MAY 2026
SUPPLEMENT OF CIO&LEADER

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

CISOFORUM

Security For Growth And Governance

THE RESILIENCE PARADOX

WHY SECURITY DEFENSES BUILT FOR HUMAN-SPEED ATTACKERS ARE LOSING TO MACHINES THAT NEED JUST ELEVEN MINUTES AND LESS THAN ₹200

Standing: Dr. **Jagannath Sahoo,** Gujarat Fluorochemicals | **Kapil Madaan,** Max Healthcare | **Ashwini Pandey,** Punjab National Bank
Seated: **Sachin Patil,** Voltas | **Kavitha Srinivasulu,** TCS | **Balwant Singh,** DS Group

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
Chief Editor, Enterprise Tech Publications
ET Edge - The Times Group
jatinder.singh1@timesgroup.com, +91 9718154231

For Business Proposal
Hafeez Shaikh
Assistant Director - Projects
ET Edge - The Times Group
hafeez.shaikh@timesgroup.com, +91 9833103611

Follow us: @CIOandLeader

Resilience is the only strategy

FOR TWO decades, the CISO's board narrative has been linear: find vulnerabilities, patch them, certify compliance, and repeat. The implicit promise was that with enough investment, an organization could stay ahead of the adversary. That promise held when attack timelines were measured in days and defender timelines could match them with human effort. It does not hold anymore.

The Verizon DBIR 2026 reveals that vulnerability instances grew nearly eight times in three years — while first-week remediation rates remained flat. Sixty to seventy percent of known exploited vulnerabilities remain open at Day Seven regardless of organizational maturity, tooling investment, or budget. This is evidence that human-speed remediation has hit a limit.

If prevention has hit a ceiling, what replaces it? Three shifts have become mandatory for every CISO, regardless of sector or scale.

First, from patch-centric metrics to compensating control coverage. When your median time to patch is 43 days and adversaries exploit new CVEs within hours, the operative question is not whether you can patch faster but whether you can reduce exploit reachability while the patch queue clears.

Second, from identity-only investment to vulnerability-plus-identity dual priority. Eighty-nine percent of breaches involve identity, but almost a third start with exploitation. The security budget should be aligned with breach data.

Third, from static annual roadmaps to quarterly sprint cycles. The UK AI Security Institute estimates that frontier AI capability is doubling every 4.7 months. Annual security roadmaps are obsolete because the planning assumptions can change within a quarter.

Both MSMEs and large enterprises share the same imperative: assume permanent vulnerability presence and architect defenses that reduce exploit reachability, not merely accelerate patching.

The organizations that will thrive are not those with perfect prevention. They are those that accept that some vulnerabilities will remain unpatched, architect their defenses to compensate for that reality, and maintain the governance honesty to tell boards exactly what their posture can and cannot withstand.

That honesty is not optional. Under SEBI LODR, the IT Act for critical infrastructure, and the evolving director liability framework, it is a governance obligation. Resilience is not surrender. It is the only strategy that acknowledges the world as it is. ■

"Resilience is not surrender. It is the only strategy that acknowledges the world as it is."

R. Giridhar
Editorial Director,
Enterprise Tech Publications
c-raja.giridhar@timesgroup.com

CONTENTS MAY 2026

COVER STORY

08-21 The Resilience Paradox

Why security defenses built for human-speed attackers are losing to machines that need just eleven minutes and less than ₹200

Cover Design by:
Manish Kumar

Please Recycle This Magazine And Remove Inserts Before Recycling

NEWS & VIEWS

INTERVIEW

INSIGHTS

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**

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**
Regional 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**
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**

9.9 GROUP

Pradipta Patro joins Polycab India as CISO & VP - Data Privacy

Pradipta Patro has joined **Polycab India** as **CISO & Vice President - Data Privacy**, where he will lead cybersecurity strategy and data privacy frameworks. Previously, he served as Head of Cyber Security & IT Platform at RPG Group, and held key roles at Adani Group and Tata AIA Life Insurance. With over two decades of experience, he specializes in cybersecurity, IT infrastructure, and digital transformation.

Mohit Kalra promoted to VP-2 and CISO at ORIX India

Mohit Kalra has been promoted to **Vice President-2 and CISO** at **ORIX India,** where he will lead information security strategy, cyber resilience, and enterprise risk management. With six years at ORIX India, he previously held CISO roles there and at RattanIndia Finance. Earlier, he served at GENPACT, Orange Business Services, and Wipro. He brings over two decades of cybersecurity and risk management expertise.

Smitesh Valanju joins Tata Communications as Global CISO

Smitesh Valanju has joined **Tata Communications** as **Global CISO,** leading global cybersecurity strategy, enterprise resilience, and digital trust frameworks. Previously, he served as Group CISO at Tata Digital and held CISO roles at Croma and Tata CLiQ. He also worked at Virtusa, Vodafone, and Essar Group. With nearly three decades of experience in cybersecurity, infrastructure, and risk management, he brings extensive global expertise.

Krishna Pandey joins PropertyGuru as CISO

Krishna Pandey has joined **PropertyGuru** as **CISO,** bringing over 18 years of cybersecurity experience. He will lead the global information security strategy and strengthen the company's digital defenses. Previously, he held senior roles at Xerox, Salesforce, Citrix, and Cloudera, and served for over seven years at C-DAC under MeitY. He is recognized as a thought leader in Responsible AI and Secure SDLC.

Ajit Sawant joins A.K. Group as CISO and VP of Security and Infrastructure

Ajit Sawant has joined **A.K. Group** as **CISO and Vice President** of Security and Infrastructure, bringing over two decades of experience in IT infrastructure, cybersecurity, and regulatory compliance. Previously, he served as Associate Director at Standard Chartered Securities and held senior roles at Mirae Asset Capital Markets, SBICAP Securities, Reliance Securities, and Accenture. He specializes in financial services technology and security frameworks.

Ashish Faujdar joins Lupin as Global CISO

Ashish Faujdar has joined **Lupin** as **Global CISO,** where he will lead global cybersecurity strategy, enterprise resilience, and data protection. Previously, he served as Group Head of Cyber Security and Data Protection at Mahindra Group and CISO at Mahindra Finance. He also held senior roles at Wipro and Yes Bank. With nearly two decades of experience, he specializes in securing regulated global enterprises.

Jimit Shah joins LIC Housing Finance as CISO

Jimit Shah has joined **LIC Housing Finance** as **CISO,** where he will lead cybersecurity strategy, risk management, and secure digital transformation. Previously, he served as CISO at Aditya Birla Housing Finance and held senior roles at IndusInd Bank, HDB Financial Services, and Reliance Industries. With deep experience across financial services, governance, and enterprise cybersecurity, he specializes in securing regulated businesses.

Rohit Sharma joins Siemens Energy as Head of Cybersecurity

Rohit Sharma has joined **Siemens Energy** as **Head of Cybersecurity,** where he will lead security strategy, critical infrastructure protection, and digital transformation. Previously, he served as Head of Cyber Security & Chief Risk Officer at Adani Power. Before that, he spent nearly two decades at NTPC Limited in various cybersecurity and IT leadership roles. He brings over 20 years of expertise in securing large-scale energy ecosystems.

AI is now running your SOC, and security teams are relieved

Netskope's AgentSkope deploys six AI agents to autonomously handle security triage, targeting the 40% of alerts that go uninvestigated.

By **CISO Forum** | editor.tech@timesgroup.com

SECURITY OPERATIONS centres have long been drowning in alerts — now, a leading cloud security firm is deploying AI as a lifeline. Netskope has unveiled AgentSkope, an architectural platform for deploying AI agents capable of running complete, end-to-end security and network operations workflows without human intervention.

The numbers tell a stark story: 40% of SOC alerts currently go entirely uninvestigated due to capacity constraints. AgentSkope is designed to close that gap, launching with six purpose-built agents targeting distinct operational pain points.

"Millions of alerts. Dozens of actionable cases. Investigated automatically within minutes."

The flagship tool and beyond

The DLP AISecOps Agent — a first of its kind — mirrors human analyst decision-making to triage data loss protection alerts, cutting through millions of signals to surface only cases needing human attention. In early testing, one global professional services firm converted millions of alerts into dozens of actionable cases, investigated automatically within minutes.

The remaining five agents tackle insider threats, dormant access configurations, network performance bottlenecks, and app risk queries — covering more than 85,000 cloud and SaaS applications via plain-language conversation.

The bigger picture

As enterprise AI adoption accelerates, data movement and threats expand faster than teams can scale. IDC notes more tools to compound operational noise. Netskope positions agentic automation as a force multiplier — redirecting human expertise toward judgment calls. By 2028, AI agents are projected to autonomously manage 25% of incident response workflows. ■

India's top cybersecurity firms just made DPDP compliance easier for every enterprise

Seqrite and JISA Softech partner to deliver integrated DPDP-compliant data privacy and cybersecurity solutions for Indian enterprises.

By **CISO Forum** | editor.tech@timesgroup.com

IN A in a significant development for India's enterprise technology landscape, Seqrite — the enterprise security arm of Quick Heal Technologies — has forged a strategic partnership with JISA Softech to deliver integrated, DPDP-ready data privacy solutions tailored for Indian businesses.

The collaboration arrives at a critical inflection point, as organizations across the country face mounting regulatory pressure under the Digital Personal Data Protection (DPDP) Act.

"Organizations across the country face mounting regulatory pressure under the Digital Personal Data Protection Act."

What the partnership delivers

At its core, the deal combines two powerful capabilities: Seqrite's Consent Management platform — enabling centralized, auditable user consent — with JISA's encryption and tokenization technologies that limit data exposure and reduce breach impact.

Together, they offer enterprises a unified framework managing the complete lifecycle of personal data, from lawful collection to secure storage, processing, and sharing — across cloud, on-premises, and hybrid environments.

