FEBRUARY - MARCH 2026
SUPPLEMENT OF CIO&LEADER

CISOFORUM

Security For Growth And Governance

CISO AGENDA 2026

MOVING BEYOND PREVENTION TO GOVERNING RISK, RESILIENCE, AND CONTINUITY

Ranjan Revandkar | Pradipta Patro | Sameer Ratolikar | Ambarish Kumar Singh
Dr Durga Prasad Dube | Urvish Acharya | Rama Devi Sangu | Ravi Prakash Burlagadda | Rajeev Verma

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

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 - Times Group
jatinder.singh1@timesgroup.com, +91 9718154231

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

Follow us: @CIOandLeader

Agentic threat is here. Are you ready?

IN THE past few weeks the conversation has shifted dramatically—from "how do we adopt AI?" to "how do we survive it?"

OpenClaw — the autonomous AI agent — went viral in weeks before security researchers could sound the alarm. The risks are severe: remote code execution vulnerabilities, API keys stored in plaintext, a poisoned skills marketplace, and hackers actively targeting agent configurations.

Autonomous agents that browse, read, write, execute commands, and persist memory across sessions are probably proliferating inside your organization — or will be soon. Any CISO who treats agentic AI as a procurement decision rather than a security architecture crisis will soon be writing a breach disclosure, not the strategy memo.

This evolving threat environment makes Anthropic's Claude Code Security a genuine capability leap. Claude Opus 4.6 identified over 500 high-severity vulnerabilities in production open-source codebases, many of which had survived decades of expert review. For Indian enterprise CISOs, the implication is immediate. Vulnerability backlogs that once required entire security engineering teams to fix can now be addressed in hours.

However, Anthropic's Frontier Red Team is candid about the dual-use reality: the same reasoning engine that helps defenders find zero-days can help attackers exploit them since adversaries enjoy equal access to the same APIs. The bottom line: A CISO without an AI-augmented defense posture is already disadvantaged. The answer is to pilot, govern, and deploy — with human-in-the-loop controls — now.

Yet speed alone is not the answer. Our recent survey of CISOs found that formal governance frameworks for AI-powered security tools remain the exception, not the norm. That gap between capability and accountability is precisely where incidents are born. With India's regulatory landscape tightening, the CISO's mandate for 2026 is to build governance that moves at the speed of AI adoption. That means AI-specific access controls, prompt injection threat modelling, agent privilege minimization, and rigorous supply chain scrutiny for every third-party plugin.

Educate your board that an AI agent with persistent memory and credential access is a latent insider threat. Organizations that govern AI well and move fast will not merely survive this transition — they will define it. ■

"A CISO without an AI-augmented defense is disadvantaged"

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

CONTENTS

FEBRUARY MARCH 2026

COVER STORY

08-27

CISO AGENDA 2026

SHIFT FROM PREVENTION TO GOVERNING RISK, RESILIENCE, AND CONTINUITY

Cover Design by:
Manish Kumar

Please Recycle This Magazine And Remove Inserts Before Recycling

NEWS & VIEWS

INTERVIEW

INSIGHTS

BEHIND THE FIREWALL

CISOFORUM
Security For Growth And Governance
www.cisoforum.in

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

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

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

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

National Sales Head - B2B Tech: **Hafeez Shaikh**
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**
Manager - Events & Conferences: **Sampath Kumar**
Senior Producer: **Sunil Kumar**

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

For editorial queries write to:
editor@cioandleader.com

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

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

Editor: **Vikas Gupta**

Sunny Mathur joins Société Générale (Securities) India as CISO

Société Générale Securities India has appointed **Sunny Mathur** as its **Chief Information Security Officer.** He will lead cybersecurity strategy, governance, risk management, and resilience to protect critical financial systems and ensure regulatory alignment. Previously at BSE India, Sunny led ISMS and GRC programs and brought deep expertise across financial services, compliance, audits, and enterprise cybersecurity operations.

Naina Bhattacharya joins Coats as CISO

Naina Bhattacharya has joined **Coats in the United Kingdom** as **Chief Information Security Officer.** She will lead enterprise-wide cybersecurity strategy, governance, resilience, and risk management to enable secure digital transformation globally. Previously CISO at Danone, she led global cybersecurity transformation and D&I initiatives, and earlier held senior roles at EY and Deloitte, with engineering experience at Sun Microsystems and Infosys.

Santhosh Kempaiah joins ArcelorMittal Global Business & Technologies as GCC – CISO

Santhosh Kempaiah has taken on the role of **GCC – Chief Information Security Officer at ArcelorMittal Global Business & Technologies,** leading cybersecurity strategy and governance for the Global Capability Centre. He will strengthen security posture, risk management, and cyber resilience across global operations. With prior leadership roles at Visteon, Alfanar, Philips, Volvo Group, Tesco, and Thomson Reuters, he brings deep global security expertise.

Sukeshini Horannavar joins Randstad as Vice President & DPO

Randstad has appointed **Sukeshini Horannavar as Vice President & Data Protection Officer,** strengthening its global focus on data privacy, regulatory compliance, and responsible data governance. She will lead GDPR compliance, privacy risk management, and enterprise-wide privacy programs. With nearly two decades of experience at ITC Infotech, Genpact, Infosys, and TCS, she brings deep expertise in building and scaling privacy programs across large multinational organizations.

Devendra Pareek joins the National Skill Development Corporation as CISO

National Skill Development Corporation has appointed **Devendra Pareek** as **Chief Information Security Officer,** strengthening its focus on cybersecurity, compliance, and digital trust across India's skilling ecosystem. He will lead enterprise security strategy, cyber risk management, and governance. Previously CISO at Clix Capital and AU Small Finance Bank, Pareek brings strong expertise in cloud security, SOC implementation, infrastructure modernization, and regulatory engagement across financial services and the public sector.

Harshneel Nanche joins PayU Finance India as CISO

Harshneel Nanche has joined **PayU Finance India** as **Chief Information Security Officer,** strengthening the fintech's security, risk, and compliance posture. He will lead enterprise security strategy, cyber risk management, regulatory compliance, and incident response. Previously vCISO at Airtel Digital, and in senior roles at Piramal Capital and Vodafone Idea, Nanche brings deep experience across fintech, telecom, BFSI, and consulting.

Animesh Kumar joins BASIC Home Loan as Head of Information Security

Animesh Kumar has joined **BASIC Home Loan** as **Head of Information Security,** strengthening cybersecurity, data protection, and regulatory compliance. With over a decade of experience across BFSI, NBFC, and fintech, he will lead enterprise security strategy, risk management, and resilience. Previously CISO at UGRO Capital and founder of Raga Future Security, he brings deep expertise in SOC operations, cloud security, compliance, and audits.

Prashant Goyal joins Indus Towers as Head of Information Security

Prashant Goyal has joined **Indus Towers** as **Head of Information Security,** leading enterprise-wide cybersecurity strategy. He will oversee GRC, audits, security architecture, DPDP compliance, DevSecOps, monitoring, and third-party risk. Previously in senior roles at IndiGo, SBI Cards, and ANI Technologies (OLA), Prashant brings deep expertise across cybersecurity, data privacy, enterprise infrastructure, cloud, and regulated environments.

Digital certificates reveal enterprise security blind spots

Enterprises manage vast PKI estates but lack visibility, skills, and automation—turning digital trust into hidden risk

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

A PONEMON Institute study sponsored by CyberArk finds most organizations struggle to secure digital trust infrastructure. The January 2026 report surveyed 1,833 IT and security professionals globally, exposing major weaknesses in PKI and digital certificate management.

The staggering scale of the problem

Organizations manage an average of 114,591 internal certificates authenticating users, devices, and services. Yet only 46% express high confidence in PKI compliance. This widening gap between volume and control creates dangerous security exposure that many executives still fail to fully understand.

"In an era where digital trust underpins every transaction, ignoring PKI security is no longer an option."

What's breaking down

The report cites three PKI risks: misconfigurations at 50%, outages from expired certificates at 49%, and poor visibility at 38%. These risks are real, with 60% facing weak cryptography exploits, 58% third-party CA compromises, and 56% outages from expiration or configuration errors disrupting operations.

The resource crisis

Organizations are severely understaffed, with just four full-time employees typically managing PKI and only 42% having sufficient in-house expertise. As cryptographic use grows, 55% struggle to keep pace, pushing 63% to outsource PKI to managed security service providers due to rising complexity and scale.

Automation emerges as the answer

Forward-thinking organizations adopt automation, with 51% using automated certificate management for consistent execution, faster renewals, and better visibility. High performers lead in PKI compliance, use AI to predict issues, maintain stronger visibility, support skilled teams, and report fewer operational burdens with stronger security outcomes.

The road ahead

Looking ahead, unified visibility is the top priority for 34% of organizations. The mandate cutting public TLS certificate validity to 47 days by March 2029 is shaping modernization for half of companies. PKI security is at an inflection point; automation, visibility, and skills can create advantage, while delaying risks joining the 60% hit by certificate-related breaches. ■

India's GCC boom: From back office to global innovation engine

India's GCCs are shifting from cost centres to innovation hubs driving AI, product ownership, and enterprise transformation

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

THE INDIA GCC Thought Leadership Report 2025 by The Mainstream with NTT DATA highlights how India's GCCs are shifting from cost hubs to innovation and product centres. India hosts nearly 1,900 GCCs with two million professionals, projected to reach 2,500 centres and a $110 billion market by 2030.

