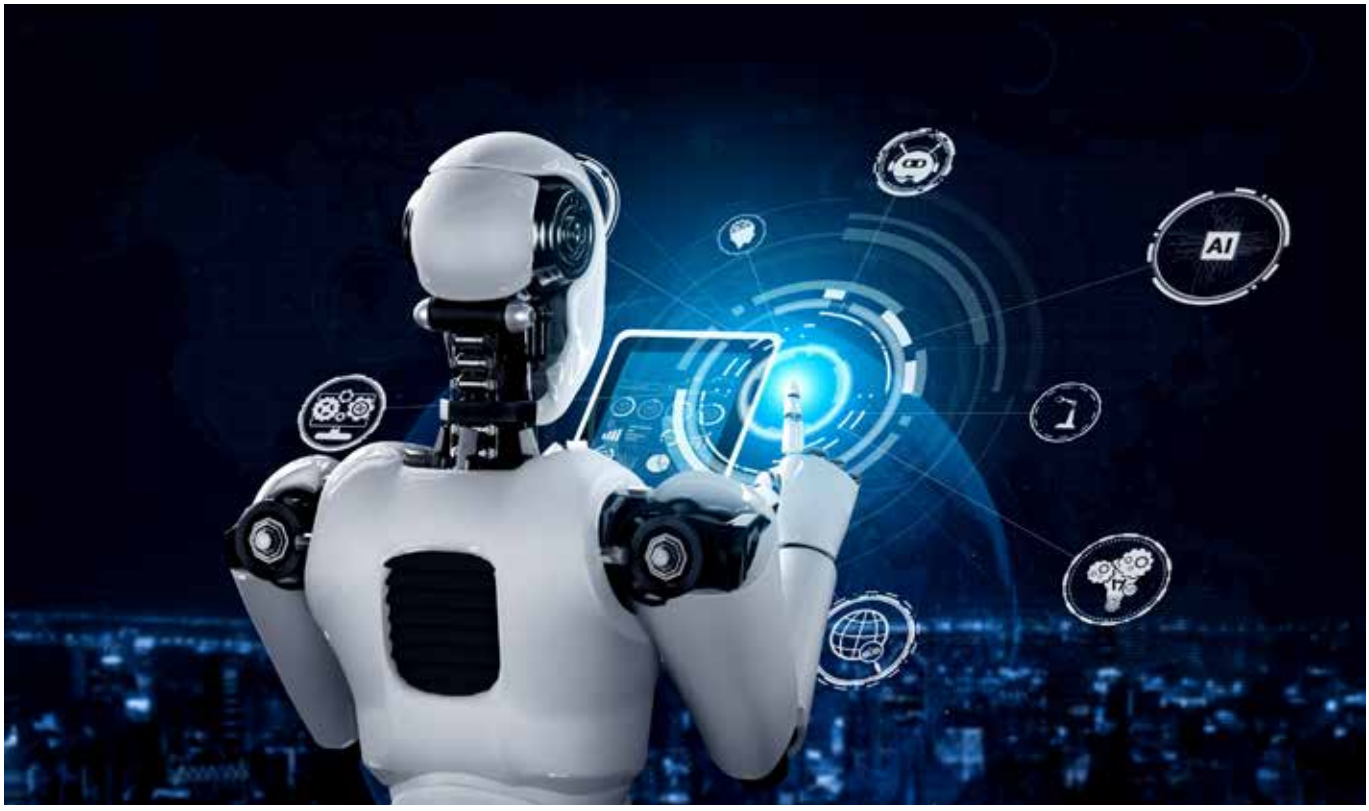
Where architectures tend to break first is at the seams. Traditional security models are often static, rule-based, and designed for predictable behavior. AI-driven attacks, however, are adaptive, fast, and capable of learning from defenses in real time. Gaps emerge in areas such as identity validation, API security, model integrity, and automated decision pipelines, where trust is often implicitly assumed. If these layers are not continuously monitored and dynamically protected, attackers can exploit them at scale. This is why organizations must constantly evolve their controls, strengthen visibility, and treat AI security as an ongoing discipline rather than a one-time implementation.