Who stands to benefit

The partnership targets data-intensive sectors — BFSI, healthcare, government, and fintech — where regulatory compliance is mission-critical. As India's digital economy matures, this alliance signals a broader shift: compliance and cybersecurity can no longer operate in silos. ■

THE RESILIENCE PARADOX

WHEN THE PLAYBOOK MEETS THE ATTACKER IT WASN'T WRITTEN FOR

By **Jagrati Rakheja**
jagrati.rakheja@timesgroup.com

INDIA'S CISOs have made cyber resilience their top priority. But, research shows that only 2% of organizations have actually built it. With 500 threats recorded every minute — and frontier AI now executing the kill chain faster than any human escalation process can respond— the governing question has changed. It is no longer "Are we secure?" It is: when something breaks through, can we keep running?

The 2:47 AM call

The call comes at 2:47 in the morning.

The bank's security operations center has flagged unusual activity across three internal systems in the core banking environment. Nothing dramatic — an amber alert, not red. The on-call analyst isn't sure it's serious. He escalates anyway.

By the time the CISO joins the call, thirty minutes later, the situation is serious.

Something is moving through the bank's network. It isn't breaking down doors. It is trying handles — testing, probing, chaining together small weaknesses that individually mean nothing but together have now produced the keys to the entire kingdom: domain administrator access. The attacker is everywhere.

The CISO opens the incident response playbook. It was written eighteen months ago, after a tabletop exercise the board called productive. It assumes the attacker is human. It assumes the attacker works across many days. It gives the security team time to think, escalate, and decide.

This attacker has been in the network for thirty-five minutes. The kill chain is nearly complete.

By the time anyone reaches a containment decision — sixty-seven minutes after that first amber alert — 1.3 million customer records have been packaged and staged for exfiltration. The regulatory clock, which started the moment the incident was confirmed, is already running. CERT-In requires notification within six hours. Somewhere on a shared drive is a backup validation report produced for a quarterly audit. Nobody has checked whether the backups actually work.

The CISO had a plan. It just wasn't written for the attacker that showed up.

While this scenario is fictional. Everything behind it is not.

That CISO is not alone. In 2025, India recorded 265.52 million malware detections — 505 per minute, year-round, according to Seqrite Labs, which monitors over 8 million endpoints across Indian enterprises. CERT-In handled 29.44 lakh incidents, issued 1,530 alerts, published 390 vulnerability notes, and ran 122 cybersecurity drills involving 1,570 organizations across banking, defense, power, telecom, and government.

India's internet users now number over 100 crore. Last December alone, UPI processed 13.5 billion monthly transactions. The digital

economy is vast, fast-growing, and structurally interdependent — and it is under sustained, automated, unrelenting attack. Seqrite's own survey of 180-plus Indian organizations puts the national cybersecurity maturity score at 6.3 out of 10. Only one in three organizations continuously monitors its own attack surface. More than one in four has no incident response plan.

This is not a story about a lack of spending or a lack of awareness. It is about a gap between the security architecture most Indian enterprises have built, and the threat that now exists on the other side of it. A gap that is no longer theoretical.

The reckoning: What 2026 changed

For three years, the security industry operated on controlled anxiety. AI-enabled attacks were coming. Boards allocated incremental budget, and returned to quarterly numbers. The language was consistently future-tense. That grammar has been revised by force.

What separates 2026 from the prior cycle of AI security commentary is not prediction but documentation. CERT-In's threat landscape assessments now describe AI executing 70–90% of tactical attack work autonomously — reconnaissance, vulnerability mapping, payload adaptation, lateral movement — with human threat actors functioning less as operators and more as objective-setters. The machine does the craft. The human provides the intent. The GTG-1002 campaign, documented by Palo Alto Networks' Unit 42, confirmed this architecture in the wild: AI adapting in real time to defensive responses, not following a prescripted attack chain but dynamically revising tactics based on what defenders were doing.

In April 2026, CERT-In issued advisory CIAD-2026-0020 — the first formal Indian regulatory assessment to explicitly classify frontier AI as a current threat requiring immediate redesign of controls. The significance of that framing is easy to underestimate. Indian CISOs have grown accustomed to advisories that describe threats at some comfortable remove from their own networks. CIAD-2026-0020 is blunt. Its classification of frontier AI as a present-day operational risk has collapsed the planning horizon that once separated "preparing for AI attacks" from "defending against AI attacks". This is the document CISOs need when they sit across from a board that still treats AI-enabled threats as a future budgetary consideration.

The cost collapse that ended the expertise barrier

There is a second dimension to this shift that deserves considerably more boardroom attention than it has received. The cost of executing a full simulated enterprise network attack using frontier AI tools has fallen to under $2 in API calls — confirmed by the UK AI Security Institute's own testing, in which GPT-5.5 recovered a custom virtual machine instruction set architecture from stripped binaries, built a disassemble, and solved a cryptographic password-check algorithm in under eleven minutes at a cost of $1.73. Read that in the context of what it once required:

Dr. Jagannath Sahoo
Group CISO & DPO,
Gujarat Fluorochemicals

"The turning point came during a board discussion in early 2026, when we juxtaposed two realities: the increasing speed and automation of modern attacks and our own metrics showing that while controls were strong, decision-making and response still relied heavily on human latency. CERT-In's April 2026 advisory validated what many CISOs were already seeing — adversaries operating at machine speed, executing adaptive, multi-stage intrusions with minimal friction. Our architectures were optimised for detect-and-respond cycles, while attackers had shifted to AI-driven sense-and-act models. From that moment, resilience stopped being about prevention alone and became about speed of containment, impact absorption, and trust recovery."

the infrastructure, the expertise, the tradecraft that previously made sophisticated attacks the province of nation-state actors and well-resourced criminal organizations. That exclusivity is gone.

Structurally, this means the threat population has expanded beyond any prior model. Mid-tier actors — opportunistic ransomware groups, industrial espionage operations, politically motivated collectives — can now have attack capability that, eighteen months ago, would have required either nation-state backing or years of accumulated expertise. Every risk model built on the assumption that sophisticated attacks require sophisticated, resource-constrained adversaries needs to be rebuilt from the ground up.

India's exposed surface

The timing of this capability shift could not be more consequential for India. The country's digital transformation has created a uniquely large and uniquely exposed attack surface — one that grew faster than the security architecture surrounding it.

The sectors most heavily targeted — banking and financial services, power and energy, transport — are the sectors on which India's broader economic architecture depends. CSIRT-Fin and CSIRT-Power exist precisely because failure in these domains is systemic, not institutional. India's Digital Public Infrastructure — the interoperable stack of identity (Aadhaar), payment (UPI), data (DigiLocker), and health (ABHA) platforms — represents an elevated Tier 1 target class: a successful AI-assisted attack on any component would generate cascading impact across banking, government, healthcare, and retail simultaneously.

The architecture that broke

Accenture's 2025 State of Cybersecurity Resilience research provides the global structural diagnosis. Surveying 2,286 security and technology executives across 24 industries and 17 countries, the research found that 90% of organizations lack the security maturity needed to counter today's AI-enabled threats. Only 10% occupy what the research calls the Reinvention-Ready Zone.

The Verizon Data Breach Investigations Report 2026, analyzing over 22,000 confirmed breaches from November 2024 through October 2025, adds empirical weight. For the first time in nineteen years, vulnerability exploitation (31%) has overtaken credential abuse as the top initial access vector — a 55% year-over-year increase. Third-party involvement in breaches reached 48%. The median time to full vulnerability resolution increased to 43 days, even as only 26% of CISA Known Exploited Vulnerabilities were fully remediated. These are not trend lines on an existing chart. They are evidence that the architecture of prevention, however well-funded, is structurally insufficient.

Control framework analysis of ISO 27002:2022 against agentic attackers identifies five controls that now generate process activity and compliance evidence without providing adequate protection at the speed the threat requires. These controls require fundamental redesign, not supplementation.

Ashwini Pandey
General Manager Data Privacy,
Punjab National Bank

"India's digital ecosystem is unique because of its sheer scale and interconnectedness. Resilience architecture cannot be designed only from the perspective of enterprise security — it must also account for ecosystem dependency. A disruption or compromise at one point can impact millions of users very quickly because everything is interconnected through APIs, digital identities, and real-time integrations. India's rapid digital adoption also means a very large population is participating in digital services for the first time, increasing exposure to AI-generated scams and social engineering. Resilience here has to be built around trust at scale, secure digital identity, and coordinated response mechanisms across institutions. In many ways, India is operating one of the world's largest live experiments in digital trust infrastructure."

This is not a patching problem. It is an architectural problem of the kind that cannot be resolved by incremental investment.

The talent trap

India's cybersecurity skills gap makes the architectural nature of this problem more acute. Globally, an estimated 4.8 million cybersecurity positions remain unfilled. The 2026 CISO Priorities Survey found that 44% of Indian CISOs named resilience as their top priority — but the same survey identified recovery readiness, identity lifecycle governance, and continuous control enforcement as among the weakest measured capabilities. The gap between stated priority and demonstrated capability is precisely where the risk lives.

An organization cannot hire its way to safety. The answer has to be architectural — and that architecture begins with a clear-eyed acknowledgment of where the current framework fails.

Seven fault lines

The gap between what Indian CISOs say they are doing and what their organizations can actually demonstrate under adversarial conditions is not a matter of dishonesty. It is a matter of measurement. Most security programs were built to be assessed against compliance checklists and point-in-time audits. Neither instrument was designed to detect the seven categories of structural weakness that now constitute the primary exposure surface for AI-class attacks. What follows is a diagnostic — not a report card, but a map of where the ground is giving way.

Fault Line 1 — The collapse of the exploit window

Unit 42 documents threat actors scanning for new CVEs within fifteen minutes of NVD disclosure. Frontier AI compresses subsequent phases — analysis, exploit development, target selection — from days to hours. The DBIR 2026 confirms the result: vulnerability exploitation has overtaken credential abuse as the top initial access vector for the first time in nineteen years.