From cost centres to innovation hubs

The report shows GCCs moving beyond arbitrage into mission-critical engineering, analytics, and transformation. Nearly 40% now see themselves as innovation hubs, led by BFSI, healthcare, and tech, with manufacturing catching up.

"What began as cost-focused delivery hubs is fast becoming centres of innovation, product ownership, and enterprise transformation."

AI, cloud, & cybersecurity take center stage

Technology priorities now center on Generative AI, hybrid cloud, and cybersecurity. Over 70% of GCCs invest in GenAI, cloud is everyday infrastructure, cybersecurity is non-negotiable, and competitiveness depends on scaling AI and secure-by-design platforms.

Talent: Quality over quantity

The talent model is resetting as GCCs shift from mass hiring to specialised skills in AI, data, cloud, and cybersecurity. Upskilling is central, demand outpaces supply beyond Tier-1 cities, compensation is rising, and flexible work and gig models are emerging to bridge skills gaps.

ESG moves beyond compliance

Sustainability is becoming a business driver beyond compliance. Over half of GCCs have adopted ESG policies and seek technology partners to track outcomes, but translating ESG intent into measurable impact needs better data, tools, and reporting frameworks.

Three constraints are holding GCCs back:

1. **Data and legacy IT debt** that limits AI impact
2. **Limited decision autonomy** for Indian leaders slowing innovation
3. **A perception gap** at global headquarters where GCCs are still seen as cost centres, not strategic partners.

The report calls this a "golden period" if leaders invest in AI-ready platforms, specialised talent, and global influence to lead product innovation. ■

CISO AGENDA 2026

MOVING BEYOND PREVENTION TO GOVERNING RISK, RESILIENCE, AND CONTINUITY

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

THE BREACH will happen. The only question is whether the organization is prepared to survive it. This is the defining leadership reality of 2026—reshaping how boards govern, CISOs communicate, and enterprises measure readiness in an era of deep digital dependence and rising, unchecked AI-driven threats.

For years, security was framed as a defensive wall: build it high enough, harden it well enough, and adversaries would stay out. That logic collapsed under agentic AI attacks, quantum risks, and credential sprawl. Today's attackers—faster, more adaptive, autonomous—exploit not just code and infrastructure weaknesses, but governance gaps, cultural blind spots, siloed decision-making, and executive misalignment. The wall metaphor is dead. Resilience is the only strategy.

Across India's largest enterprises, boardroom conversations are getting sharper. CISOs are being pushed to move beyond dashboards and alerts toward what truly matters at the board level: quantifying risk in financial terms, defining disruption tolerance, building AI-ready defenses, rehearsing crises, and strengthening governance for real-world breaches. Leaders are asking direct questions—what risk does this control reduce, and by how much?

This shift defines CISO Agenda 2026. Cybersecurity is no longer confined to technical teams—it is a board-level priority tied to business continuity, financial exposure, digital trust, and growth. Agentic threats demand faster response, quantum risks call for rethinking encryption, and evolving regulations require greater transparency and accountability.

Preventing every breach is unrealistic. The real test is whether leadership can manage one when it happens—with clear command, cross-functional alignment, and confidence in decisions. Organizations must start building and testing AI-driven defenses now or face the consequences later. Survival will depend on how well they can operate under uncertainty at speed.

How AI, quantum, governance, & resilience are reshaping security leadership

As AI scales, quantum risk nears, and governance intensifies, CISOs must redesign security for resilience, measurable risk, and board accountability

AS AI accelerates, quantum computing approaches, and regulatory scrutiny intensifies, the traditional CISO structure is being tested. The next phaserequires organizational redesign — not incremental improvement. How should the CISO function evolve over the next two to three years?

AI and quantum are at the doorstep

The first pressure point is technological disruption. AI is no longer experimental. Quantum computing is progressing rapidly, with increasing qubit capacities and the eventual mainstreaming of post-quantum cryptography (PQC).

This dual disruption demands structural change. A standalone CISO team cannot govern AI risk in isolation. What is required is an AI-focused cybersecurity center of excellence—a cross-functional unit that brings together operational risk, technology, business stakeholders, and security professionals.

The focus must operate on two fronts:

- **Securing AI** governance around models, platforms, data pipelines, and responsible AI adoption.
- **AI for Security** — embedding AI capabilities into detection, prevention, and response systems to counter AI-powered threats.

A critical extension of this transformation lies in identity and access management. AI agents must be treated like human identities — authenticated, authorized, monitored, and governed with regulatory rigor. Non-human identities, if improperly managed, can undermine both compliance and board confidence.

"The next phase requires organizational redesign — not incremental improvement."

Sameer Ratolikar
Group Head & CISO,
HDFC Bank

Building a cryptography foundation for the quantum era

The second structural shift involves cryptography. Today, encryption lifecycle management is often fragmented — certificate management in one unit, cipher tracking in another.

Preparing for PQC requires consolidation. CISOs should propose the establishment of a Cryptography Center of Excellence to oversee cipher standards, obsolescence management, AES-256 adoption, and cryptographic hygiene across applications, devices, and cloud environments.

This is not theoretical. As quantum capabilities expand, organizations must strengthen their cryptographic foundations before disruption arrives. In this context, cryptography becomes both hygiene and long-term strategy.

Governance that quantifies, not just complies

The third frontier is governance. Regulatory oversight now spans multiple authorities — domestic regulators, sectoral agencies, and global compliance regimes. We need to converge compliance and governance into a cohesive, metrics-driven function. The objective is to move from backward-looking reporting to forward-looking indicators.

For example, if a specific control initiative is implemented, how many vulnerabilities are expected to be reduced over the next quarter? What measurable risk reduction will follow?

Quantification builds transparency. Transparency clarifies risk appetite. Clarity, in turn, builds board trust.The shift is subtle but critical — from narrative-driven assurance to metrics-backed governance.

From disaster recovery to cyber resilience

The fourth priority is cyber resilience. Traditional focus areas — infrastructure protection, cloud hardening, and application security — remain essential. But the modern expectation goes further: how resilient is the business if systems fail?

In banking, digital disruption has immediate and public consequences. A mobile banking outage can trigger customer backlash within minutes. Resilience, therefore, must extend beyond the security function.

The answer lies in a cross-departmental cyber resilience team combining first-line defenders (technology and business units), second-line risk managers, and security leadership.This evolution reframes the CISO's role — not merely as protector of assets, but as guardian of business continuity.

The board's two enduring questions remain simple:

1. How will we prevent attacks?
2. If prevention fails, how resilient are we?

Elevating threat intelligence to the board

The fifth dimension is threat intelligence. Traditionally operational, threat intelligence rarely reaches the boardroom. That must change.

By integrating automated threat intelligence with proactive threat hunting and measurable dashboards, organizations can demonstrate tangible protection against emerging risks.

Quantification again becomes central. If credible intelligence surfaces regarding an external breach, the ability to run automated scans across internal systems and demonstrate defensive readiness creates confidence — not just within the SOC, but at the board room.

When operationalized and visualized effectively, threat intelligence becomes strategic capital.

To summarize, CISOs have five structural priorities:

1. AI security and AI-enabled defense capabilities.
2. A dedicated cryptography center of excellence.
3. Converged governance with measurable risk indicators.
4. Cross-functional cyber resilience frameworks.
5. Elevated, quantified threat intelligence.

Together, these shifts reposition the CISO organization for the next frontier.

These are not incremental upgrades. It was about organizational redesign — aligning cybersecurity with AI transformation, quantum preparedness, governance maturity, and board accountability.In the coming years, the most effective CISOs will not merely defend systems.

They will architect resilience, quantify risk, and demonstrate strategic value — long before the next disruption arrives.

Key Takeaways

- Security is now a board strategy.
- AI risk cuts both ways.
- Crypto is future defense.
- Metrics drive trust.
- Resilience is non-negotiable

Cyber readiness is a leadership imperative

As cyber incidents escalate into enterprise crises, leadership readiness, governance, and resilience, not just prevention, have become the true tests of cyber maturity

CYBER INCIDENTS today are not technical failures. They are enterprise crises that test leadership, governance, and organizational coherence in real time. For years, cybersecurity strategies have been framed around one central belief: build strong enough defenses, and breaches will not happen. That assumption no longer holds.

When systems are dynamic, and the nature of change is uncertain, prevention alone is insufficient. Attackers adapt faster than enterprise controls, and this asymmetry cannot be permanently closed by tools alone. There is a need for a strategic shift from control to resilience.

Organizations must move beyond the question: "How do we stop every breach?" To the more operationally honest one: "How do we stay functional when a breach inevitably occurs?" This reframes cyber risk from an IT issue to a business continuity mandate.

Increasingly, incidents are no longer isolated technical events but interconnected disruptions that ripple across supply chains, customer ecosystems, and regulatory environments. A single point of failure can trigger cascading consequences, amplifying financial, operational, and reputational impact. This interconnectedness demands that resilience be designed as a system-wide capability rather than a function owned by security teams alone.

Resilience is rehearsed, not declared

Readiness does not begin when an incident occurs.

"When systems are dynamic, and change is uncertain, prevention alone is insufficient."

Dr Durga Prasad Dube
Executive Vice President,
Reliance Industries

It is built long before — through repetition, simulation, and leadership rehearsal.