"In an AI-driven enterprise, machines are identities too, and zero trust must treat them that way."

CISO Forum: Looking ahead to 2026, what will truly distinguish a future-ready CISO: deep technical expertise, architectural foresight, or the ability to govern emerging technologies at enterprise scale?
AMAL KRISHNA: One of the most defining capabilities of a future-ready CISO will be the shift in how the role is perceived and practiced. Traditionally, cybersecurity leaders have often been seen as the final checkpoint after technology is implemented, or worse, as an obstacle that says what cannot be done. That mindset is no longer sustainable. The new paradigm must be about enablement. Instead of saying no, the CISO should guide the business on how to do things differently and more securely.

When security is ignored early, organizations may move quickly at first, only to suffer setbacks after a breach or major incident that damages infrastructure and trust. To prevent this, CISOs must remain in constant dialogue with business and technology leaders. Cybersecurity considerations should be embedded at the foundation of every initiative, ensuring that as new technologies are adopted, the security posture is clear, intentional, and resilient from the outset. ■

AI bots, fraud, and the new cyber arms race



AI-driven bots are exploding, powering fraud at scale and forcing enterprises to rethink cyber defenses urgently.

By **CISO Forum** | editor@cisoforum.com

AKAMAI'S STATE of the Internet: Fraud and Abuse Report 2025 – Charting a Course Through AI's Murky Waters paints a revealing picture of how artificial intelligence is reshaping the cybercrime landscape. Drawing on billions of web requests across industries and regions, the report exposes the growing threat posed by AI-driven bots, which blur the line between helpful automation and harmful exploitation.

AI bot traffic surges 300%

In 2025, Akamai recorded a 300% surge in AI bot traffic, which now makes up nearly 1% of all global internet traffic. Commerce sites alone saw over 25 billion bot requests in two months. These AI bots fall into three categories — training bots, agent/assistant bots, and search bots — with training bots representing 75% of all detected activity.

While some bots enable legitimate functions like search indexing or accessibility, others exploit data, overload systems, and imitate human users. The distinction between good and bad bots is growing increasingly complex, as even beneficial bots can violate website rules or drain resources.

AI fuels fraud-as-a-service & crimeware

The report highlights the alarming rise of Fraud-as-a-Service (FaaS) — a booming underground market where criminals rent out AI-powered tools. Malicious chatbots like FraudGPT and WormGPT can generate phishing emails, fake documents, and malware in seconds. These tools have dramatically lowered the entry barrier for cybercrime, allowing even unskilled users to orchestrate sophisticated scams.

AI has also fueled ad fraud, projected to exceed $50 billion globally in 2025, and return fraud, where bots exploit refund systems using falsified data. Together, these trends show how automation has become both a weapon and a shield — benefiting some industries while crippling others.

Who's getting hit hardest

AI bots are affecting industries differently:

- Publishing faces an existential threat, with 63% of AI bot activity in digital media targeting publishers. AI chatbots scrape their content without attribu tion, leading to traffic loss and falling ad revenue.
- Commerce accounts for 47% of total AI bot detec tions, as retailers face automated scraping, skim ming, and price-monitoring attacks.
- Financial services (4%) and healthcare (90% of AI bot triggers from scrapers) are also under pres sure, balancing innovation with data security and compliance demands.

"AI has democratized cybercrime. The same intelligence that drives innovation is empowering fraud at scale."

Global spread and security response

North America dominates AI bot traffic, accounting for over half of global activity, followed by EMEA and APAC. Across all regions, bots like GPTBot, Bytespider, and ClaudeBot top detection lists.

Akamai urges organizations to move beyond simple bot blocking. Instead, companies must analyze intent, deploy adaptive detection systems, and collaborate across industries to strengthen defenses. Frameworks like OWASP's Top 10 help map vulnerabilities and guide proactive protection.