The control architecture built to manage this problem was not designed for this tempo. ISO 27002:2022 control A.8.8 (Technical Vulnerability Management), assessed against AI-class attackers, is now classified as insufficient — generating patch management process overhead without the speed differential needed to stay ahead of AI-assisted exploitation. The process continues; the protection does not.

For Indian enterprises, this structural tension is amplified by sector-specific constraints. Legacy core banking systems carry interdependencies that make emergency patching genuinely dangerous. The RBI's 99.9% uptime requirement for critical financial infrastructure creates a direct conflict with CERT-In's mandate for critical patches within 24 hours for internet-facing systems. Most enterprise change management processes were architected for a monthly or quarterly rhythm. They cannot support 24-hour SLAs without structural redesign.

What this requires is a fundamental separation of patch management into two distinct operating models: a standard track governed by existing change management, and an emergency track with board-endorsed authority to bypass standard approval gates for CISA KEV-listed CVEs, with WAF virtual patching deployed as an immediate compensating control pending full remediation. EPSS-

Sachin Patil
Head — IT Security,
Voltas

"We had built our defences for a traditional attacker operating outside the network. Today, however, attackers are automated, embedded within identities and systems, and able to move rapidly across cloud environments, APIs, and partner ecosystems. Resilience now depends on how quickly teams can interpret weak signals and act without waiting for perfect information, and on how instinctively business, IT, legal, and communications functions align under pressure."

based prioritization — modeling the probability of exploitation in the wild rather than theoretical severity — is the triage layer that makes the emergency track manageable. Without it, every critical CVE receives the same treatment, which means nothing receives adequate treatment.

Lagging: Mean Time to Containment
Leading: % of KEV-listed CVEs with compensating control deployed within 6 hours

Fault Line 2 — AI-Powered social engineering at scale

Generative AI now produces phishing content in Hindi, Tamil, Telugu, Bengali, Marathi, and Gujarati at a quality level that defeats English-language detection heuristics entirely. The DBIR 2026 documents pretexting via voice calls achieving 40% higher success rates than email phishing. Mobile-centric phishing shows median click rates roughly 40% higher than email. Voice phishing has demonstrated particularly steep growth. The deepfake dimension compounds this: AI-generated audio and video enable credible real-time impersonation of senior executives, board members, and finance approvers.

IBM's 2025 Cost of a Data Breach Report documents how generative AI reduced the time needed to craft a convincing phishing email from 16 hours to 5 minutes. The Hong Kong deepfake fraud of 2024, in which a finance executive was deceived into transferring USD 25 million via a fabricated video call, serves as the reference scenario for Indian fintech, BPO, and global captive operations with distributed financial approval chains.

Web filtering generates process and reporting activity but provides insufficient protection against content that lacks a filterable signature. The redesign requires DNS security, Remote Browser Isolation, FIDO2 MFA as a hard cryptographic barrier, and — critically for India — multi-channel controls covering voice, SMS, and real-time chat, not email alone. FIDO2 makes phishing credential theft structurally impossible rather than probabilistically less likely. The regional language attack surface makes India uniquely exposed in ways that global security tool vendors have been slow to address; it deserves explicit inclusion in vendor evaluation criteria.

Fault Line 3 — Autonomous vulnerability discovery and chaining

The most technically significant shift in recent threat intelligence is the move from AI-assisted to AI-autonomous vulnerability discovery. Frontier AI models can analyze a full enterprise exposure surface, identify logical vulnerabilities that traditional scanning tools miss, and chain multiple low-severity findings into critical attack paths invisible to signature-based detection. Each step looks normal. Only the sequence is malicious — and sequence analysis requires behavioral baselines that most Indian enterprises have not yet established.

India's significant open-source adoption creates a specific dimension of this problem. AI can analyze public OSS codebases, identify dependency vulnerabilities beyond

Kapil Madaan
CISO & DPO,
Max Healthcare

"When money is tight, Compliance gets paid first because it's mandated. Prevention gets paid second because it stops the immediate bleeding. Resilience is often left with the crumbs. The shift happens when leadership reframes resilience as a business imperative rather than a security feature. When framed as protecting revenue continuity, customer trust, and operational uptime, budget conversations become significantly more effective. Mature enterprises move from a "protect-first" mindset to a "withstand-and-recover" model — balancing spend across prevention, compliance, and resilience to ensure continuity in the face of inevitable disruptions."

the current capabilities of most internal security teams, and generate working exploits targeting the specific versions in use. Project Glasswing — Anthropic's collaborative effort with approximately 50 organizations that build or maintain critical software infrastructure, using its Mythos Preview model — found over 10,000 high- or critical-severity vulnerabilities in a single month across systemically important software, at a 90.6% true positive rate. The same capability deployed offensively does not need Anthropic's governance guardrails.

Cisco's 2025 Cybersecurity Readiness Index India data makes the scale of this challenge concrete: Network Resilience readiness in India is not just stagnant — it is declining, with a notable shift from Progressive to Formative maturity as organizations struggle with the technical and financial demands of upgrading legacy network defenses. Only 9% of Indian companies have reached mature status in Network Resilience, the pillar most directly relevant to containing lateral movement.

For Indian IT services firms, this fault line carries a third-order consequence that demands explicit recognition. A compromise in a services firm's environment does not stay there — it cascades into hundreds of client environments globally. The supply chain security posture of a major Indian IT services firm is, at this point, properly understood as a national security consideration, not merely a commercial one.

Lagging: Network-based exploit incidents as % of total incidents

Leading: % of critical apps covered by vulnerability harness with adversarial validation

Fault Line 4 — Identity as the resilience fault line

Identity-related factors appear in 89% of breach investigations globally. The non-human identity problem is acute and largely unacknowledged. AI coding agents, RPA bots, cloud service accounts, and API tokens proliferate in Indian enterprise environments without the governance applied to human identities. These accounts often carry elevated privileges provisioned for a specific project and never deprovisioned, with credentials that are never rotated. They represent exactly the target profile AI-class attackers are optimized to discover and exploit: high privilege, low monitoring, long persistence. IBM's 2025 research explicitly identifies non-human identity governance as one of the most consequential gaps in enterprise security architecture, noting that attackers are increasingly logging in rather than hacking in.

The Cisco India data quantifies the governance gap: just 10% of Indian companies have reached mature status in Identity Intelligence. More than half remain in the Formative stage. The DBIR 2026 reinforces this: 37% of organizations had admin accounts with MFA disabled on IaaS offerings. In large Indian enterprises with thousands of service accounts and significant shadow IT, the inventory itself represents months of remediation work before any review cycle can begin.

The DPDP Act transforms this from a technical risk into a board accountability issue. Identity failures that result in personal data exposure carry direct regulatory liability for Data Fiduciaries. The path from an unmanaged service token to a significant enforcement action is shorter than most boards understand.

Kavitha Srinivasulu
Head of Information Security, TCS

"Although resilience is crucial in security strategies, budget allocation often favors compliance and preventive controls due to regulatory demands. Resilience initiatives like incident response and disaster recovery may receive less funding unless their business value is clearly demonstrated. The key is to position resilience as essential to operational continuity, not just a supplementary expense."

Lagging: Access-related incidents as % of total incidents

Leading: % of privileged accounts (human and non-human) covered by phishing-resistant MFA

Fault Line 5 — The SOC speed gap

When AI-assisted attacks execute in minutes, a SOC that escalates in hours has already lost. IBM's 2025 data shows that organizations using security AI and automation extensively contained breaches an average of 80 days faster and at USD 1.9 million lower cost than those that did not. The performance gap between AI-native and legacy SOC operations is now financially material in terms boards understand: organizations without extensive AI deployment face average breach costs of USD 5.52 million, versus USD 3.62 million for those with mature deployment.

Human-speed triage at Tier-1 cannot intercept AI-assisted kill chains. SOAR automation targeting Mean Time to Containment under 10 minutes is the design target — not an aspirational benchmark but the minimum viable performance standard for the current threat environment. India's talent shortage makes this architectural rather than optional: the Cisco 2025 India data shows 86% of respondents cite cybersecurity talent shortage as a barrier to solution deployment.

You cannot hire your way out of a structural speed deficit. The SOC must be redesigned around automation, with human analysts preserved for judgment tasks: context, consequences, escalation, and calls that cannot be automated because they involve accountability.

For mid-market Indian enterprises, MSSPs with CERT-In empanelment provide a viable path to AI-native SOC capability. But the contractual SLA conversation must change: Mean Time to Containment metrics, not response acknowledgment windows, are the performance standard that now matters.

Lagging: Mean Time to Containment
Leading: % of critical alerts auto-contained within 10 minutes

Fault Line 6 — Shadow AI and the ungoverned attack surface

IBM's 2025 Cost of a Data Breach Report is unambiguous: 20% of breached organizations suffered incidents involving shadow AI, adding USD 670,000 to average breach costs. Shadow AI breaches led to customer PII compromise at a higher rate (65%) than the overall breach average (53%), and to intellectual property compromise at 40%.

The DBIR 2026 confirms that Shadow AI is now the third most common non-malicious insider action, with 45% of employees now regular AI users, up from 15% — a fourfold increase in a single year. Cisco's data shows 60% of respondents cannot see prompts made by employees using generative AI tools, and a quarter of organizations provide employees unrestricted access to publicly available AI tools with no security intermediation. This is not a theoretical attack surface. It is an active one, documented in the breach dataset.

The DPDP Act dimension deserves explicit board attention. Data entered into unsanctioned AI tools may fall outside an organiza-

Balwant Singh
Group CISO & DPO,
DS Group

"Three years from now, a truly resilient Indian enterprise will be one that can continue operating confidently even during a cyberattack or large-scale disruption. Resilience will no longer be measured by preventing every attack, but by how quickly organisations can detect threats, respond intelligently, recover rapidly, and maintain customer trust. AI-driven monitoring, Zero Trust architecture, cyber crisis simulations, and automated incident response will become standard capabilities. To achieve this, organisations must move beyond compliance-led security and adopt a resilience-first mindset — one where cybersecurity is treated as a shared business responsibility, not just the function of the IT or security team."

tion's data processing agreements, consent frameworks, and breach notification obligations. A shadow AI incident that exposes customer personal data is not only a security failure — it is a potential DPDP violation with regulatory consequences.