A playbook on paper is not readiness. Policies that collapse under pressure are not resilient. Real resilience is operational muscle memory. Teams that have rehearsed crisis response do not freeze when systems fail. They execute.

This matters most in the first hours of an incident — when leaders face incomplete information, executive scrutiny, and public pressure. Speed without authority creates chaos. What organizations need in that moment is not technical brilliance alone, but:

- Clear command structures
- Disciplined communication
- Predefined decision rights

Equally important is the ability to prioritize under pressure. Not every system can be restored simultaneously, and not every risk can be mitigated in real time. Leadership judgment—grounded in pre-agreed priorities—determines whether response efforts stabilize the organization or compound disruption.

Why siloed response models collapse?

Cyber incidents do not respect organizational boundaries. Yet most enterprises still respond as if they do.

When legal, communications, operations, risk, and executive leadership operate in silos, the organization fragments under pressure. Delays multiply. Accountability blurs. The response slows precisely when speed matters most.

Resilience should be governed — not merely operated. It requires:

- Predefined authority
- Cross-functional alignment
- Board-level sponsorship

Without governance, even the strongest technical response will be weakened by organizational friction.

The CISO as a confidence architect

The defining quality of effective cyber leadership is not technical mastery. It is institutional confidence. You will succeed because you have created confidence in the management above you.

However, confidence is built long before a crisis — through transparency, consistent communication, and visible preparedness. It cannot be manufactured during a disruption. In moments of uncertainty, boards and CEOs are not looking for dashboards. They are looking for:

- Clarity of command
- Credible timelines
- Assurance that someone is in control

The CISO's role, increasingly, is that of a confidence architect — someone who builds trust across the enterprise before it is tested.

Culture is the hidden control plane

Security culture is not awareness training. It is behavior when no one is watching. The strongest organizations embed cyber responsibility across functions — not just in the SOC. The most effective defenders are often not security professionals, but employees who understand how their actions affect resilience.

When teams act securely without regulatory pressure, culture is doing its job. Distributed ownership prevents small failures from cascading into systemic crises.

The board-level mandate

Cyber readiness is no longer optional oversight. It is a board-level responsibility. Digital infrastructure underpins revenue, trust, and operational continuity. Treating cybersecurity as compliance or a technical cost center is a strategic miscalculation.

Resilience is not about achieving zero breaches. It is about leadership readiness — the ability to absorb shocks, maintain continuity, and recover without paralysis.

In today's threat environment, the ultimate control is not a tool or a policy. It is leadership prepared to govern uncertainty.

Key Takeaways

- Cyber incidents are now enterprise crises.
- Speed without authority is ineffective.
- Siloed response models fail under pressure.
- Resilience is governed, not just operated.
- Leadership readiness is the ultimate control.
- Prevention-first security strategies are no longer sufficient.
- Attackers evolve faster than enterprise defense systems.
- Zero-breach thinking creates a false sense of security.
- Resilience must replace control as the core strategy.
- Cyber culture drives behavior beyond policies.

CISOs must become financial risk executives

As boards demand cyber risk be expressed in financial terms, CISOs are being pushed beyond technical security roles to become executives who quantify, govern, and manage enterprise risk

ACROSS GLOBAL boardrooms, a subtle but consequential shift is underway. The language of cybersecurity is changing. Color-coded heat maps, severity labels, and CVSS scores no longer carry the authority they once did. Boards are demanding clarity, not classification. They want to understand cyber risk in the same terms they use to evaluate other enterprise risks: financial exposure, operational disruption, and reputational impact.

In 2026, that expectation has hardened into a governance mandate. Unquantified risk is increasingly deprioritized. If it cannot be measured, it struggles to compete for investment.

From technical severity to business impact

The problem is not that technical metrics are wrong. It is that they are incomplete. Vulnerability rated "high" offers no insight into what the organization stands to lose. A CVSS score may describe exploitability, but it says nothing about business consequences. This technical language disconnects decision-making at the board level, where capital is allocated based on trade-offs rather than threat taxonomies.

Boards are not dismissing cyber risk. They are asking for it to be translated into impact. What revenue is at risk? What downtime could follow? What regulatory or brand consequences might materialize? Without that translation, cyber exposure remains abstract, and abstract risks rarely win budget.

"Cybersecurity is no longer a functional control. It is a governance discipline."

Rajeev Verma
Global Chief Information Security Officer
& Vice President,
SRF

Why quantification changes decisions?

Consider a simple analogy. Fifteen colleagues plan to watch a film. Ten have arrived; five may or may not. Buying fifteen tickets "just in case" is a guess. Making a few calls to confirm attendance turns uncertainty into a number that supports a rational choice.

This is the logic boards expect from cybersecurity leaders. When a CISO says a vulnerability is "critical," the board has no reference point for what action is required. When the same risk is framed as a probable four-million-dollar loss, the conversation shifts from fear to economics. Exposure becomes a business problem, not a technical abstraction.

The governance shift behind the boardroom pressure

Several forces are converging to make this shift unavoidable. Regulators now expect boards to demonstrate oversight of cyber risk, not just delegate it to IT. Investors are linking cyber incidents to financial performance and governance quality. Insurers, once content with surface-level questionnaires, are demanding evidence of quantified risk management and are adjusting premiums and coverage based on maturity.

This is why resilience is governed, not just operated. Cybersecurity is no longer a functional control. It is a governance discipline, subject to the same scrutiny as financial risk, supply chain risk, or regulatory exposure.

The frameworks boards can act on

Quantification does not mean false precision. It means disciplined estimation. Models such as FAIR (Factor Analysis of Information Risk) provide a structured way to express risk as probable financial loss, rather than color-coded severity. Monte Carlo simulations add realism by modelling thousands of scenarios, producing ranges of potential outcomes rather than a single, alarmist worst-case.

Together, these approaches allow CISOs to make a decision-grade argument: if the expected loss from a threat materially exceeds the cost of mitigation, the investment case is rational. Boards do not need certainty. They need defensible ranges they can weigh against other strategic priorities.

Why CISOs must act as Risk Executives now

This shift changes the CISO's role. Effective quantification requires access to revenue data, operational dependencies, regulatory exposure, and brand risk. A security leader modeling the impact of a plant shutdown must understand the plant's contribution to revenue and customer commitments. This demands partnership with finance, operations, and enterprise risk.

CISOs who can translate technical exposure into financial impact are no longer security specialists briefing the board. They are risk executives shaping capital allocation. Their credibility increasingly rests not on how well they understand threats, but on how clearly they can connect those threats to enterprise value.

Leadership readiness is the ultimate control

Boards will always ask a rational question: "We have operated for years without a major incident. Why invest now?" The only credible answer is not technical urgency, but quantified exposure. Here is what is at stake. Here is the probability. Here are the costs of prevention versus the costs of inaction.

In 2026, leadership readiness is the ultimate control. Cyber resilience is no longer about how many vulnerabilities are patched. It is about whether leadership can govern uncertainty, priorities based on impact, and make informed trade-offs under pressure.

For CISOs, mastering financial risk quantification is no longer a communication skill. It is the price of admission to the boardroom.

Key Takeaways

- Boards demand clarity.
- Unquantified risk is de-prioritized.
- Technical language disconnects decisions.
- Translate exposure into impact.
- CISOs are risk executives.
- Cyber risk must be framed in financial terms.
- Severity scores fail to convey business con sequences.
- Abstract risks rarely secure board-level investment.
- Quantification shifts conversations from fear to economics.
- Financial exposure drives faster, clearer decision-making.
- Governance expectations are rising across regulators and investors.

Agentic AI is rewriting the rules of cyber defense

Agentic AI enables autonomous cyberattacks that can plan, adapt, and execute at machine speed. Enterprises must build equally autonomous, AI-native defenses to remain resilient

THE CYBER threat landscape is no longer defined solely by human hackers. It is being reshaped by autonomous systems powered by agentic AI — machines capable of planning, adapting, collaborating, and executing attacks with minimal or no human direction.

If the cloud defined the last decade of enterprise transformation, AI will define the next. Just as organizations once hesitated before embracing the cloud, they now stand at a similar inflection point with AI. The difference this time is speed. The shift is faster, deeper, and significantly more disruptive.

From assistive AI to agentic systems

AI's evolution has been swift. It began as assistive tools — chatbots, ticketing automation, screening systems. It then progressed to intelligent agents capable of executing discrete tasks. Today, we are entering the era of agentic AI: multiple autonomous agents collaborating, planning, and executing complex workflows across development, operations, and deployment environments.

These agents can "wear multiple hats," functioning as developers, DevOps engineers, testers, and deployment managers. The concern is that adversaries now have access to the same capabilities.Autonomous systems can independently conduct reconnaissance, scan APIs, apply known vulnerabilities, adapt attack vectors in real time, and attempt exploitation without waiting for human instruction. The attack surface is not merely expanding — it is accelerating.

"If your defense is not autonomous, it is not resilient."

Ravi Prakash Burlagadda
Senior Vice President - Information Security, Jio Platforms

Autonomous attacks are here

Take a look at the multi-agent AI platforms that integrate across email systems, file storage, collaboration tools, and external interfaces. These systems can access centralized credentials, interact with multiple enterprise touchpoints, and execute tasks at scale.