The takeaway

The Akamai report makes one thing clear: AI has democratized cybercrime. The same intelligence that drives innovation is empowering fraud at scale. Businesses must now distinguish between "helpful" and "harmful" automation — and build smarter, AI-aware defenses before bots gain the upper hand. ■

Ransomware 2025: Retailers strengthen defenses as cybercriminals double down

Retailers are recovering faster from ransomware, but rising demands, smarter attacks, and human strain keep the threat critical.

By **CISO Forum** | editor@cisoforum.com

THE SOPHOS State of Ransomware in Retail 2025 report paints a complex picture of progress and peril. Based on insights from 361 IT and cybersecurity leaders across 16 countries, it highlights how retailers are improving their recovery capabilities while facing rising ransom demands and persistent human stress.

Retail still a prime target

For the third consecutive year, exploited vulnerabilities were the leading cause of ransomware incidents, responsible for 30% of attacks. However, the issue runs deeper than software flaws — 46% of retail victims had security gaps they were unaware of, and 45% lacked the expertise to stop attacks in time, the highest rate of any industry surveyed. Phishing attacks also spiked from 15% in 2024 to 23% in 2025, while compromised credentials rose to 26%, showing that attackers are increasingly exploiting both system and human weaknesses.

Fewer encryptions, but smarter attacks

There's encouraging news: only 48% of ransomware incidents led to data encryption, the lowest in five years, down from a peak of 71% in 2023, highlighting the need for stronger early detection and containment. However, 29% of encrypted victims also suffered data theft, and 6% faced extortion-only attacks. Most retailers proved resilient, with 98% recovering data, though reliance on backups fell to 62%. A notable 58% still paid ransoms, reflecting ongoing pressure and disruption.

Demands double, payments hold steady

Ransom demands surged, with the median doubling from $1 million to $2 million in 2025. Nearly two-thirds of attackers demanded over $1 million, and high-end demands above $5 million grew by 59%. Yet, retailers are showing more bargaining power — the average payment rose just 5% to $1 million. On average, they paid 81% of the initial demand, with 59% paying less than the initial amount.

Recovery costs drop, response time improves

The average cost of recovery fell 40%, from $2.73 million in 2024 to $1.65 million this year. Over half (51%) of retailers recovered within a week — a sign of improved incident response and investment in cyber readiness.

"Retailers are becoming tougher and faster in recovery, but not invincible."

The human impact behind the numbers

Every retailer hit by ransomware reported fallout for IT and security teams. 47% experienced higher pressure from leadership, 43% reported stress and anxiety, and 37% saw staff absences linked to mental health issues. In 26% of cases, leadership changes followed the incident, revealing the heavy toll ransomware takes beyond financial losses.

Outlook: Smarter defense, shared responsibility

Sophos concludes that retailers are becoming tougher and faster in recovery, but not invincible. As ransomware tactics evolve toward extortion and data theft, focus must shift from reaction to prevention by closing security gaps, investing in managed detection and response, and building human resilience. Retailers are winning battles, but vigilance remains essential. ■

Speed kills: How cyber-criminals are winning the race against defenders

Attackers now move faster than defenders, using AI to execute malware instantly across endpoints, cloud, and browsers.

By **CISO Forum** | editor@cisoforum.com

THE CYBERSECURITY landscape has fundamentally transformed. Gone are the days of patient, methodical intrusions. Today's attackers operate at breakneck speed, deploying malicious code immediately upon entry rather than lurking in the shadows. According to Elastic Security Labs' 2025 Global Threat Report, this shift represents the defining challenge facing organizations worldwide.

Windows under siege

The statistics tell a striking story: execution-focused attacks on Windows systems have nearly doubled in just one year, now accounting for 32% of all malicious behavior. Attackers aren't bothering to hide anymore—they're racing to run their code before defenders can react. This makes runtime protection and blocking initial access more critical than ever.

Your cloud's achilles heel

Over 60% of cloud security incidents boil down to three goals: gaining initial access, establishing persistence, and stealing credentials. Whether you're on AWS, Azure, or Google Cloud, attackers are laser-focused on compromising identities. The message is clear: strengthen your authentication systems and monitor privileged access religiously.