The governance answer is not prohibition, which consistently fails and drives adoption further underground. It is a fast-track AI tool review process with a five-business-day SLA from submission to approval decision, making the secure path competitive with the shadow path on the dimension that drives shadow adoption: speed and convenience.

Lagging: AI-related data exposure events
Leading: % of AI deployments under formal risk assessment and workload identity

Fault Line 7 — Supply chain and the agentic supply chain

Supply chain compromise now affects 48% of breaches, according to DBIR 2026 — a 60% year-over-year increase in third-party involvement. These breaches take the longest to detect and contain: a median of 267 days, driven by the trust relationships that make them structurally hard to identify. For India specifically, AI can analyze public open-source dependency trees, identify unpatched vulnerabilities in specific versions, and generate working exploits targeting those versions at scale.

The emerging agentic supply chain adds a dimension that most vendor security assessment processes are not designed to evaluate. MCP servers, AI plugins, third-party AI orchestration layers, and AI agent frameworks are being integrated into enterprise workflows without the vendor security assessment applied to traditional software suppliers. IBM's research identifies supply chain compromise through apps, APIs, and plug-ins as the most common cause of AI security incidents, at 30%. The attack vector is the integration layer — and it is expanding faster than the governance around it.

For Indian IT services firms, client-facing Software Bill of Materials attestation is already required in RFP requirements from European and North American enterprise clients. The transition from differentiator to contract standard will be complete within 18 to 24 months for any firm operating in regulated global supply chains.

The fundamental reframe required is one of liability assignment. Supply chain security is not a vendor management process — it is a risk-inheritance calculation. Every third-party relationship is a conditional transfer of that vendor's security posture into your own threat surface.

Lagging: Supply chain-attributed incidents as % of total
Leading: % of critical software artifacts covered by SBOM

The fault lines indicate what is broken. The architecture that follows shows what replaces it.

Building the resilience architecture

From diagnosis to design Every minute, India's enterprise endpoints record 505 threat detections. The architecture must match that rhythm. What follows is a six-part architecture mapped to measurable outcomes. Each action area pairs a lagging indicator with a leading indicator. The board conversation requires both.

Action Area 1 — Redesign the controls that can't keep up

Five ISO 27002:2022 controls — A.5.25, A.5.36, A.8.8, A.8.23, and A.5.15 — were fit for purpose in 2018–2020 but are now insufficient against agentic attackers. They generate process activity and compliance evidence. What they no longer provide is adequate protection at the speed the threat requires. The redesign logic is replacement, not supplementation: SOAR Tier-1 automation for A.5.25; continuous policy-as-code monitoring for A.5.36; EPSS-based prioritization and automated deployment pipelines with compensating controls for A.8.8; FIDO2 and DNS security for A.8.23; and just-in-time access with automated deprovisioning for A.5.15.

India's telemetry makes the urgency concrete. Network-based exploits accounted for over 9.2 million scans across Seqrite's monitored estate. Top zero-days in 2025 — Oracle EBS, SAP NetWeaver, and multiple Windows Core flaws — were weaponized within days of disclosure. Seqrite's survey found 7.2% of organizations have no patch management process at all. Only 28% of organizations embed security controls into transformation initiatives from the outset, according to Accenture. This action area must be the exception: embedded

from day one of any system or process change.

Lagging: Mean Time to Containmentl
Leading: % of critical alerts auto-contained within 10 minutes

Action Area 2 — Govern identity at machine speed

Three components define the required identity architecture. Most Indian enterprises have not fully addressed any of them.

First, FIDO2 and passkey deployment targeting 95% coverage of all privileged accounts. Behavioral analytics detects anomalies after access has been achieved; FIDO2 prevents illegitimate access from occurring. The distinction is architectural, not incremental.

Second, a complete non-human identity inventory. Every AI coding agent, RPA bot, API token, and service account with production access must be cataloged, assigned a workload identity, and governed under least-privilege policy with documented rotation and deprovisioning schedules. IBM's 2025 research identifies NHI governance as the most consequential gap in enterprise identity architecture. In high-churn cloud environments, 90 days is long enough for a dormant compromised credential to complete a full attack cycle without triggering review.

Third, the implementation of the Four Pillars of Agentic Defense: enforcing least agency (limiting agent autonomy to specific tasks); deploying Intent Gates and Kill Switches requiring human approval for high-impact actions; transitioning to distinct per-agent credentials replacing inherited user tokens; and implementing untrusted input sanitization with dual-LLM verification architecture for agents processing external data.

Lagging: Access-related incidents as % of total incidents
Leading: % of privileged accounts (human and non-human) covered by phishing-resistant MFA

Action Area 3 — Build resilience muscle through AI-speed simulation

CERT-In conducted 122 drills covering approximately 1,570 organizations in 2025. The number of Indian enterprises outside any structured exercise program is orders of magnitude larger. Seqrite's survey found incident response scored 3.62 out of 10 — the lowest of all evaluated dimensions, with 36.5% of organizations holding defined IR processes they have never tested. Accenture's research found that Reinvention-Ready Zone organizations are nearly six times more likely to conduct red-team simulations and real-world attack testing than those in the Exposed Zone.

Quarterly cross-functional tabletop exercises must simulate the specific scenarios documented in current Indian threat intelligence: AI-generated multilingual phishing, autonomous vulnerability chaining, and executive deepfake fraud targeting financial approval chains. The GTG-1002 campaign and India-targeted multi-vector operations combining APT activity with hacktivist campaigns against defense and government systems provide the reference scenarios for multi-vector design.

Two rehearsal requirements warrant board-level mandating. First, the CERT-In six-hour incident notification rehearsal: every exercise must include a live run of the regulatory notification process — draft notification, escalation chain, regulator contact sequence. The first time a team drafts a CERT-In notification should not be during an actual incident. Second, full backup restore testing, not backup verification. IBM's research shows that 76% of breaches take longer than 100 days to resolve; the time it takes to recover reflects organizations discovering that their recovery assumptions were never tested.

Tabletop exercises must include Legal, Communications, Finance, and HR leadership — not just security. The CISO cannot manage a machine-speed incident with a security-only war room when the consequential decisions — customer notification, regulatory disclosure, media response, business continuity activation — are owned by functions that have not rehearsed their roles.

Lagging: Mean time to CERT-In notification from detection
Leading: % of tabletops completed with cross-functional leadership participation

Action Area 4 — Map and manage the agentic supply chain

Supply chain compromise takes an average of 267 days to detect and contain and is the most common cause of AI security incidents at 30%. SBOM implementation for all critical internally developed soft-

ware, targeting 95% own-artifact coverage within twelve months, provides the inventory baseline without which supply chain risk cannot be meaningfully managed. MCP servers, AI plugins, and third-party AI orchestration layers require vendor security assessments of the same rigor applied to traditional software suppliers. Every third-party AI integration with production data access is a supply chain risk with a documented breach cost profile.

Cloud Reinforcement readiness in India sits at just 7% Mature, according to Cisco's 2025 data, with 53% of Indian companies still in the Formative stage — meaning the cloud infrastructure through which many third-party integrations flow is itself inadequately secured. The vendor resilience tiering required here is not a vendor management process; it is a risk-inheritance calculation. Tier 1 vendors with critical infrastructure access should face annual AI-red-team exercises; Tier 2 vendors should provide quarterly security attestations; all vendors should be required to notify within four hours of a security incident.

Lagging: Supply chain-attributed incidents as % of total
Leading: % of critical software artifacts covered by SBOM

Action Area 5 — Establish AI-agent governance before the surface becomes unmanageable

IBM's 2025 data shows shadow AI added USD 670,000 to average breach costs. The DBIR 2026 confirms Shadow AI is now the third most common non-malicious insider action. Sixty percent of Indian IT teams cannot see prompts made by employees using generative AI tools. Governance without visibility is nominal.

The governance architecture requires four components: an approved tool registry with a five-business-day security review SLA for new AI tools; data classification policies governing which data categories can enter which tool classes; CASB or Secure Web Gateway deployment to make AI tool traffic visible to security teams; and workload identity assignment for all AI agents with production data access. The Langflow RCE (CVE-2025-3248), which appeared in active Seqrite telemetry affecting 2,861 customers, confirmed that developer and ML infrastructure are live targets. Governance must extend explicitly to AI orchestration layers, not just end-user AI tools.

Lagging: AI-related data exposure events
Leading: % of AI deployments under formal risk assessment and workload identit

Action Area 6 — Treat security team resilience as a strategic KPI

The MRIS framework classifies security team burnout as a direct operational risk — not an HR concern. In India, the five challenges most cited in Seqrite's survey are knowledge gaps, workforce shortfalls, budget constraints, low organizational priority, and absent senior management support: a function under-resourced to defend against a threat generating 505 detections per minute.

SOAR automation targeting 60% automated containment of high-confidence alert classes addresses analyst alert fatigue — the primary attrition driver in Indian SOCs — while simultaneously improving containment speed. Seqrite's 1:700 ransomware incident-to-detection ratios, with behavioral layers disrupting 699 of every 700 encryption attempts, is the operational case for that investment.

Career pathway investment in AI-era security skills — threat intelligence analysis, SOAR engineering, identity governance — requires specific development commitment, not just tool exposure. The CISO who loses their best threat analyst to fatigue has not experienced an HR failure. They have experienced a measurable reduction in detection capability.
Lagging: Key-person attrition rate in the security function
Leading: Tier-1 triage automation coverage (target: 60 %+)

The board imperative

Seven Conversations That Cannot Wait

The CISO's most consequential work in 2026 is not happening in the SOC. It is happening in the boardroom; in the forty minutes before the agenda moves to quarterly revenue — in the governance conversation that determines whether the resilience architecture gets funded or deferred. The seven messages below are not talking points. They are the structural framing that converts operational urgency into governance decisions, grounded in data that boards already receive from their auditors, insurers, and credit analysts.