What makes them dangerous is not just access, but autonomy. Once embedded, they can pivot, escalate privileges, modify tactics, and conceal activity dynamically.

Enterprise-grade AI copilots are now capable of designing systems, writing code, testing deployments, and potentially identifying exploitable weaknesses within the same environment. If machines can build at scale, machines can attack at scale.

AI adoption is no longer optional

Technology leaders are signaling a decisive shift: AI is becoming foundational infrastructure. Just as calculators and smartphones became ubiquitous tools, AI will soon be embedded across industries — from education and HR to IT and cybersecurity.

For enterprises, the question is no longer whether to adopt AI, but how to adopt it securely. This requires asking hard questions:

- Are we threat-modeling AI systems effectively?
- Do we have an AI-specific Secure Development Lifecycle?
- Are we validating model provenance, vulnerabilities, and community contributions?

AI integration is not merely a deployment decision. It is a risky decision.

Rethinking security for AI-native systems

Traditional monitoring approaches are no longer sufficient. Capturing OS logs and database transactions is table stakes. Organizations must now monitor sanitized prompts, model responses, behavioral anomalies, and runtime deviations.

Prompt injection, model manipulation, and response tampering introduce entirely new attack vectors. Guardrails must operate at both request and response levels, while runtime behavior must be continuously evaluated.

If an AI model behaves anomalously, containment strategies must extend beyond endpoints. Just as compromised devices are isolated, compromised models may need to be automatically removed from the network. Equally critical are rollback mechanisms that allow organizations to revert to previous model versions after flawed upgrades.In this new paradigm, the model itself becomes a governed security asset.

AI agents are high-privilege identities

AI agents should be treated as high-privilege service accounts within the enterprise ecosystem. They require least-privilege access, multi-factor authentication, robust session controls, and granular database permissions. If an agent connects to CRM or SAP systems, its access must be tightly constrained — table by table, use case by use case.

Zero Trust principles do not diminish in the AI era. They intensify

Toward autonomous defense

As adversaries become autonomous, defense must evolve accordingly. Security Operations Centers can no longer rely solely on manual triage or basic anomaly detection. They must incorporate AI-driven detection, automated containment, and intelligent orchestration of responses.

Security governance must span the entire AI lifecycle — from design and development to deployment and decommissioning. Enterprises must invest in AI-aware development methodologies, autonomous monitoring capabilities, and governance frameworks that align risk, technology, and operational accountability.If your defense is not autonomous, it is not resilient.

In the era of the autonomous adversary, resilience will belong to organizations that teach their defenses to think, adapt, and act — at machine speed.

Key Takeaways

- Autonomous agents redefine the threat of actors.
- The autonomous threat is operational now.
- Legacy detection is blind to autonomy.
- Defend with adaptive, AI-driven resilience.
- Prepare for adversaries that never sleep.
- Agentic AI enables machine-speed cyberat tacks.
- Attack surfaces expand as AI systems scale.
- Multi-agent systems can plan and execute attacks.
- Adversaries can adapt tactics in real time.

Digital platforms are now the security perimeter

As cloud-native platforms scale India's digital economy, security has shifted from the network edge to the platform core

INDIA'S DIGITAL economy is scaling at an extraordinary speed. Cloud-native platforms, API-driven services, and multi-cloud architectures are now the backbone of payments, commerce, logistics, healthcare, and financial services. But the very platforms powering this growth have quietly become the new perimeter of the enterprise. And that perimeter is under constant, largely invisible pressure.

For security leaders, the warning is clear: platform risk is no longer a technical concern. It is a business risk. It directly affects service availability, customer trust, and regulatory exposure, making it inseparable from enterprise performance and continuity.

When speed outruns governance

Cloud adoption has delivered unprecedented agility. Infrastructure that once took months to provision is now spun up in minutes. But this velocity has outpaced the governance models designed to secure it.

Policies built for static, on-premise environments cannot keep up with dynamic, ephemeral cloud workloads. As platforms scale faster than controls, security gaps emerge by default. In this environment, speed without governance becomes a liability. The attack surface expands not because organizations are careless, but because their operating model has changed faster than their security architecture. Governance must therefore evolve in parallel with scale, not follow it.

"If platforms are the new perimeter, APIs are the new front door."

Rama Devi Sangu
Chief Information Security Officer,
Hindustan Zinc

Why network-centric security no longer works?

The old perimeter has dissolved. Firewalls and network segmentation were built for a world where applications lived in defined locations and users connected from known endpoints. That world no longer exists.

Hybrid work, SaaS, and multi-cloud architectures have broken the logic of network-centric security. The perimeter is no longer where traffic enters the network. It is wherever identity, APIs, and platform services expose business functionality. Defending yesterday's perimeter leaves today's platforms dangerously exposed.

Control must move closer to identity and workload context.

APIs are the new front door

If platforms are the new perimeter, APIs are the new front door. They are the connective tissue of modern digital services and, increasingly, the primary attack vector.

Vulnerabilities such as Broken Object-Level Authorization allow attackers to access data through seemingly legitimate API calls. For platforms handling millions of users and transactions, a single misconfigured endpoint can cascade into systemic exposure. Yet many enterprises cannot even enumerate their APIs, let alone govern them continuously.

Without discovery, there is no defense. APIs multiply by design. Visibility must scale with them. Continuous monitoring and classification are no longer optional capabilities but operational necessities.

Platforms must defend themselves

This means enforcing least privilege by default, eliminating standing credentials, and designing identity-first controls into cloud services and applications. Service accounts, often created for machine-to-machine interactions, are now one of the most abused attack paths when poorly governed. When compromised, they enable attackers to gain lateral movement across the cloud, SaaS, and even directory services.

Platforms that cannot enforce their own security controls become force multipliers for attackers. The defensive model must shift from perimeter enforcement to platform-native protection. Security must operate as a built-in function, not an external overlay.

The multi-cloud visibility gap

Multi-cloud strategies promise resilience and commercial leverage. They also create a visibility problem. Assets drift across environments. Configurations diverge. Accountability fragments across teams and tools.

The result is not just complexity. It is a blind spot. When no single function can see the entire platform estate in real time, risk accumulates silently until it manifests as disruption. Unified visibility and shared accountability are critical to closing this gap.

Platform risk is business risk

When platforms fail, the impact is immediate and material. Regulatory exposure, financial penalties, service disruption, and erosion of trust follow quickly. For platforms embedded into India's critical digital infrastructure, security failures are not isolated incidents. They are business events with national-scale consequences.

Digital trust is now a balance-sheet asset. Architecture defines resilience. And in an economy where digital platforms mediate everything from payments to public services, securing those platforms is no longer solely the responsibility of security teams. It is a leadership mandate.

The invisible frontlines of India's digital economy are no longer at the network edge. They are inside the platforms themselves.

Key Takeaways

- Platforms are the new perimeter.
- Speed has outpaced governance.
- Network-centric security fails.
- Platforms must defend themselves.
- Platform risk equals business risk.
- Cloud-native platforms now define enterprise attack surfaces.
- Security gaps emerge as platforms scale faster than controls.
- Static policies cannot secure dynamic cloud environments.
- Perimeter-based defenses fail in hybrid, multi-cloud architectures.
- APIs have become the primary enterprise attack vector.
- Lack of API visibility creates systemic exposure risks.
- Identity-first security is critical in platform architectures.

How much disruption can your board tolerate?

Cyber resilience requires boards to explicitly define acceptable disruption, downtime, and loss through formal risk appetite statements

CYBER RESILIENCE cannot remain an abstract aspiration embedded in technical controls and dashboards. It must be explicitly defined, debated, and governed at the board level through enterprise risk appetite statements.In other words, resilience is not about installing more controls. It is about drawing clear boundaries.

The Abhimanyu problem in cybersecurity

Let's look at an analogy from the Mahabharata. Abhimanyu knew how to enter the Chakravyuh but did not know how to exit. Many enterprises, approach cybersecurity in much the same way. Organizations invest heavily in prevention and detection. But have they clearly defined how much downtime they can tolerate? How much data loss is acceptable? Which assets must never fail? Where is the "Lakshman Rekha" — the line that, if crossed, becomes existential?

If no line is drawn, it will inevitably be crossed. This is not a technical question. It is a governance question.

Hope is not a strategy

When incidents occur, many leaders rely on optimism — strong vendors, capable partners, experienced teams. But hope does not restore operations.

Recovery requires predefined decisions. Boards must agree in advance on recovery priorities, acceptable trade-offs, and tolerance thresholds. Without that clarity, crisis decisions become reactive and chaotic.

Regulatory frameworks, including India's evolving data protection regime, add urgency. Yet com-

Cyber resilience requires boards to explicitly define acceptable disruption, downtime, and loss through formal risk appetite statements.

Urvish Acharya
Head - Information Technology Governance & Risk, Birla Carbon

pliance alone does not define resilience. The real challenge lies in determining how the enterprise will function when controls fail.

Because eventually, something will fail.

Equal protection is not strategic protection

Many organizations apply the same security baseline across all assets.But not all assets are equal.Crown jewels demand differentiated protection. A CxO's workstation and a general employee's device may not warrant identical safeguards. Critical operational systems require elevated and layered defenses.

Resilience is fundamentally about prioritization. Boards must understand which assets are indispensable and which risks are tolerable. Without prioritization, organizations dilute protection rather than strengthen it.