AI: The great equalizer

Artificial intelligence isn't just helping defenders—it's democratizing cybercrime. The report reveals a 15.5% surge in generic malware threats, likely driven by attackers using AI tools to generate effective malicious code rapidly. Even less-skilled criminals can now create working malware, dramatically increasing both the volume and variety of threats organizations face.

The browser battlefield

Perhaps most concerning: more than one in eight malware samples is explicitly designed to steal browser credentials. These stolen credentials fuel a thriving underground economy, providing attackers with ready-made keys to corporate cloud accounts. Your browser has become ground zero for credential theft.

"Defense is no longer about prevention alone—it's a race for context."

The GitHub problem

Source code leaks create permanent vulnerabilities. As Elastic's own security team discovered, a single accidental commit—whether of API keys or sensitive documents—becomes part of an immutable, distributed history that's nearly impossible to erase.

What this means for you

The report's central message is sobering: defense is no longer about prevention alone—it's a race for context. Organizations must use AI-driven analysis to connect real-time events with historical patterns, revealing attacks as they unfold. Static defenses and signature-based detection are insufficient against threats that evolve faster than traditional security can adapt.

The winners in this new landscape will be those who can analyze their data fastest, understand their environment deeply, and make decisions at machine speed while maintaining human judgment. ■

Securing hybrid cloud environments: Challenges, trends, and best practices

Hybrid cloud security demands Zero Trust, AI automation, and strong IAM to manage risk, compliance, and complexity.

By **Dr Logesh Rajendran** | Assistant Vice President & Cloud Infra Architect, Citicorp USA

AS ORGANIZATIONS increasingly adopt hybrid cloud infrastructures to balance performance, flexibility, and cost, they also face significant security challenges. Hybrid cloud models integrate on-premises data centers with private and public cloud environments, making consistent security enforcement complex. Cyber threats are evolving, and security misconfigurations, insider threats, and regulatory compliance gaps can expose critical data. The shift towards Zero Trust security models, AI-powered cybersecurity, and cloud-native security solutions is reshaping how organizations approach hybrid cloud security.

Security challenges in hybrid cloud environments

Visibility and control issues

Managing security across multiple cloud providers and on-premises infrastructure can result in blind spots that increase the risk of security breaches. Without centralized monitoring, it becomes difficult to detect anomalies and respond to threats in real time.

Identity and access management (IAM) complexities

Hybrid cloud environments require consistent authentication and authorization policies across multiple platforms. Weak IAM configurations can lead to unauthorized access, credential theft, and privilege escalation attacks. Mismanaged permissions are a leading cause of cloud security incidents.

Data security and compliance risks

Hybrid cloud architectures must comply with diverse regulatory standards, including GDPR, HIPAA, and PCI-DSS. Data encryption, secure storage, and access controls must be implemented uniformly across environments. Organizations that fail to enforce compliance monitoring and audit trails face significant security risks and legal penalties.

API security and workload protection

Hybrid cloud deployments rely on APIs for data exchange between different cloud services and on- premises systems. Weak API security can lead to data leakage, unauthorized access, and API abuse. Additionally, workload protection is critical to securing cloud-native applications running in containers, Kubernetes, and virtual machines.

Incident response and disaster recovery challenges

Security incidents require a rapid and coordinated response across cloud environments. Without automated remediation and cloud-wide visibility, responding to attacks in a hybrid cloud can be slow and ineffective. Organizations must implement disaster recovery (DR) and business continuity plans (BCP) that integrate cloud-native backup and failover strategies.

Current trends in hybrid cloud security

Adoption of zero trust architecture

Enterprises are moving away from traditional perimeter-based security to Zero Trust models, which continuously verify user identities, devices, and workloads before granting access. This approach minimizes lateral movement in hybrid cloud environments, reducing insider threats and external breaches.