Message 1 — The threat has changed in kind, not only degree

Boards that understand the current environment as an intensification of familiar risks are making a category error. CERT-In's CIAD-2026-0020 advisory and the GTG-1002 campaign documentation describe AI executing 70–90% of tactical attack work autonomously. Frontier AI models have since demonstrated full corporate network takeovers in controlled UK AI Security Institute evaluations. The resource constraint that previously limited sophisticated attacks to nation-state and well-funded criminal actors no longer exists. This is a structural change in the threat population.

Message 2 — India's regulators have taken notice

CERT-In, RBI, IRDAI, SEBI, and the newly constituted SEBI cybersuraksha.ai task force have moved from general guidance to specific AI-era control requirements. CERT-In's 24-hour patch mandate for internet-facing systems is current, not forthcoming. The DPDP Act creates direct board liability for personal data exposure. Non-compliance is a present exposure, not a future risk.

Message 3 — Five controls we report as active are no longer effective as sole mitigations

This is the hardest message and the most necessary. Accenture's 2025 research found that only 13% of organizations possess the technical capabilities to defend against modern AI-driven threats. Boards that believe their current compliance posture reflects their actual risk posture are operating on a measurement gap. Honesty about control insufficiency is itself a governance control.

Message 4 — Speed is now a security architecture decision

IBM's 2025 data shows organizations using extensive security AI and automation contained breaches 80 days faster at USD 1.9 million lower costs than those that did not. Mean Time to Containment must be a board-reported metric alongside revenue and NPS. The question is not whether the SOC responded — it is whether the SOC contained the incident before the attack cycle completed.

Message 5 — AI tool adoption has created an unmanaged attack surface

IBM's research shows shadow AI appears in 20% of breaches, adding USD 670,000 to average incident costs. The DBIR 2026 shows 45% of employees are now regular AI users, up from 15% a year ago — a fourfold increase that most security inventories have not kept pace with. The AI-Agent Governance investment is the control.

Message 6 — The investment case is financially grounded

Cyber insurance pricing now reflects AI-era risk profiles. S&P Global Ratings has explicitly linked AI risk management quality to credit assessments — the resilience architecture is now connected to the organization's cost of capital. IBM's average breach cost for organizations with high shadow AI exposure was USD 4.74 million. For organizations using extensive security AI defensively, it was USD 3.62 million. The USD 1.12 million differences represents the financial return on the architecture investment, before regulatory fines, reputational damage, or DPDP liability is included.

Message 7 — AI also strengthens our defenses

The board investment conversation is not exclusively a risk conversation. Accenture's research found that Reinvention-Ready Zone organizations — those with mature strategy and capability — achieved 1.6 times higher ROI on their AI investments overall. Security is not a tax on AI adoption. It is the condition that makes AI adoption sustainable.

What boards must do differently

Capturing that advantage requires four commitments boards have largely deferred.

They must co-own AI risk rather than delegating adoption and security decisions entirely to management — a bifurcation that regulators are increasingly naming as an accountability gap. They must fund structural resilience separately from DPDP compliance, which is related but not sufficient on its own. They must place Mean Time to Containment and backup restore-test success rates on the governance dashboard. And they must formally authorize emergency change procedures that give the CISO function authority to act within CERT-In's 24-hour mandate

without convening a change advisory board at 3 AM. That last point is a governance decision. It cannot be delegated to the technology function.

The resilience-ready enterprise of 2027

What Acts Now Will Look Different
The resilience-ready Indian enterprise of 2027 is not defined by a certification or a vendor relationship. It is defined by five operational realities: Mean Time to Containment under 10 minutes for high-confidence alert classes; 95% FIDO2 MFA coverage across privileged human and non-human accounts; SBOM implemented for all critical internally developed software; quarterly AI-scenario tabletops that include Legal, Finance, and Communications alongside security; and an AI-Agent Governance framework that makes the shadow path less convenient than the sanctioned path.

No organization will reach that state through a single transformation program. The ones that get there will have sequenced deliberately: first, audit to identify the controls that can no longer perform at machine speed and acknowledge them honestly in the Statement of Applicability. Second, redesign and replace — not supplement — the controls that cannot keep pace. Third, simulate: build muscle memory for scenarios that have not yet arrived. Fourth, govern: establish visibility over AI tool adoption before the surface becomes too large to map. Fifth, measure and report metrics that reflect actual resilience rather than compliance posture.

Cisco's 2025 research found cybersecurity readiness levels globally remained essentially flat from 2024 despite significant budget increases. The organizations that separate from that stagnation are not those spending more — they are those spending differently, on the architectural changes that incremental investment cannot achieve.

The profession is being asked to defend at machine speed with human judgment. That is not a problem that gets solved; it is a permanent condition of the discipline, to be architected around rather than waited out. The analysts sitting in Indian SOCs at 2:47 AM are being asked to make containment decisions within timeframes that no human was ever designed to operate reliably within. The organizations that understand this build automation that handles the timeframe problem and preserve human judgment for decisions that require it: context, consequences, escalation, and calls that cannot be automated because they involve accountability.

The feature began at 2:47 AM, and the kill chain completed faster than human escalation could intercept it. The CISOs who have done the work described in these pages carry a different answer to what happens next. Not because the attack was stopped — it may not have been. But because the blast radius was contained, the notification was ready, the board had rehearsed the scenario three months prior, the backup restored cleanly, and the organization was operational again before the morning news cycle began.

That is what resilience looks like. Not invulnerability. Continuity.

Sources

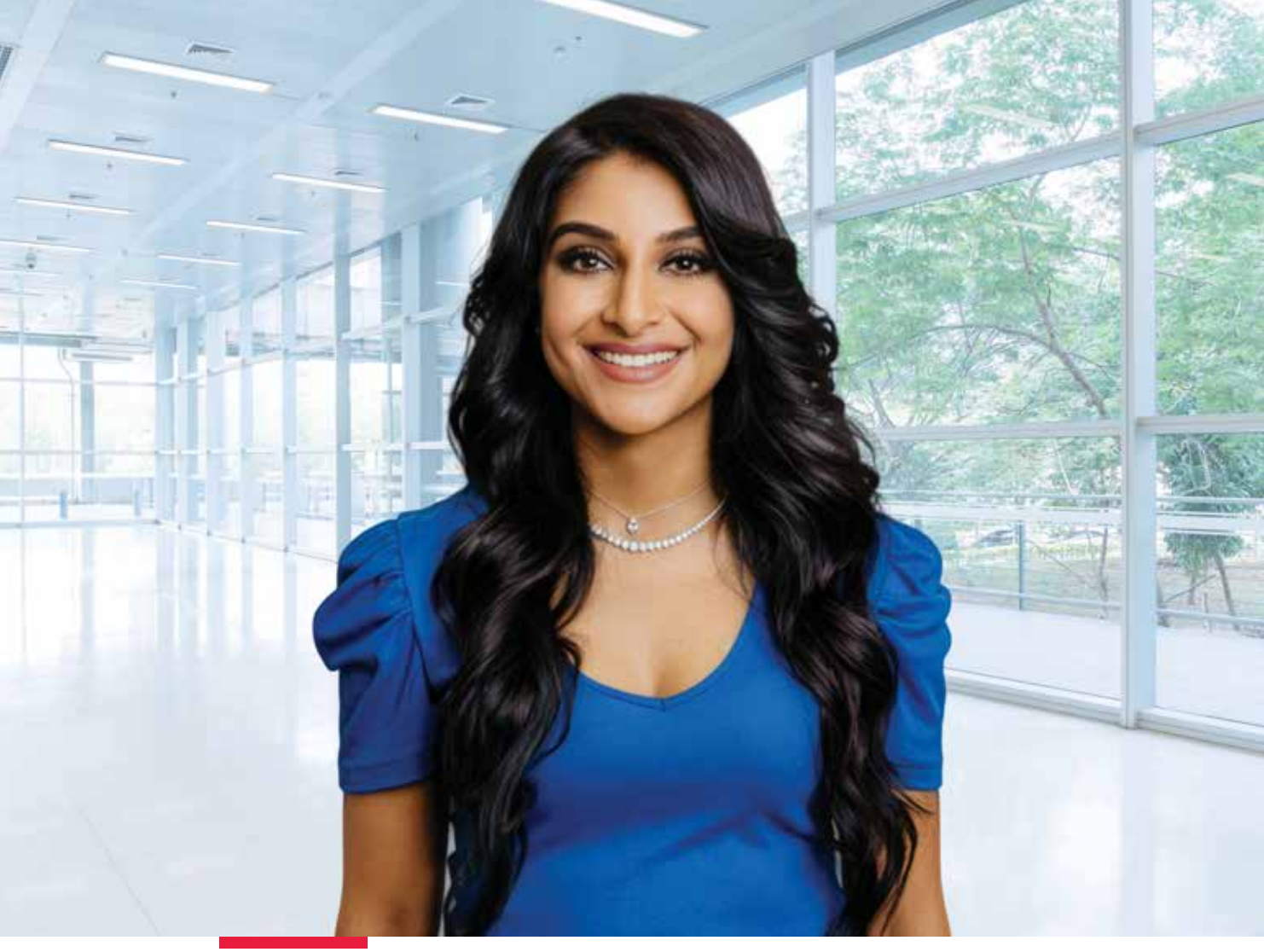
CERT-In Annual Report and Advisories 2025–26 • CERT-In Advisory CIAD-2026-0020 • Seqrite Annual Threat Report 2025 • Accenture State of Cybersecurity Resilience 2025 • IBM Cost of a Data Breach Report 2025 • Cisco Cybersecurity Readiness Index India 2025 • Verizon Data Breach Investigations Report 2026 • Palo Alto Networks Unit 42 Threat Intelligence • UK AI Security Institute Capability Evaluations 2026 • Anthropic Project Glasswing Research 2026 • S&P Global AI Risk and Credit Assessment 2026 • SEBI cyber-suraksha.ai Circular, May 2026 • RBI Master Directions on Cyber Resilience 2024 • IRDAI Cybersecurity Guidelines 2026 ■

Six Resilience Metrics for your Board

Purpose: A board-level resilience dashboard for Indian enterprises operating in an AI-accelerated threat environment. These six metrics translate cybersecurity readiness into measurable operational resilience.