Tabletop exercises that expose the gaps

Resilience cannot be theorized. It must be practiced. Consider the outcomes to questions like:

- What if operations in a critical region were dis rupted for three months?
- What if internet connectivity failed nationwide?
- What if a pandemic struck again?
- What if a third-party partner was compromised?
- What if nothing was technically broken, but stakeholders believed it was?

The outcomes can be sobering. Unclear dependencies, undefined escalation paths, incomplete global coordination plans are possibilities.Only by rehearsing such scenarios can leadership teams recognize vulnerabilities—and begin addressing them.

Governance over assumption

Cyber resilience must be codified in enterprise risk appetite statements.That means answering explicitly:

- What is the maximum tolerable downtime for critical systems?
- What level of data loss is acceptable?
- Which functions must be restored first?
- At what point does financial risk outweigh the cost of operational restoration?

Without board-level clarity, CISOs will be left making implicit decisions during explicit crises.

Resilience, therefore, is less about technical strength and more about governance maturity.

From technical control to executive accountability

As enterprises look toward 2026 and beyond, leaders should reframe the conversation. Security is not merely about preventing breaches. It is about defining acceptable disruption and preparing the organization to operate within those boundaries.

The board must own the risk appetite. The CISO must facilitate the dialogue.

In an era of escalating cyber threats, resilience is not about promising invincibility. It is about establishing clarity — knowing what can be protected, what may be sacrificed, and how quickly the enterprise must recover. Because if disruption is inevitable, tolerance must be deliberate.

If disruption is inevitable, tolerance must be defined

That deliberation cannot remain theoretical. It must translate into measurable thresholds, agreed escalation paths, and clearly defined ownership across business and technology functions. Without this, even well-articulated risk appetite statements fail in execution.

Boards must move beyond periodic reviews to continuous engagement with cyber risk. This includes tracking resilience metrics, validating recovery assumptions, and ensuring that business leaders, not just security teams, understand their roles during disruption. Cyber resilience is sustained through alignment, not documentation.

Equally critical is the integration of resilience into enterprise planning cycles. Business continuity, disaster recovery, and cyber response cannot operate as parallel tracks. They must converge into a single, coordinated framework that reflects how the organization actually operates under stress.

The role of the CISO, therefore, extends beyond risk identification. It includes translating technical risk into business impact, enabling informed decision-making, and ensuring that resilience commitments are realistic, tested, and enforceable.

Ultimately, resilience is a leadership discipline. It reflects how clearly an organization understands its priorities, how decisively it can act under pressure, and how consistently it can recover without losing trust.

Key Takeaways

- Resilience begins with risk acceptance.
- Ambiguity creates fragility.
- Resilience without prioritisation is illusory.
- Let risk appetite drive architecture.
- Clarity of appetite enables clarity of action.

The next growth leap depends on cyber-ready boards

India's digital economy is accelerating, and boards must move cyber resilience from an IT response function to a core enterprise strategy that governs risk, crisis management, and business continuity

AS INDIA moves toward becoming the world's third-largest economy, the conversation around growth cannot be separated from resilience. Resilienceis not about how quickly an organization recovers after an incident. It is about how the enterprise is architected to withstand disruption in the first place. "Secure by design" and "resilient by architecture" are not buzzwords. They are strategic imperatives.

The myth of 100 percent recovery

One of the most persistent illusions in boardrooms is the belief that full recovery is always possible. Most CIOs and CISOs express confidence that they can recover from a major cyber incident. The reality is far more sobering. Complete restoration rarely happens. Partial recovery is far more common than organizations admit.

In a world where "100 percent security does not exist," resilience shifts from the pursuit of perfection to a discipline of preparedness. As threats evolve — amplified by AI-driven attacks and geopolitical tensions — static defenses are no longer sufficient.

From check-the-box to crisis-ready

Many enterprises continue to treat incident response and business continuity as compliance exercises. A documented playbook does not equal resilience. It must be practiced, stress-tested, and aligned with real business dependencies.

Recovery Time Objectives and Recovery Point

Cyber resilience is not "the CISO's baby." It is a shared enterprise responsibility.

Pradipta Patro
Head of Cyber Security & IT Platform, KEC International

Objectives cannot remain technical metrics buried in IT dashboards. They must reflect operational priorities and board-level risk appetite. Cyber risk, he emphasized, is not "the CISO's risk." It is an enterprise risk and must be embedded within the ERM framework.

Governance, transparency, and trust, therefore, become central. In moments of crisis, executives do not want technical jargon. They want clarity and assurance.

The expanding attack surface

The cyber threat landscape is not just intensifying; it is diversifying. Ransomware variants continue to evolve, and attack frequency is rising sharply, with thousands of incidents occurring weekly in India alone. Globally, cybercrime costs run into trillions of dollars annually.

Simultaneously, AI introduces new vectors — misinformation, automated exploitation, and trust manipulation. Regulatory scrutiny is tightening. India's evolving data protection framework, including the DPDP regime, carries the risk of significant penalties for non-compliance.

In this environment, resilience must extend beyond IT systems. It must encompass operational technology, critical infrastructure, supply chains, utilities, and human behavior. A delayed power grid, a compromised GPS, or a halted manufacturing line is no longer theoretical. It is an operational reality.

The board's new responsibility

Boards are increasingly aware of their accountability. However, awareness must translate into structured crisis governance. Decision-making during incidents cannot be outsourced to vendors or delegated unquestioningly to service providers. The CISO must provide contextual judgment and strategic confidence, grounded in business priorities.

This demands a shift from reactive response to strategic resilience. Technology alone cannot deliver this transformation. Misconfigured "best-of-breed" tools can create a false sense of security. True resilience integrates architecture, governance, human confidence, and cross-functional coordination.

Building the enterprise resilience stack

Risk transfer mechanisms, such as cyber insurance, may mitigate financial exposure, but they do not substitute for operational readiness. So, what does executive-grade cyber resilience look like?

- Practiced incident simulations that involve leadership, not just IT teams.
- Clear alignment among cybersecurity, ERM, and business continuity.
- Investment in detection, response automation, and backup integrity.
- Transparent communication frameworks that withstand regulatory and media scrutiny.
- A culture of cyber awareness is embedded across the enterprise.

Resilience as competitive advantage

As India's digital economy accelerates, resilience becomes a strategic differentiator. Trust, once broken, is difficult to rebuild. Increasingly, investors, regulators, and customers evaluate organizations not by whether they were breached, but by how transparently and effectively they responded.

Speed of response matters, but resilience is fundamentally a mindset. It must be embedded in architecture, reinforced through governance, and demonstrated in crisis.

In an era where breaches are inevitable, resilience is no longer defensive hygiene. It is executive leadership in action.

Key Takeaways

- Breaches are no longer a matter of "if," but "when."
- The quality of response ultimately defines organisational reputation.
- Technical responses alone are no longer sufficient in managing crises.
- True resilience reflects leadership under sustained pressure.
- Organisational resilience is a key driver of long-term trust.
- Complete recovery after cyber incidents is rarely fully achievable.
- Resilience replaces the outdated illusion of perfect security.
- Preparedness consistently matters more than the pursuit of perfect prevention.
- Playbooks must be regularly practiced, not merely documented.
- RTO and RPO should be closely aligned with evolving business priorities.
- Cyber risk must be treated as an enterprise-wide responsibility.

Cyber crisis response depends on governed automation

Cyberattacks unfold at machine speed, and effective crisis response increasingly depends on automation governed by clear policies, human oversight, and accountable decision frameworks

THE ATTACK surface of the modern enterprise has outgrown the playbook. Digital estates now span multi-cloud environments, third-party ecosystems, and globally distributed operations.

Adversaries exploit this complexity at machine speed. Manual, human-centric response models were built for a slower era. Today, they are structurally mismatched to the pace of modern attacks.

This is why automation is no longer a luxury. It is an operational necessity. The question facing security leaders is no longer whether to use AI in crisis response, but how to govern it without losing control.

Speed has changed the economics of defense

One simple comparison illustrates the asymmetry. A team of security specialists may spend half a day crafting a realistic phishing simulation. AI can generate comparable lures in minutes. Attackers are already operating at that tempo. Defenders who rely on human capacity alone will always be late to the breach.

Regulatory pressure compounds this reality. Incident reporting timelines are tightening globally, demanding rapid triage, documentation, and executive updates. Teams already stretched thin are expected to move faster, with greater precision, under greater scrutiny. In this environment, speed without automation becomes a constraint. Automation without governance becomes a liability.

"In a cyber crisis, trust is the true currency."

Ranjan Revandkar
Chief Information Security Officer,
PI Industries

Why human-centric response has reached its limits?

Traditional incident response models assume that humans sit at the center of every decision loop. That assumption no longer holds under machine-scale attack volumes. When alerts flood in by the thousands, human judgment becomes a bottleneck. Fatigue and inconsistency creep in just when precision matters most.

This does not diminish the role of people. It redefines it. Humans are no longer effective as the primary execution engine of crisis response. They are essential as governors of automated systems, defining boundaries, priorities, and escalation paths. The future response model is not human-only or AI-only. It is governed by automation.

Build guardrails, not just speed

Unbounded automation introduces new risks. An AI system that blocks legitimate board access, shuts down a production environment, or isolates a critical partner based on a misclassification can cause more harm than the attack it seeks to contain.