Dr Logesh Rajendran
Assistant Vice President & Cloud Infra Architect, Citicorp USA

AI-driven security automation

Artificial intelligence and machine learning are transforming threat detection, anomaly detection, and security incident response. AI-powered SOC (Security Operations Center) tools analyze large datasets in real time, detecting patterns of cyberattacks faster than traditional methods.

Cloud-native security solutions

Cloud-native security tools, such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP), provide automated compliance checks, misconfiguration detection, and policy enforcement across hybrid cloud environments.

Compliance and governance automation

With the complexity of regulatory requirements, automated compliance frameworks are being implemented to enforce security policies, track audit logs, and generate real-time compliance reports. Security as Code (SaC) is emerging as a best practice to standardize security configurations.

Secure DevOps and infrastructure as code (IaC)

DevSecOps is gaining traction as organizations integrate security into CI/CD pipelines, ensuring secure deployments in hybrid cloud environments. Infrastructure as Code (IaC) helps automate secure configurations and policy enforcement across multi-cloud deployments.

Best practices for hybrid cloud security

Implement strong identity and access management (IAM)

Adopt multi-factor authentication (MFA), single sign-on (SSO), and role-based access control (RBAC) to enforce least privilege access across all environments. Continuous identity verification and behavioral analytics can further reduce insider threats.

Encrypt data at rest and in transit

Data should be encrypted using strong cryptographic algorithms like AES-256 to ensure protection against unauthorized access. Additionally, organizations should enforce end-to-end encryption for API communications to secure hybrid cloud interactions.

Enforce centralized security monitoring and threat intelligence

Deploy Security Information and Event Management (SIEM) solutions integrated with threat intelligence feeds to detect and respond to suspicious activity in real time. Extended Detection and Response (XDR) solutions provide unified security monitoring across hybrid cloud environments.

Automate security policy enforcement and compliance checks

Use cloud security automation tools to enforce real-time compliance checks, vulnerability assessments, and risk-based security controls. AI-powered policy engines can dynamically adjust security settings based on threat intelligence and compliance requirements.

“Hybrid cloud security is no longer about perimeter defense—it’s about continuous trust, visibility, and automated resilience.”

Develop a resilient incident response and disaster recovery plan

TA well-structured incident response plan (IRP) as part of larger Business Continuity Plan (BCP) should be in place, incorporating automated threat containment, cloud-native backup solutions, and geo-redundant disaster recovery sites to ensure business continuity in the event of an attack.

The future of hybrid cloud security

Hybrid cloud security is evolving toward a more automated, AI-driven, and compliance-focused model. As threats become more sophisticated, organizations will need proactive defense mechanisms powered by AI, Zero Trust, and automated security policy enforcement. The future of hybrid cloud security will see increased adoption of self-healing security architectures, quantum-safe cryptography, and predictive analytics for threat forecasting. Organizations must continuously refine their security frameworks to keep pace with emerging threats and evolving regulatory landscapes.

By implementing Zero Trust, AI-powered security operations, encryption, and compliance automation, businesses can secure their hybrid cloud environments effectively while maintaining agility and scalability. ■

When AI becomes both shield and weapon: Inside the future of enterprise

Bhaskar Gorti, Executive Vice President of Cloud & Cybersecurity Services at Tata Communications, explains how AI and Zero Trust are redefining enterprise security strategy.

By **Jagrati Rakheja** | jagrati.rakheja@9dot9.in

IN THE era of hybrid work and sprawling multi-cloud environments, the enterprise perimeter has dissolved—and with it, traditional security models. Bhaskar Gorti, Executive Vice President of Cloud & Cybersecurity Services at Tata Communications, is navigating this transformation at the intersection of AI, geopolitics, and regulatory fragmentation. In this wide-ranging conversation, Gorti reveals how Zero Trust architectures, AI-powered threat detection, and data sovereignty mandates are reshaping cybersecurity from a defensive function into a strategic enabler of digital transformation. As cyberattacks grow more sophisticated and AI systems themselves become targets, enterprises face a new reality: security is no longer just about protecting data—it's about preserving the intelligence that defends it.

CISO Forum: With the proliferation of hybrid workforces and multi-cloud environments, how can enterprises ensure secure global connectivity without compromising performance?