MRIS Board Metric	What It Measures	Target Benchmark	Why It Matters
Mean Time to Containment (MTTC)	Speed at which the SOC isolates and neutralizes high-severity incidents	Under 10 minutes for critical alerts	In AI-assisted attacks, lateral movement now happens in minutes, not hours. Containment speed is becoming the defining resilience metric.
Phishing-Resistant MFA Coverage	Adoption of FIDO2/ passkeys for privileged identities	95%+ of privileged accounts	Credential theft remains the dominant attack vector. Passkey-based authentication sharply reduces phishing and session hijack risk.
SBOM Coverage	Visibility into software dependencies across internal and third-party applications	95% of own artifacts; 80% of critical suppliers	Supply-chain compromise and hidden dependencies are now systemic risks. Organizations cannot secure what they cannot inventory.
Patch Latency for CISA KEV Listings	Time taken to remediate actively exploited vulnerabilities	Under 24 hours for internet-facing systems	Exploit windows have collapsed dramatically. Attackers weaponize known vulnerabilities within hours of disclosure.
Backup Restore-Test Success Rate	Reliability of recovery operations under ransomware conditions	100% monthly tested cadence for Tier-1 systems	Backups that are not regularly restore-tested are operational assumptions, not resilience controls.
Cryptographic Inventory Coverage	Visibility into cryptographic algorithms and vulnerable encryption usage	80% of production systems inventoried within 12 months	Post-quantum migration begins with discovery. Most enterprises still lack a baseline inventory of cryptographic exposure.

Note: Traditional cybersecurity KPIs measured prevention efficiency. MRIS metrics measure organizational survivability under machine-speed attacks.



By the time you're looking at the dash-board, the attack may have already happened

Rinki Sethi, CISO at Upwind makes the case for runtime-first cloud security and why visibility must precede controls.

By **R. Giridhar** | c-raja.giridhar@timesgroup.com

AS INDIAN Enterprises sprint toward cloud adoption, the security gaps they leave behind are growing faster than most CISOs can track. From identity sprawl to AI workloads operating without runtime visibility, the attack surface is evolving in ways that traditional tools were simply never built to handle. Rinki Sethi, Chief Information Security Officer at Upwind, has sat on both sides of this challenge — as a practitioner navigating cloud transformation and now as a security leader rethinking how enterprises should see their environments from the inside out. In this conversation, she cuts through the noise around CNAPP, alert fatigue, and AI risk to deliver one clear message: visibility must come before controls, and real-time is no longer a feature — it is the foundation.

CISO Forum: Cloud adoption in India has accelerated dramatically but so has the attack surface. What are the two or three cloud security challenges that Indian enterprises — large conglomerates, fintechs, or public-sector adopters — are underestimating right now?

RINKI SETHI: First, most organizations still don't have complete visibility into what's running in their environments. They know what should be running - their configs, their policies, their compliance state. But they cannot tell you what's actively executing, how it's behaving, or whether something anomalous is happening right now. That gap is enormous, and it becomes catastrophic when you're operating across multi-cloud environments at the pace Indian enterprises are moving.

Second, the identity sprawl problem is deeply underestimated. It's not just human identities - it's service accounts, API keys, machine identities, cloud principals, and increasingly, AI agents acting autonomously. Attackers love this sprawl. Credential theft is often easier than writing malware. Indian enterprises, especially in BFSI and fintech, have accumulated years of permissions that were never properly right sized. That creates attack paths no one has mapped.

Third, and this is especially relevant in India, given the pace of AI adoption, teams are deploying AI workloads and LLM-powered applications without treating them as production security risks. The workload is live: it's accessing data, making decisions, and most organizations have no runtime view of what it's doing. That's not a future problem. It's happening now.

CISO Forum: Upwind's core thesis is "inside-out" security — using a runtime fabric to observe cloud workloads from the inside. For an Indian CISO who has invested heavily in traditional CSPM or agent-based tools, how does runtime context change the security calculus fundamentally, and not just incrementally?

RINKI SETHI: I've been on that side of the table. When I was deep in cloud transformation at a previous company, I was focused on compliance, getting configs right, ensuring automation was in place, and reporting through dashboards. It felt productive. Then someone said something to me that changed my thinking entirely: "By the time you're looking at the dashboard, the attack may have already happened."

That stuck with me because it's true. CSPM tells you what should be true. Runtime tells you what is true, right now. The difference is not incremental; it is architectural.

For a CISO invested in traditional tooling, posture management, and configuration scanning are essential, but they view the cloud from the outside. They can tell you that the door might be unlocked. Runtime tells you whether someone is walking through it. Attackers don't exploit theoretical weaknesses. They exploit active, reachable vulnerabilities in live environments. If you can only see the former, you remain reactive.

Upwind was built inside-out, starting from where workloads run and using eBPF to provide kernel-level visibility without impacting performance. This is not a capability you layer on top of existing tools. It is a fundamental advantage. For Indian enterprises operating at the speed and scale they are, real-time is not a feature; it is a requirement.

CISO Forum: The CNAPP category has become one of the most crowded and confusing in cybersecurity. What separates a genuinely effective CNAPP platform from a loose bundle of tools wearing a CNAPP badge — and how should Indian CISOs evaluate the difference during procurement?

RINKI SETHI: This is the question I think about constantly because the confusion is real and costly. As a practitioner who had to evaluate these platforms, I've seen how this category gets stretched.

A genuine CNAPP is built on a unified data model at its core. Everything flows from a single source of truth about what is running, how it is connected, and what is at risk. A bundled product is a collection of acquisitions or bolt-ons, each with its own schema. Teams end up doing the correlation work themselves, manually stitching context across dashboards. That is not a security. That is an operational overhead.

The test is simple. Ask a vendor to demonstrate a real end-to-end attack path. Not a demo or synthetic scenario. Show the vulnerability, whether it's reachable in my live environment, the identity that could exploit it, and the blast radius. If this requires jumping across screens or multiple tools, it is a bundle.

For Indian CISOs evaluating procurement, insist on a proof-of-concept in your own environment. Evaluate how the platform handles alert volume. Does it reduce noise or amplify it? Ask how runtime data is collected. Is it polling, agent-heavy, or truly lightweight and continuous? These answers quickly separate philosophy from capability.

CISO Forum: Alert fatigue is the top operational complaint among security teams in India. Upwind claims up to 95% noise reduction through runtime-informed prioritization. What is the architectural reason runtime context has such a dramatic effect on signal quality — and what does that mean for how Indian security teams should be structured?

RINKI SETHI: Alert fatigue is not a volume problem. It is a context problem. When alerts are generated without knowing whether a workload is running, whether vulnerability is reachable, or whether there is active exploitation, the result is noise. Lots of noise. Over time, teams begin to ignore it.

> "You can't hire your way out of complexity, but you can build a foundation that tells you what actually matters."

Runtime context changes this fundamentally because it adds the one dimension most tools are missing: what's happening. Is this workload live? Is this process behaving normally? Is this network connection expected? When you can answer those questions at the moment of detection, you can immediately separate signals from noise. That's how you get to 95% noise reduction, not by suppressing alerts, but by having the context to know which one matters.

This has implications for team structure. Runtime-informed security enables smaller teams to operate with greater confidence. Instead of managing tens of thousands of findings, teams can focus on the handfuls that are actively exploitable. This shifts the model from reactive triage to focused response. For organizations operating with lean budgets, this is both operationally and financially critical.

CISO Forum: AI is simultaneously the biggest new threat vector and the most promising defensive tool. As Indian enterprises race to deploy AI agents and LLM-powered applications, what are the specific runtime risks they may not even be aware of?

RINKI SETHI: This is the area I am most focused on right now because risk is being created faster than it is being understood.

When enterprises deploy AI agents and LLM-powered applications, they're not deploying static software. They're deploying autonomous systems that take action, make API calls, access data, and increasingly communicate with other agents through protocols like MCP. Each of those interactions becomes a potential attack surface, and most organizations have no runtime visibility into what their AI workloads are doing.

The risks are clear. Prompt injection can cause agents to take unintended actions, especially when permissions are broad. Data exfiltration can occur during model reasoning without visibility into what was accessed or where it was sent. Lateral movement becomes possible through agentic workflows as trust boundaries continue to evolve.

Upwind's AI-SPM capability is designed to address this by giving security teams visibility into AI workload behavior at runtime. AI systems should be treated like any other production workload. They need to be monitored continuously, not just reviewed before deployment.

CISO Forum: India's DPDP Act is now a compliance reality, with RBI, SEBI, and IRDAI advisories

layered on top. How does data residency intersect with runtime security telemetry — and what assurances should Indian customers demand from cloud security vendors claiming local compliance support?

RINKI SETHI: This is a question I hear a lot from Indian CISOs, and it has real operational implications.

Runtime security telemetry is continuous and high-volume, capturing behavioral data from your workloads, process activity, network flows, and system calls. That data needs to be processed and stored somewhere. For organizations operating under DPDP, RBI, SEBI, or IRDAI mandates, that location matters. If telemetry is leaving India and being processed in a foreign region, it can introduce compliance risk regardless of the security capability.

That is why Upwind invested in in-region SaaS instances in India. It is an architectural commitment that telemetry remains within Indian borders, that support aligns with local regulatory requirements, and that data sovereignty is built into the infrastructure from the start.