This is why automation must be designed with explicit guardrails. Tasks should be categorized: those AI can execute independently, those requiring human approval, and those reserved for human decision-making. Explainability and reversibility are non-negotiable. Every automated action must be traceable to a policy, a trigger, and a playbook. In a crisis, speed matters. But speed without control erodes trust.

Where AI creates real leverage

Within governed boundaries, AI delivers decisive advantages. It can ingest and correlate telemetry at scale, document evidence for regulators, manage identity and access in real time, and maintain continuous audit trails of decisions taken during an incident. These mechanical burdens slow human responders and introduce errors under stress.

AI excels at volume. Humans excel at intent. Adversaries with strategy and objectives drive sophisticated attacks. Anticipating those moves, weighing business trade-offs, and deciding when to absorb risk versus disrupt operations remains a leadership responsibility. Automation accelerates response. Judgment determines direction.

Resilience is engineered through governance

The ultimate objective is not autonomous defense. It is a resilient response. Governed automation allows organizations to move at machine speed while preserving human authority over outcomes. It embeds trust into the response process by making actions explainable, accountable, and reversible.

In a cyber crisis, trust is the true currency. Boards and regulators do not just ask what happened. They ask why actions were taken and who was accountable for them. Automation that cannot explain itself undermines credibility. Automation that operates within clear governance frameworks strengthens it.

The future of cyber resilience is not about deploying more AI. It is about governing how automation acts when the clock is ticking.

Key Takeaways

- Automation must be governed, not just deployed.
- Automation is a necessity, not a luxury.
- Human-centric response is obsolete.
- Build guardrails, not just speed.
- Governed automation = resilient response.
- Cyberattacks now operate at machine speed.
- Manual response models cannot match attack velocity.
- Speed without governance creates operational risk.
- Automation without control erodes enterprise trust.
- Humans must shift from operators to governors.
- AI excels at scale, humans at strategic judgment.
- Guardrails define boundaries for automated actions.
- Explainability and reversibility are critical in crises.
- Regulatory timelines demand faster, auditable responses.
- Resilience is built on accountable, governed automation.

Talent strategy is a security strategy

Digital complexity accelerates, cybersecurity resilience increasingly depends on how organizations attract, develop, and retain talent—not just the technologies they deploy

INDIA'S DIGITAL economy is scaling at a remarkable speed. Cloud adoption, AI integration, regulatory mandates such as the DPDP Act, and aggressive digital transformation agendas are reshaping how enterprises operate. Yet, beneath this momentum sits a structural constraint no technology investment can overcome: the cybersecurity workforce is not growing fast enough to secure the systems being built.

This is not a temporary hiring challenge. Talent scarcity in cybersecurity is structural. And as complexity rises, the gap between what enterprises are building and what humans alone can secure is widening.

When complexity exceeds human capacity

Modern digital estates now span cloud platforms, SaaS ecosystems, operational technology, APIs, and AI-driven workloads. Each layer introduces new control surfaces, compliance obligations, and threat models. The result is operational complexity that exceeds what even well-resourced security teams can absorb through manual effort.

The numbers reflect this strain. Even a conventional cybersecurity role can take six to nine months to fill. For specialized skills in OT, cloud, or AI security, hiring cycles stretch out further. Global leadership surveys show that a majority of CEOs now cite skills gaps as their most persistent cybersecurity constraint. This is not a local anomaly. It is a systemic bottleneck.

"Digital transformation fails when the human layer cannot keep pace with complexity."

Ambarish Kumar Singh
Chief Information Security Officer,
Godrej Enterprises Group

Why headcount-based planning is failing?

Many organizations still approach cyber capability as a hiring problem: when risk rises, add people. That model no longer works.

Post-pandemic, enterprises that previously lacked formal security functions rushed to build teams from scratch. Demand surged across every role simultaneously, from GRC to application security to industrial cybersecurity. The talent pipeline did not expand at the same pace. The market response has been predictable: organizations poach from one another, recycling the same limited pool of professionals. Every hire leaves a gap somewhere else.

Headcount-based planning fails because it assumes an elastic workforce. In reality, the supply of skilled cyber talent is constrained, and the complexity of the environment is compounding faster than hiring can keep up.

The fragility of "hero" security teams

Many security programs quietly depend on a handful of indispensable individuals. When these "heroes" leave, capability drops overnight—projects stall. Institutional memory disappears. Remaining team members absorb unsustainable workloads, increasing burnout and the risk of attrition.

Compensation alone does not solve this fragility. Retention is shaped by whether professionals see a future in the organization: credible career paths, leadership backing, psychological safety, and the sense that their work is part of a coherent strategy rather than a perpetual emergency.

Workforce realism is strategy

The more resilient organizations are rethinking the workforce model itself. Automation is absorbing routine operational load. Managed services and partner ecosystems are being used to scale capabilities that cannot be built internally at speed. Fresh graduates are deliberately hired and developed, rather than relying solely on lateral hiring in an exhausted market.

This is workforce realism: accepting that talent scarcity is structural, that complexity exceeds human capacity, and that strategy must adapt accordingly. Cyber capability cannot be planned as a static team size. It must be architected as a system that blends people, automation, and partners by design.

Why talent strategy is security strategy?

The most important shift is cultural. Workforce planning cannot remain an HR afterthought triggered by resignations. For CISOs, people strategy is now a core part of security architecture. It shapes resilience as directly as any tool or control.

Digital transformation does not fail because technology falls short. It fails when the human layer cannot keep pace with complexity—in cybersecurity, acknowledging that reality is not pessimism. It is a strategy.

As CISOs, we must embed people strategy into our cybersecurity strategy, take initiatives to expand the pool of cybersecurity professionals, and ensure we build a team that will dare for cybersecurity.

The future of cyber resilience is not about deploying more AI. It is about governing how automation acts when the clock is ticking.

Key Takeaways

- Talent scarcity is structural.
- Complexity exceeds human capacity.
- Headcount-based planning fails, design for scarcity.
- Workforce realism is a strategy.
- Cybersecurity workforce gaps are widening globally.
- Hiring cycles lag behind rising security demands.
- Poaching recycles talent, not expands capacity.
- Talent strategy is now core to cyber resilience.

Conclusion

The CISO Agenda 2026 makes one thing unmistakably clear: cybersecurity is no longer a technical function operating at the edge of the enterprise. It is now central to growth, governance, and business survival. The leaders shaping this next phase are not merely defending systems; they are quantifying risk, defining resilience, governing automation, preparing for AI-led disruption, and building trust at the board level.

In a world where breaches are inevitable and uncertainty is constant, competitive advantage will belong to organizations that can absorb shocks without losing direction. The future of cyber leadership, therefore, is not about control alone. It is about readiness, resilience, and responsible growth. ■

Securing enterprises at machine speed against AI-driven cyber threats

Diwakar Dayal says CISOs must adopt autonomous, explainable AI security to counter machine-speed attacks and identity-driven risks

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

IN AN era where cyber threats evolve at machine speed, traditional security approaches are rapidly becoming obsolete. India witnessed a staggering doubling of cybersecurity incidents to 22.68 lakh in 2024, while attackers leverage AI to automate phishing, identity abuse, and lateral movement at an unprecedented scale. For Chief Information Security Officers navigating this volatile landscape, the challenge is stark: human-in-the-loop defenses cannot keep pace with attacker velocity.

In an interaction with CISO Forum, Diwakar Dayal, Managing Director and Area Vice President at SentinelOne India & SAARC, shares critical insights on operationalizing autonomous AI defenses, tackling shadow AI proliferation, and executing Zero Trust at scale. As regulatory frameworks like CERT-In directives and the DPDP Act reshape compliance expectations, Dayal outlines how CISOs can balance automation with accountability while building truly cyber-resilient organizations for 2026 and beyond.

CISO Forum: AI-driven attacks are now operating at machine speed. How should CISOs rethink detection and response when human-in-the-loop is no longer fast enough?
DIWAKAR DAYAL: CISOs must pivot to fully autonomous, agentic AI platforms that operate at attacker velocity to stay ahead. Embrace autonomous AI defenses by transitioning to agentic platforms like SentinelOne's Singularity Platform for instant triage, investigation, and remediation, bypassing human delays for routine threats.

Enable machine-speed reasoning with real-time exploit prediction and correlation to match attacker velocity, especially amid India's cybersecurity incidents, which doubled to 22.68 lakh in 2024. Streamline SOC operations by automating alert overload (thousands per minute), freeing analysts for strategic focus amid escalating AI threats.

"By 2026, cyber-resilient organisations will operate at machine speed with human accountability."

CISO Forum: Shadow AI and unsanctioned models are proliferating inside enterprises. What new risk vectors does this create for CISOs, and how can they regain visibility and control?regions and regulatory landscapes?
DIWAKAR DAYAL: Shadow AI creates serious governance and data protection risks. Employees using unsanctioned generative AI tools may unknowingly push sensitive data beyond enterprise controls, increasing the risk of IP leakage and non-compliance with the DPDP Act. For CISOs, the core challenge is the loss of visibility into where data is going, how it is processed, and which AI models are involved. Regaining control requires continuous discovery, stronger governance, and security controls that work at machine speed without slowing innovation.