BHASKAR GORTI: Strengthen access with the Zero Trust principle With the proliferation of hybrid workforces and multi-cloud environments, enterprise attack surfaces have expanded, making perimeter-based security models obsolete. The Zero Trust principle advocates that no user or device should be inherently trusted – verification must occur continuously, regardless of location or network. By embedding Zero Trust into network design, access management, and policy enforcement, enterprises can ensure that only authenticated and authorised interactions take place. This approach enables secure, seamless, and high-performance connectivity while reducing exposure to lateral movement and internal threats.

Adopt a unified, cloud-delivered security framework

Integrate Secure Access Service Edge (SASE) to unify networking and security functions in a single cloud-based model. This ensures consistent policy enforcement, real-time threat protection, and secure, high-performance access for users across geographies and devices.

CISO Forum: What are the most pressing cybersecurity challenges when operating across diverse regions and regulatory landscapes?

BHASKAR GORTI: Operating across diverse regions has made cybersecurity as much about governance and accountability as it is about technology. The challenges lie in balancing compliance, visibility, and coordination across a patchwork of regulations and threat landscapes.

Data sovereignty & residency

Cross-border data restrictions now require localized SOCs, SIEMs, and storage, fragmenting visibility and increasing costs. Yet this decentralisation is inevitable. India is adapting rapidly through the DPDP Act, RBI and IRDAI directives, and sovereign cloud initiatives — all of which are steering the country toward a compliance-aligned, AI-ready security model. As the digital economy expands, AI-powered monitoring and local trust infrastructure will become increasingly vital in protecting national data assets.

Fragmented regulations & maturity gaps

With rules ranging from India's DPDP to Europe's GDPR and China's CSL, maintaining a unified security posture is increasingly complex. Each jurisdiction brings unique reporting and audit requirements, leading to compliance fatigue and rising operational overhead. Simultaneously, regional disparities in cybersecurity maturity result in uneven protection, creating soft targets in distributed setups.

Region-specific threats & tale gaps

Attackers now tailor their campaigns to target specific language, cultural, and policy gaps. Without context-aware, region-specific intelligence, enterprises risk delayed detection. Add to that talent shortages and time zone gaps, and coordination becomes critical. The future lies in a centralised governance model with local execution, where sovereignty, AI, and collaboration converge to ensure consistent resilience.

CISO Forum: How can security be embedded seamlessly into large-scale digital transformation initiatives, including AI-driven operations?

BHASKAR GORTI: Security is the enabler for all digital transformation. As more applications and data are consumed and more information is exchanged, it becomes the very foundation of digital trust. To safeguard this rapidly expanding ecosystem, enterprises must embed security by design into every layer of transformation — protecting not only applications but also the communication flows between them. A robust edge distribution platform that secures all connections end-to-end ensures this protection remains seamless, scalable, and adaptive.

Enterprises must also harness AI for adaptive threat detection and resilience. As cyberattacks grow in speed and sophistication, AI- and analytics-driven automation can predict, detect, and neutralize threats in real-time. Embedding these intelligent defences within the network and cloud fabric strengthens resilience and ensures secure, uninterrupted operations across digital environments.

Equally critical is maintaining data integrity and governance. AI and digital platforms rely on trusted data — but without strong classification, masking, and encryption, enterprises risk breaches and regulatory exposure. Embedding these practices from data ingestion to inference safeguards both

compliance and confidence. Digital transformation is inherently hybrid, spanning SaaS, IaaS, OT, and edge environments. Enterprises require a unified visibility layer and control plane to eliminate silos and facilitate rapid incident response across their entire digital footprint.

CISO Forum: What approaches help cultivate a security-first mindset internally and among enterprise customers?

BHASKAR GORTI: Building a security-first mindset starts with shared responsibility, anchored by the BISO (Business Information Security Officer) model. Security can no longer be the sole responsibility of the CISO's office — each business unit must own its own cyber posture. Embedding a BISO within functions ensures that security aligns with business goals, shifting from a reactive, compliance-driven task to a proactive, business-enabling one.