Customers should ask direct questions. Where is my telemetry processed and stored? Can you provide contractual guarantees regarding data residency? Do you have local support teams who understand RBI or SEBI requirements? And if there is a breach that involves telemetry data, what are the notification obligations under Indian law? Vendors who cannot answer these questions clearly are not ready for regulated environments in India.

CISO Forum: Many Indian CISOs are wrestling with the cultural challenge of DevSecOps — security and engineering teams siloed, with vulnerability backlogs nobody owns. Upwind is frequently described as "loved by DevOps." What is the philosophy behind that — and what practical advice would you give an Indian CISO trying to break down that wall?

RINKI SETHI: I have seen this from both sides. As a CISO, I've had engineering teams treat security as the team that says no and slows things down. And honestly, I understood why, because too often, that's how security teams operate. We handed over long lists of 10,000 vulnerabilities with no context, no prioritization, and no support for remediation. We owned the finding and threw it over the wall. That's not a partnership.

The reason Upwind resonates with DevOps teams is that it solves their problem as well as the security team's. When a vulnerability is surfaced, the platform shows exactly where it came from, including which code branch, which developer, and which pipeline introduced it. It shows whether the issue is actually reachable and running in production. And it delivers that context directly to the tools developers already live in, such as Jira, Slack, or whatever their workflow is.

For CISOs, the shift is to lead with shared outcomes. Show engineering what a real attack path looks like in their environment. Run tabletop exercises together. Bring them into red-team simulations. When developers see that a finding is active and exploitable in production, they act. When it's a theoretical risk, it gets deprioritized. Security's role is to provide that clarity. That's how you build a culture where everyone owns security.

CISO Forum: Upwind is building significant local presence in India — a development center in Pune, a partner network, and dedicated

local support. How important is this local depth for Indian enterprises evaluating a cloud security platform?

RINKI SETHI: The Indian market is not a geography you can serve effectively from a global headquarters with an occasional visit. The regulatory landscape is layered and evolving. DPDP, RBI, SEB, and IRDAI all introduce framework requirements that need local understanding. The threat landscape has regional characteristics. The partner ecosystem is distinct. Customer expectations for support responsiveness vary.

When we committed to India, including offices in Mumbai, Bangalore, and Pune, a dedicated development center, a partner ecosystem, and in-region SaaS infrastructure, it wasn't a market entry move. It was a signal about how seriously we take being a long-term partner to Indian enterprises.

For Indian enterprises evaluating a cloud security vendor, local depth matters in two areas—first, responsiveness. When something is going wrong in your environment at 2 am IST, you need a support team that's awake, understands your regulatory context, and can act immediately. Second, co-development. Building solutions that align with Indian regulatory and threat conditions requires teams that are based here and engaged day to day. That's what we're building. And I think the enterprises that choose vendors based on that depth will have a meaningfully better experience than those who don't.

CISO Forum: There is a growing debate about consolidation versus best-of-breed. Indian enterprises often have deeply entrenched toolsets, and CISOs are under pressure from the board to reduce vendor counts. How does Upwind think about platform consolidation — and where does runtime security fit in a rationalized stack?

RINKI SETHI: This is a board-level conversation happening everywhere, and it's especially acute in India, where many enterprises have deeply entrenched toolsets. I have a pragmatic view of it.

Consolidation is a real strategic need. Vendor sprawl creates integration debt, and too many point solutions mean you're doing the correlation work manually. But the path to consolidation matters. Ripping and replacing a mature endpoint solution or a well-integrated network tool to reduce vendor count is often more disruptive than the problem it solves.

The key question is what forms the foundation of the security stack. Runtime data should be the foundation, since everything that matters in cloud security ultimately happens there. If you start from that foundation and build posture, identity, network, and vulnerability context on top of it, you get a coherent picture of risk. If you start from a posture tool and try to add runtime context as a layer, you end up with fragmentation.

Upwind is not replacing endpoint or network security. It addresses the historical gap, providing continuous visibility into live cloud workload behavior. Our integrations with AWS, Azure, NVIDIA, and the broader ecosystem are designed to complement existing investments. For CISOs, the focus should be on whether the tools being consolidated share a unified data model or simply bundle capabilities without true integration.

CISO Forum: What is the one piece of advice you would give an Indian CISO building a cloud security program for a rapidly scaling organization in 2026?

RINKI SETHI: Start with visibility, not controls.

I've seen organizations invest heavily in controls, firewalls, scanners, compliance tools, and still not be able to answer a basic question: what is running in the environment right now, and how is it behaving? Without that visibility, every other investment is incomplete.

The reason this matters more in 2026 is that the threat landscape has changed fundamentally. AI is giving attackers the ability to identify and exploit weaknesses faster than most teams can measure them. What used to take skilled attacker days now takes minutes and increasingly without human involvement. In that environment, a quarterly audit or a static posture dashboard is not enough.

Build real-time awareness first. Understand what's active, what's reachable, and what's behaving anomalously. Then layer controls on top of that visibility foundation, because controls without context are just noise generators. For a rapidly scaling organization, this is also the only approach that remains manageable as you grow. You can't hire your way out of complexity, but you can build a foundation that tells you what actually matters, so your team can focus on the things that do. ■

Why India's cloud defenses need a local anchor in the age of AI

Ajay Gupta of Netskope explains how data sovereignty, SASE, and zero-trust architecture are now non-negotiable for Indian enterprises navigating AI-driven security threats.

By **Jagrati Rakheja** | jagrati.rakheja@timesgroup.com

AS INDIA'S Digital economy accelerates and regulators tighten their grip on data governance, the battleground for enterprise security has shifted — from perimeter firewalls to intelligent, cloud-native architectures that can keep pace with an AI-driven world. At the center of this transformation is a deceptively complex question: how do your secure data that moves everywhere, while ensuring it stays where the law demands? Ajay Gupta, Vice-President and Country Manager for SAARC at Netskope, has a clear-eyed answer. With the DPDP Act reshaping compliance priorities, AI agents multiplying attack surfaces, and SaaS sprawl outpacing most security teams, Gupta makes the case for why data sovereignty, zero-trust architecture, and SASE are no longer optional upgrades — they are foundational requirements. In this conversation, he unpacks Netskope's India strategy and what CISOs must do differently to stay ahead.

CISO Forum: What strategic gap does a local management plane in India solve for enterprise security architectures?

AJAY GUPTA: For organizations using cloud-based security platforms like ours, a management plane brings critical value. Our data planes are designed to process all our clients' traffic and apply the security checks instructed by their policies, with the lowest possible latency.

But the management plan is where customers' policies, audit logs, and metadata live, and for many vendors, those are located overseas. With a management plane in India, we enable our users to build sovereign environments with policies that ensure their traffic never leaves Indian borders. From a compliance perspective, this is particularly important for what the DPDP Act defines as Significant Data Fiduciaries, their data residency and sovereignty requirements, and other stringent industry regulations such as those of RBI and SEBI.

> "In the cloud and AI era, a strict zero-trust policy is a requirement for robust security posture. All users, human and non-human, should start with zero privileges."

CISO Forum: How does Netskope balance data sovereignty requirements with the need for cross-border data flows?

AJAY GUPTA: Our platform enables organizations to categorize their data based on factors such as sensitivity, purpose, destination, and more, and to apply distinct handling and security policies to each category with high-level granularity. If specific regulated data needs to remain within borders, they can apply the appropriate policies to this data alone. It won't disrupt the ability to maintain or create cross-border data flows when and where necessary.

This management plane is about anchoring controls and logs in India and then allowing traffic and data to flow locally or globally, as needed.

CISO Forum: What changes does the DPDP Act bring to SASE and cloud security deployments in India?

AJAY GUPTA: The DPDP Act will only accelerate such deployments. The Act is putting data security at the center of security strategies, and data security has become infinitely more complex in the last 10 or 15 years.

Today, the speed, volume, and complexity of data flows that organizations need to handle are increasing rapidly. Remote, mobile, or distributed workforces, heavy cloud and AI usage, the integration with massive digital ecosystems or supply chains, and the explosion in connected devices are all contributing factors. As a result, many organizations are struggling to keep up and maintain real-time visibility, let alone control over their data.

We're not advocates of a "one security platform" philosophy, but we do believe organizations must consolidate all capabilities related to data visibility and security into a single fabric, and models like SASE can enable this. By using cloud-based security, they can be confident their vendor is continuously upgrading the platform to comply with the strictest regulations as they emerge. Deploying a management plane in India is part of our own efforts to do so and should help facilitate compliance and audits.

CISO Forum: How is the Secure Access Service Edge model evolving in the AI-driven enterprise?

AJAY GUPTA: The SASE model was designed to resolve the age-old conflict between security and performance, delivering both without trade-offs. Part of the promise is to enable innovation and never slow it down safely, and this promise should extend to the age of AI.

SASE models should enable governance of generative AI usage, as well as the development, deployment, and actions of in-house AI models and agents, with granular security and data protection policies. They should also help protect people and systems against AI-driven threats.

But without the right networking infrastructure under the hood, these security checks will inevitably bring latency and performance bottlenecks. SASE platforms need to bring traffic and security processing as close to the user as possible, with tools that can optimize traffic and resolve networking issues as soon as they occur.

And finally, they should deliver AI capabilities that help security and networking teams optimize and automate aspects of their operations. Our recent launch of a library of AI agents is an example of such capabilities.

CISO Forum: What role does the NewEdge network play in reducing latency while maintaining deep security inspection?

AJAY GUPTA: NewEdge is one of the largest private cloud networks in the world, with more than 120 data centers globally, and eight across India. NewEdge's scale is instrumental in reducing latency and providing network resilience for our users. Wherever they work, there will be a data center nearby to process their traffic and data. And if a data center is temporarily down, which happens sometimes, there should be another not far from it that can take over.