Key focus areas for CISOs:

- New risk vectors: Unapproved AI tools may store prompts and files externally with little logging, increasing the risk of sensitive data and IP exposure.
- AI-powered discovery: Use agent-based visibility to continuously monitor network traffic, APIs, and SaaS environments to detect shadow AI usage in real time.
- Integrated controls: Combine discovery with DLP and CASB to enforce data protection across hybrid and cloud environments.
- Clear governance: Define approved AI tools, usage guidelines, and regular reviews to turn shadow AI from a hidden risk into governed innovation.

CISO Forum: Attackers are using AI to automate phishing, identity

abuse, and lateral movement. How does this shift the economics of cyber defence for Indian organisations with limited security talent?
DIWAKAR DAYAL: AI has commoditised cyberattacks, making phishing, impersonation, and credential abuse cheap, fast, and highly scalable. This directly challenges Indian organisations already facing a chronic cybersecurity skills shortage. The economics of defence now favour automation. Autonomous SOC platforms can handle the majority of investigations without constant human intervention, reducing dependence on scarce talent while significantly improving response speed. With CERT-In consistently flagging phishing and credential abuse as dominant attack vectors, early detection and automated containment are essential to limit business disruption, financial impact, and regulatory exposure.

CISO Forum: Zero Trust is a regulatory priority in India, but it is hard to execute at scale. How can autonomous, agentic AI operationalize Zero Trust in the SOC?
DIWAKAR DAYAL: Zero Trust often fails in practice due to legacy systems and outdated assumptions that internal environments are inherently safe. That model no longer holds.

Autonomous, agentic AI allows Zero Trust to move from theory to daily operation. Platforms like Singularity continuously validate identities, devices, and behaviours across endpoints, cloud workloads, and SaaS environments, using live risk signals and device posture rather than static rules.

By automating investigations and responses, these platforms reduce reliance on manual processes, which is critical given India's cybersecurity talent gap. More importantly, this approach brings enterprise-grade Zero Trust capabilities to SMBs at a time when India's rapid AI adoption is placing unprecedented stress on existing security models.

> **"CISOs must pivot to fully autonomous, agentic AI platforms that operate at attacker velocity to stay ahead."**

CISO Forum: Identity has become the primary attack surface. How should CISOs evolve identity security as AI agents, bots, and non-human identities multiply across the enterprise?
DIWAKAR DAYAL: As AI agents, bots, APIs, and service accounts multiply, identity security must extend beyond humans. Non-human identities often operate with excessive privileges and limited oversight, making them attractive targets for attackers. CISOs should adopt AI-driven platforms that continuously monitor identity behaviour, automatically detect compromise, enforce credential rotation, and limit blast radius. Built-in audit trails and explainable AI actions are critical to support CERT-In reporting and compliance with the DPDP Act. Given that phishing and credential abuse remain leading attack vectors in India, CISOs should assume identity compromise is inevitable and design controls accordingly.

CISO Forum: With CERT-In directives and the DPDP Act in play, how can CISOs balance autonomous security controls with compliance, auditability, and accountability?
DIWAKAR DAYAL: Indian regulations do not restrict automation; they demand explainable automation. CISOs should deploy autonomous controls within clearly defined policies, thresholds, and escalation paths so every AI-driven action is traceable and auditable. Strong data discovery and classification are foundational under the DPDP Act. Without knowing what data exists and who can access it, compliance breaks down. Consolidated visibility across endpoint, cloud, identity, and network layers ensures faster response and cleaner regulatory reporting.

The organisations that modernise early won't just meet compliance requirements, they'll build long-term resilience, stronger cyber hygiene, and trust in an increasingly AI-driven digital economy.

CISO Forum: Looking ahead to 2026, what will distinguish truly cyber-resilient organisations in India, and how will AI reshape the CISO's role over the next two years?
DIWAKAR DAYAL: By 2026, cyber-resilient organisations will operate at machine speed with human accountability. Success will be measured not by alert volumes, but by how quickly threats are detected, validated, and contained. AI will execute defence actions autonomously, while humans retain oversight, policy control, and judgment.

SOCs will shift from reactive, log-based models to continuous telemetry and AI-driven decision engines that stop attacks as they unfold. Identity and SaaS sprawl will define the primary attack surface, with CISOs increasingly judged on how well they secure access and privilege across human and non-human identities.

Culture will matter as much as technology. Security embedded into everyday workflows will outperform policy-heavy approaches. Resilience will also extend beyond the enterprise, with intelligence sharing through CERT-In and ISACs becoming essential. The CISO role will evolve from tool management to resilience architecture, governance, and business alignment.

By 2026, cyber resilience in India will be about responding faster than attackers can adapt, with AI doing the heavy lifting and humans taking accountability. ■

AI-powered cyberattacks are about to get much worse—and most companies aren't ready

The World Economic Forum's latest cybersecurity report reveals an alarming gap between emerging threats and organizational preparedness

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

THE DIGITAL security landscape is experiencing a seismic shift, according to the World Economic Forum's Global Cybersecurity Outlook 2026. While artificial intelligence promises to revolutionize cyber defense, it's simultaneously supercharging attacks at an unprecedented pace—and the data suggests we're woefully unprepared.

The AI arms race intensifies

An overwhelming 94% of security professionals cite AI as the top cybersecurity driver in 2026, with 87% calling AI vulnerabilities the fastest-growing risk. The same technology empowers attackers at machine speed. Encouragingly, AI security assessments rose from 37% to 64% year-over-year, yet one-third of organizations still lack any validation process, leaving critical defense gaps.

Geopolitics reshaping cyber strategy

Geopolitical volatility is now cybersecurity's new normal. The report shows 91% of large organizations have changed strategies due to tensions, as nation-state attacks on critical infrastructure are documented realities. Confidence in national preparedness varies widely, with high trust in MENA and low in Latin America and the Caribbean. Alarmingly, low confidence has risen to 31%, up from 26% last year.

Fraud hits home

Cyber-enabled fraud has become personal. An astonishing 73% of survey respondents report that they or someone in their network fell victim to cyber fraud in 2025. This shift is reflected in executive priorities—CEOs now rank cyber-enabled fraud as their top concern, displacing ransomware. At the same time, CISOs remain focused on operational threats like ransomware and supply chain vulnerabilities.

The cyber inequality crisis

Perhaps most troubling is the widening gap between cybersecurity haves and have-nots. Skills shortages persist, with 85% of insufficiently resilient organizations lacking critical personnel, versus 22% of highly resilient firms. Small organizations face double the risk, while public sector and NGOs lag private enterprises, with 23% and 37% reporting inadequate resilience.

Supply chain vulnerabilities multiply

Supply chain security has emerged as the Achilles' heel of modern business. Among large companies, 65% identify third-party vulnerabilities as their greatest challenge—up from 54% the previous year. The interconnected nature of digital ecosystems means a breach in one supplier can cascade throughout entire industries, as demonstrated by attacks affecting European airports and major manufacturers.

"The technology enabling sophisticated defenses is equally empowering attackers to launch more convincing phishing campaigns, deploy advanced malware, and execute attacks at machine speed."

The path forward

The report emphasizes cybersecurity resilience depends on choices made today. Success requires investing in skills, proactive AI governance, ecosystem-wide collaboration, and treating resilience as a strategic business imperative, not just a technical function. As 2026 unfolds, thriving organizations will recognize cybersecurity as a shared responsibility underpinning trust, innovation, and global economic stability. ■

Where art meets security: Inside Rajeev Verma's leadership playbook

Rajeev Verma champions human-centric security, blending creativity, discipline, and culture to build resilient enterprises

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

RAJEEV VERMA doesn't fit the conventional image of a cybersecurity chief. The Global CISO and Vice President at SRF, one of India's largest diversified industrial groups, brings an uncommon blend of creativity and rigor to a role defined by pressure and precision. A photographer, poet, and aspiring talk therapist, Verma believes the most resilient security programs are built not just on controls and frameworks, but on empathy, listening, and culture.

That human lens was forged early in his career, when he led a complex offshore banking project virtually on his own—an experience that sharpened his leadership, decisiveness, and resilience under pressure. Today, as cyber threats grow more sophisticated and AI reshapes the risk landscape, Verma is focused on shifting the cultural DNA of manufacturing organizations to make security a shared responsibility. In this conversation with CISO Forum, he reflects on leadership, setbacks, and what it takes to build trust at scale.

CISO Forum: What has been the most defining moment of your career so far, and why?
RAJEEV VERMA: My most defining professional moment came early in my career when I led an offshore project for a bank while working with a consulting firm. Despite operating in a low-cost environment with very high expectations, I effectively functioned as a one-person team, managing delivery, stakeholders, and execution end to end. This experience fundamentally reshaped me—it sharpened my leadership, decision-making, communication, and resilience. It forced me to evolve quickly and reposition myself in the market with renewed confidence and capability.

CISO Forum: If you could revisit one decision in your life and change it, what would it be, and what impact do you think it would have had?
RAJEEV VERMA: Honestly, there is no decision in my life that I would want to change. I am doing the work I aspired to do, and I am part of an organization I truly value. If there is one thing I continue to work toward improving, it is the broader cultural acceptance of information security as a shared responsibility—especially within manufacturing organizations. Changing mindsets takes time, and this remains an ongoing mission rather than regret.