Once this foundation is set, leadership must lead by example. When CXOs champion cybersecurity in boardrooms and strategy discussions, it signals that security is not a constraint but a catalyst for growth. Their visible advocacy reshapes culture—transforming security from a "cost" into a "confidence" driver.

The next step is to democratise learning. Gone are the days of generic, one-size-fits-all training. Modern enterprises utilize role-based and gamified modules—such as secure coding for developers, phishing simulations for employees, and data privacy drills for HR—to make awareness contextual and engaging. Continuous, micro-learning formats ensure that cyber vigilance becomes second nature.

Equally vital is making security effortless. Embedding controls like MFA, automated compliance nudges, and hygiene checks into everyday workflows shifts the burden from users to systems.

Finally, an authentic security-first culture extends beyond the enterprise. Sharing threat intelligence, co-developing assurance plans, and hosting ecosystem-wide cyber drills strengthen collective resilience. This shared-responsibility model—anchored by roles like the BISO—redefines security as everyone's business, not just IT's.

"AI is no longer just a defensive tool—it has become the nervous system of modern enterprise cybersecurity."

CISO Forum: How can organizations measure the effectiveness of network and infrastructure security in mitigating complex threat vectors?

BHASKAR GORTI: Achieve complete visibility across the network and infrastructure:

Organisations can only protect what they can see. Gaining a comprehensive view of assets, traffic flows, and attack surfaces is essential for identifying vulnerabilities and assessing security readiness, ensuring no blind spots in their defense posture.

Continuously monitor and benchmark network performance and threat posture: Utilize real-time telemetry, security analytics, and automated incident reporting to assess the effectiveness of network defenses in detecting, blocking, and responding to advanced threats. Metrics such as MTTD, MTTR, and anomaly rates help quantify resilience and response efficiency.

Validate controls through continuous simulation and adaptive testing: Traditional security assessments that were once periodic, conducted quarterly or half-yearly, are no longer sufficient in today's dynamic threat landscape. Organisations must adopt a model of continuous assessment, leveraging threat and breach simulations, red teaming, penetration testing, and attack surface evaluations to measure the real-world effectiveness of their defences. These ongoing exercises help identify blind spots, validate the strength of firewalls and segmentation policies, and drive continuous optimisation of security architectures and incident response frameworks

CISO Forum: How will emerging technologies like AI transform enterprise cybersecurity strategies in the near term?

BHASKAR GORTI: Emerging technologies—particularly AI and GenAI—are transforming enterprise cybersecurity from static defence to adaptive resilience. The battlefield has shifted from human versus machine to AI versus AI, where both attackers and defenders deploy intelligence at scale. This evolution has turned cybersecurity into a form of psychological and systemic warfare. Attackers now exploit context, trust, and human decision-making — and increasingly, they target the very AI systems that power enterprise defences. New vectors such as data poisoning, prompt injection, and model evasion threaten to corrupt training data, manipulate outputs, and bypass detection logic.

Enterprises must therefore not only use AI for security but also secure the AI itself. Protecting data pipelines, hardening models, and continuously monitoring AI behaviour are now foundational. Governance frameworks, such as the NIST AI RMF, and roles like AI Security Officers or BISOs for AI are emerging to ensure transparency, accountability, and resilience.

At the same time, AI-enabled contextual detection allows systems to detect intent, not just anomalies. Autonomous response capabilities within Security Operations Centers enable real-time triage and containment, dramatically reducing mitigation times.

CTEM frameworks close the loop using live simulations and AI-driven risk mapping. Ultimately, AI becomes cybersecurity's nervous system, defining enterprise resilience, trust, and adaptability in the GenAI era. ■

Why the right technology still goes wrong

OVER A recent weekend, my colleague R. Giridhar, our Group Editor, and I engaged with a cross-section of senior technology leaders to explore a deceptively simple question: how do enterprises really evaluate technology today, and why do so many well-intentioned projects still stumble?