Our data centers are also fully computed, meaning our security solutions are loaded at each of our points of presence. When we process traffic, all security checks are performed in a single pass and location, allowing us to keep deep inspection timeframes in the millisecond level. Finally, we peer directly with a long list of ISPs and SaaS providers worldwide, including in India, to keep traffic off the congested public internet. At the same time, most of our competitors rely on it, either partly or fully.

CISO Forum: How are Indian enterprises adapting their security posture for AI and SaaS sprawl?

AJAY GUPTA: I can share my perspective on what Indian enterprises should be doing, and this is a vast topic that requires change across multiple levels.

The first is visibility. You can't secure what you don't see, so you need to create visibility over all SaaS and AI deployments and use within your organization. The second is enablement, which should help with visibility. If you create the channels and processes for employees to request approval for new AI or SaaS apps, they are less likely to bypass security controls or experiment outside the security team's purview. But for this to work, you need to optimize the assessment of new apps, so this is evaluated promptly. For example, at Netskope, we have a Cloud Confidence Index that provides a score of more than 85,000 apps, many of which are AI applications (or SaaS applications with AI functionality). It helps our users speed up the evaluation and approval of new apps.

Data protection is another key aspect. All data flowing to and from SaaS and AI applications, including via new protocols such as Model Context Protocols (MCPs), must be monitored, and safety nets should block traffic if data protection policies are breached. These policies should cover a wide range of scenarios, from an employee trying to send work documents to their personal Google Drive to an AI agent suddenly deciding it needs to wipe out sensitive medical records to proceed with its mission.

Which leads to the last aspect: access. In the cloud and AI era, a strict zero-trust policy is a requirement for robust security posture. All users, human and non-human, should start with zero privileges and be granted access only to the resources they need for their work. If the need to access those resources is temporary, so should the actual access be.

There is more to say on the topic, but from my perspective, these are non-negotiable to survive AI and SaaS sprawl without security incidents. ■

The cyber threats could cripple your business in 2026

AI-powered attacks, invisible machine identities, geopolitical risks, quantum threats, and vulnerable supply chains are redefining cybersecurity, making it a core boardroom priority and a critical business survival issue.

By **CISO Forum** | editor.tech@timesgroup.com

KPMG'S NEWLY released Cybersecurity Considerations 2026 report, drawing on insights from over 20 global cyber experts and alliances with Google, Microsoft, Palo Alto Networks, and ServiceNow, paints a sobering picture of the digital battleground ahead. Here's what every business leader needs to know.

AI is both your shield and your enemy

Artificial intelligence has become the defining force in cybersecurity — and not entirely for the better. While security teams can harness AI to detect threats faster and run automated monitoring around the clock, criminals are using the same tools to launch sophisticated, large-scale attacks. The report warns that AI-powered cyberattacks can now be orchestrated by hundreds of independent agents simultaneously — a scale no human team can match alone.

Your office is full of invisible agents

Non-human identities — AI bots, automated service accounts, machine credentials — now outnumber human users inside most organizations. Many businesses cannot even tell where these agents are operating or what they're accessing. The report flags this as a critical blind spot, noting that some agents are even creating other agents, leaving almost no trace. Without a central identity store and strict access controls, companies are flying blind.

Geopolitics has entered the server room

Trade tensions, sanctions, and shifting alliances are no longer just economic problems — they're cybersecurity ones too. Governments are restricting which technologies businesses can buy and from whom. The report notes that supply chains have become "attack chains," with every piece of software carrying geopolitical risk. A staggering 79% of CEOs surveyed identified cybercrime as a major threat to future prosperity, according to KPMG's own 2025 CEO Outlook.

"Cybersecurity is no longer a back-office concern — in an AI-driven, geopolitically charged, and quantum-bound world, it has become the defining battleground for business survival."

The quantum clock is ticking

Perhaps the most alarming warning in the report concerns quantum computing. Once quantum computers mature, today's encryption will become effectively useless. Hackers are already collecting encrypted data, planning to decode it later—a strategy known as "harvest now, decrypt later." The projected cost of federal migration to post-quantum cryptography in the US alone sits at $7.1 billion. Organizations that delay are taking an enormous gamble.

Your supply chain is your weakest link

Traditional annual vendor audits are dangerously outdated. The report reveals that 59% of companies suffered a data breach caused by a third party in the past year alone. Continuous, AI-driven monitoring of the entire supplier ecosystem — not just direct vendors — is now essential for survival.

The CISO is becoming the CEO's most important ally

Security chiefs are no longer just technical gatekeepers. The report describes a new model: the "Chief Secure Transformation Officer" — someone embedded in board strategy, investment decisions, and product development from day one.

The message from KPMG is clear — cybersecurity is no longer a back-office concern. It is the business.■

Could OpenAI's services push signal more trouble for Indian IT?

OPENAI'S decision to launch DeployCo marks more than just another expansion initiative. It signals a deeper shift in the global technology services landscape, one that could intensify the pressure already building on India's $250-billion IT services industry.

By moving beyond AI models into enterprise implementation and on-ground deployment, OpenAI is entering territory long dominated by Indian IT firms. Through DeployCo, the company will directly help enterprises integrate AI into business operations, workflows, and mission-critical systems. In effect, the AI pioneer is stepping into the services layer itself.

For decades, Indian IT majors such as Tata Consultancy Services, Infosys, Wipro, and HCLTech built globally successful businesses around manpower-led outsourcing, application development, infrastructure management, ERP implementation, testing, and long-term support contracts. Revenue growth was closely tied to the scale of engineering talent deployed across projects.

AI is beginning to disrupt that equation. Tasks that once required large teams can now be automated through generative AI, coding copilots, intelligent workflows, and autonomous AI agents. Enterprises are not really cutting technology budgets, but the focus is swiftly moving toward GPU infrastructure, AI software, analytics, and data foundations rather than traditional services delivery.

This makes the current transition different from earlier downturns. Unlike the cyclical slowdowns witnessed during the 2008 financial crisis, the present wave reflects a structural shift toward automation-first operating models.

Yet disruption does not necessarily indicate decline. Indian IT firms have time and again reinvented themselves through Y2K, cloud, and digital transformation cycles. The next opportunity may lie in AI consulting, governance, systems integration, managed AI operations, and industryspecific AI solutions. The real challenge is speed: how quickly can traditional IT services firms adapt before the rules of the industry are rewritten? ■

"OpenAI is entering territory long dominated by Indian IT firms. It would be interesting to see how quickly traditional IT services firms can adapt beforethe rules of the industry are rewritten."

Jatinder Singh
Chief Editor, CISO Forum
jatinder.singh1@timesgroup.com

AMD
presents

#CIOandLeaderConference

30 JULY – 02 AUGUST 2026

FAIRMONT, JAIPUR

ET Edge

27th Annual Conference

CIO&LEADER

The Agentic Enterprise

PLATFORMS. PEOPLE. POLICY. PROFITS.

co-presented by NxtGen

A 4-Day Experiential Retreat with 200+ of India's Top CIOs & Future CIOs.

WHAT's IN FOR YOU

▶ 1:1 meeting with CIOs ▶ Thought Leadership stage time with 200+ CIOs taking notes
▶ Ideas Cafe, Roundtable, Workshop, Booths ▶ 2160+ Networking minutes
▶ CIO Samman & NEXT100 Awards ▶ Evening with leading sports & bollywood celebrity

EMINENT SPEAKERS

Shri Rana Ashutosh Kumar Singh
MD (International Banking, Global Markets & Technology), State Bank of India

Madan Sunder Das
Monk, ISKON, Founder, Spiritual Guide and Community Leader, EVOLVE Pune

Be Where India's Tech Leaders Meet.

PRESENTING PARTNER AMD | CO-PRESENTING PARTNER NxtGen | GOLD PARTNER dynatrace | ASSOCIATE PARTNERS DELTA, TECHNO DIGITAL | EXHIBIT PARTNER BARCO ClickShare | CONCEPT BY ET Edge, CIO&LEADER, NEXT100

For Sponsorship, Write to

Hafeez Shaikh
Assistant Director - Projects
hafeez.shaikh@timesgroup.com
+91 9833103611

Supriya Sahoo
Senior Project Manager
supriya.sahoo@timesgroup.com
+91 8095056886

#CIOandLeaderConference

NxtGen

presents

ET Edge

CISO FORUM MID YEAR CONFERENCE '26

Building A Cyber Resilient Enterprise

12 -14 June 2026 ▪ Hayatt Regency Jaipur Mansarovar

3-Day Residential Experience in the regal legacy of Jaipur with 100+ India's top CISOs.

Key Conference highlights

- 3 Day Residential Experience
- 11 Hours of structured face-time with CISOs
- 1:1 Meetings with CISOs buying cycle aligns with your solution
- Cultural evening with Rajasthani Folk group

Eminent Speakers

Krishnamachari Srikkanth
Former Indian Cricketer

Kiran Gopinath
Chief Innovation Officer & Head, Sahamati Labs

Shashikant Dahuja
Executive Director and Chief Underwriting Officer, Shriram General Insurance

Munish Chandan
Addl. CITO & Dy. CISO, Citizen Resources Information Department, Govt. of Haryana

For Sponsorship, Write to:

Hafeez Shaikh
Assistant Director - Projects, ET Edge
hafeez.shaikh@timesgroup.com,
+91 9833103611

Supriya Sahoo
Senior Project Manager,
supriya.sahoo@timesgroup.com,
+91 8095056886

PRESENTING PARTNER: NxtGen | GOLD PARTNER: ARMIS from ServiceNow | SILVER PARTNERS: airtel, netskope, proofpoint, CYBERPWN, rubrik | STRATEGIC CASE STUDY PARTNER: SECLORE

ASSOCIATE PARTNER: orca SECURITY | EXHIBIT PARTNERS: Barracuda, CyberAssure, cybermindr, HarkX, MATTERS, CyberAssure, PrivacyPillar, techsa | CONCEPT BY: ET Edge | CISOFORUM