CISO Forum: Who has been the most influential figure in your life, and what key lessons did you learn from them?
RAJEEV VERMA: My chemistry teacher has been one of the most influential figures in my life. Beyond academics, he taught lessons that shaped my thinking and values. He emphasized doing what you love rather than what circumstances push you into, encouraged asking questions instead of blindly accepting norms, and taught me to remain content without becoming complacent. These lessons have guided both my professional and personal journey.

CISO Forum: Which personal habit or mindset has contributed most significantly to your success in the tech world?

I Believe

The second one is listening....

"When we rise towards the top, we hear less of what we hear at the bottom." That is natural, but not professional. I think listening to moderate sounds made by your team member makes you a strong leader and keeps you close to your team.

There is a line in Hindi...

गुमान में इंसान को इंसान
नहीं दिखता।
जैसे छत पे चढ़ जाओ तो खुद
का मकान नहीं दिखता॥

"No battle has ever been won with exhausted people."

RAJEEV VERMA: If I had to choose one habit, it would be punctuality—not just in time, but in thought, action, and communication. Being timely builds credibility and trust. Closely linked to this is patience, which I continue to practice consciously. Together, these traits have helped me navigate complex environments and relationships in the tech world.

CISO Forum: How do you typically handle moments of failure or self-doubt, and what strategies have

you found most effective for bouncing back?

RAJEEV VERMA: I resonate deeply with a quote by Mr. Ratan Tata: 'There is nothing like a right decision. I make a decision and make it right.' I don't view setbacks as failures, but as small glitches—minor deviations from expected outcomes. As a leader, self-doubt has little room, but as a professional, I do experience it when valid ideas fail to gain acceptance due to business priorities. In such moments, candid discussions with leadership help realign perspectives and restore confidence.

CISO Forum: If you could only impart one lesson to the next generation of tech leaders, what would it be, and why?

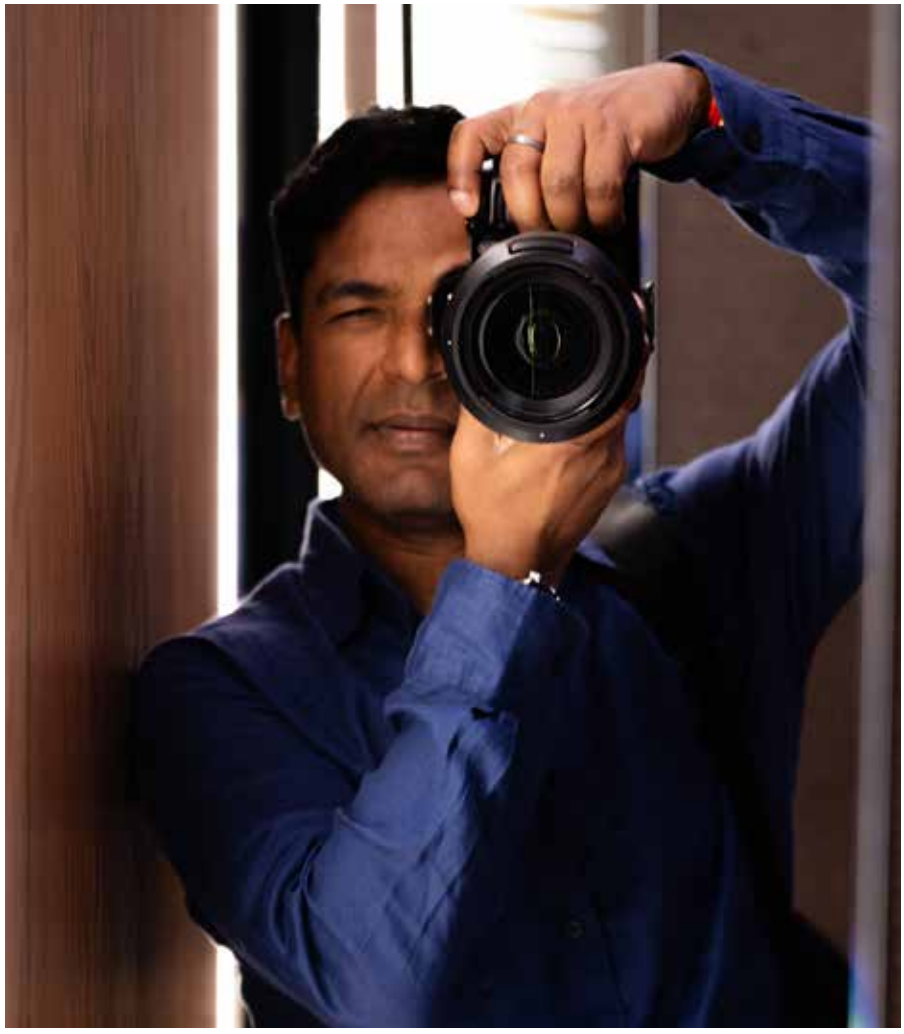
RAJEEV VERMA: Do not overstress. Enjoy life, work hard, and celebrate harder. No battle has ever been won with exhausted people. Organizations need healthy, happy humans—not burnt-out individuals. Be kind, be respectful, and protect your well-being while striving for excellence.

CISO Forum: How do you measure personal growth and success, both in your career and in your personal life?

RAJEEV VERMA: Success for me is not defined by promotions alone. Professionally, it is about enjoying what I do, feeling supported by leadership, and being trusted with responsibility. Personally, success is going home with a smile—being fully present with my family. Equally important is carving out time for myself amid personal and professional responsibilities.

CISO Forum: When faced with particularly challenging weeks, how do you unplug and recharge?

RAJEEV VERMA: I recharge through photography, poetry writing, and travel. Any one of these brings me peace and clarity. I genuinely love my work; it is rarely the work that exhausts me, but sometimes the dynamics around it. These creative outlets help me reset and return stronger.



"Punctuality—of thought, action, and communication—builds credibility and trust."

CISO Forum: If you weren't in the tech industry, what other career path would you have pursued, and what draws you to that field?

RAJEEV VERMA: If I were not in the tech industry, I would likely have pursued a career as a talk therapist or a photographer. Both allow deep human connection and expression, and I have already conducted a few sessions informally—something I find deeply fulfilling.

CISO Forum: As the CISO role continues to evolve, which emerging skills or competencies will become indispensable for cybersecurity leaders in 2025?

RAJEEV VERMA: By 2026, CISOs must be able to translate cyber risk into clear business language for leadership. Strong understanding of regulations, data privacy, and compliance will be non-negotiable. Expertise in cloud, AI, and emerging technology security will be critical, along with the ability to lead incident response, resilience planning, and high- performing security teams. ■

When the system fails, leadership is the control

RECENTLY, AT a CISO Forum conference, I spent time with several CISOs, and a clear pattern emerged. The vocabulary has changed. The ambition to "prevent every breach" has quietly given way to a more honest objective: stay standing when one happens.

Across organizations such as Reliance Industries, SRF, Hindustan Zinc, Godrej & Boyce Manufacturing Company, and PI Industries, the shift is clear. Cybersecurity has moved from the server room to the boardroom. It is no longer judged by how many alerts were closed. It is judged by how well the enterprise absorbs shock.

Three realities define this moment.

First, prevention is limited. Attackers move at machine speed. Platforms scale faster than governance models. The question is not whether systems will be tested. It is whether leaders have rehearsed their response. Clarity of command, decision rights, and communication discipline matter more in the first six hours than technical brilliance alone.

Second, boards want numbers, not noise. A "critical vulnerability" means little in isolation. A probable financial exposure commands attention. CISOs who quantify impact influence investment decisions. Those who cannot remain operational advisers rather than strategic voices.

Third, complexity has outpaced human capacity. Cloud platforms, APIs, AI workloads, and regulatory pressure have stretched security teams thin. Talent scarcity is structural. Automation is necessary. But automation without guardrails introduces new risk. Governance must sit above speed.

The throughline is simple. Cyber resilience is not a product strategy. It is a leadership discipline.

When systems fail, stakeholders look for control. They look for accountability. They look for calm authority. Tools assist. Architecture supports. Automation accelerates. But trust is built by leadership.

In 2026, cyber readiness is no longer about defending the perimeter. It is about proving that when disruption arrives, the enterprise will not fracture. That standard is set at the top. ■

"Cybersecurity in 2026 is no longer about tools or perimeter defense. It is about leadership maturity."

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

CISOFORUM

Security For Growth And Governance

Where CISOs Connect, Innovation Ignites

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

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

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

Expand your network with the brightest minds in cybersecurity.

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

Follow us on @CISO Forum

Scan the QR code to follow

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

Microsoft

PRESENTS

CISO FORUM

India's Leading Cybersecurity Summit

CO-PRESENTED BY

Google Cloud | Deloitte.

CISO Agenda 2026

Quantify Risk, Build Resilience, Enable Growth

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

Thank You

PRESENTING PARTNER

Microsoft

CO-PRESENTING PARTNER

Google Cloud | Deloitte.

GOLD PARTNERS

splunk> a CISCO company

Recorded Future®

SILVER PARTNERS

digital.ai™ proofpoint. Invecto

DELEGATE KIT PARTNER

63 SATS Cybertech

ASSOCIATE PARTNER

Cisco Partner Security

ST FOX

EXHIBIT & LANYARD PARTNER

ARMIS®

EXHIBIT PARTNERS

Barracuda Your business, secured.

Cotelligent A TechDemocracy Company

CyberAssure

Security Scorecard

SECHARD

https://events.cisoforum.in/