One insight emerged almost immediately. Peer feedback has become the most trusted source of truth. Technology leaders increasingly place greater confidence in candid, experience-led conversations with peers than in formal evaluation frameworks alone. Real-world narratives about what worked, what broke, and what required course correction carry far more weight than glossy product claims.

Analyst frameworks from firms such as Gartner and Forrester continue to play an important role, but largely at the product or OEM evaluation stage. They help shortlist technologies but do not guarantee success. When it comes to final decisions, most organizations insist on proof-of-concept engagements, because in cybersecurity or AI, seeing is believing. Internal scoring matrices add rigor, but they rarely capture the messiness of real-world execution.

This is where the conversation took a critical turn. Despite choosing the right technology, many security and transformation initiatives still fail. Technology and security leaders pointed to familiar fault lines such as timeline slippages, scope misunderstandings, poor solution design, limited flexibility around change requests, weak post-deployment support, and perhaps most damaging, insufficient involvement from internal business and IT teams.

The uncomfortable truth is this: the biggest gap is not the product. It is the implementation ecosystem. More tellingly, leaders acknowledged that failure is rarely the vendor's burden alone. It is often a shared responsibility, rooted in gaps in internal governance, unclear ownership, and fragmented collaboration between security, IT, and business stakeholders.

In an environment where CISOs are increasingly accountable for business resilience, regulatory exposure, and AI-driven risk, execution failures are no longer tolerable footnotes. They are frontline security and business risks.

This realization marks a shift in how enterprises are redefining success. The conversation is moving beyond what technology to buy toward how it is implemented, governed, and sustained over time. At the upcoming CISO Forum conference, we will dive deeper into this critical issue, not just celebrating success stories but examining where initiatives failed and why. ■

"The real failure in most technology and security programs isn't the product—it's the implementation ecosystem. Success breaks down in execution, ownership, and collaboration far more often than in technology choice."

Jatinder Singh
Editor, CISO Forum
jatinder.singh@9dot9.in

CISOFORUM

Security For Growth And Governance

Where CISOs Connect, Innovation Ignites

Join the **CISO Forum LinkedIn Group** - a dynamic community where top security leaders like YOU connect, collaborate, and exchange insights. With active engagement, it's the ultimate platform to stay informed, inspired, and ahead in the fast-evolving cybersecurity landscape.

Acquaint with curated content, expert perspectives, and thought leadership designed specifically for today's CISO & security experts.

The CISO Forum community is your gateway to insightful discussions, emerging technologies, and practical strategies - empowering you to lead with confidence in an ever-changing security environment.

Expand your network with the brightest minds in cybersecurity.

Join the CISO Forum LinkedIn Group today and elevate your leadership journey.

Follow us on @CISO Forum

Scan the QR code to follow

You can also visit us at:
https://cisoforum.in/

CISO FORUM

India's Leading Cybersecurity Summit

CISO Agenda 2026

Quantify Risk, Build Resilience, Enable Growth

13–14 February 2026
Radisson Blu Hotel & Spa, Nashik

100+ India's top CISOs Shaping Trust, Resilience & Security for CISO Agenda 2026 at The CISO Forum

Meaningful engagement with 100+ India's top CISOs

Musical evening with a Bollywood celebrity
Experience the magic of Sula Vineyards & Sunrise @ Gangapur Dam

Partners

GOLD PARTNER — Recorded Future®

EXHIBIT & LANYARD PARTNER — ARMIS®

EXHIBIT PARTNER — Barracuda. Your business, secured.

MEDIA PARTNER — CNBC TV18

CONCEPT BY — CISOFORUM

For Sponsorship, please contact

Hafeez Shaikh
National Sales Head,
B2B Tech
hafeez.shaikh@9dot9.in
+91 98331 03611

Sourabh Dixit
Regional Sales Head - North,
B2B Tech
sourabh.dixit@9dot9.in
+91 99714 75342

Subhadeep Sen
Senior Sales Manager,
B2B Tech
subhadeep.sen@9dot9.in
+91 96113 07365

https://events.cisoforum.in/