

CIO & LEADER

TRACK TECHNOLOGY • BUILD BUSINESS • SHAPE SELF

A 99 GROUP PUBLICATION
cioandleader.com  cioandleader  cioandleader/

Is AI Going to Catapult the CIO Into the Boardroom?

As AI rewrites the rules of business, the CIO is stepping up as the visionary architect shaping the enterprise of tomorrow. PG 18



Vijay Sethi
MentorKart

Dr. Tapan Sahoo
Maruti Suzuki India

Vamsi Krishna Ithamraju
Axis Mutual Fund

Amit Pradhan
Dixon Technologies

Sharat Sinha
Airtel Business



CIO&LEADER studiotalks

CIO&LEADER STUDIOTALKS— WHERE TECHNOLOGY MEETS THE SPOTLIGHT!

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

WHY JOIN STUDIOTALKS?

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

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

Be featured among India’s top technology leaders.

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

SECURE YOUR SPOT NOW!

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

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

Follow us: @CIOandLeader



Time to bring the CIO into the boardroom!

C CIOs **HAVE** long aspired to be seen as more than just operational leaders within their organizations. In the early 2000s and 2010s, there was considerable discussion about why CIOs were not being considered for boardroom roles or broader business leadership positions.

While the CIO role evolved significantly during the 2000s and 2010s, it remained largely disconnected from revenue generation, customer experience, and brand strategy. At the time, CIOs were rarely included in board-level succession planning. The role was still predominantly seen as one focused on maintaining servers, datacenters, internal networks, and desktops.

So, when I proposed this month's cover story on AI catalyzing the CIO's path to a board seat during our editorial meeting, it triggered an intense debate among our editors: was this a timely topic, or were we simply revisiting an old conversation?

But the landscape has shifted dramatically in recent years. From customer experience to business model innovation, nearly every aspect of enterprise value creation is now tech-enabled. With AI at the centre of this shift, CIOs have become central to how organizations streamline operations, generate new revenue streams, and elevate customer experience. They are no longer just responsible for technology—they now drive change, innovation, and help organizations remain resilient and competitive.

As nearly every organization looks to build a comprehensive AI strategy, boards are increasingly turning to CIOs for guidance. AI is not plug-and-play. Its promise is closely tied to data quality, ethical governance, infrastructure readiness, and risk management. CIOs, who sit at the confluence of data, security, and strategy, are not just relevant—they are the architects of tech-driven transformation.

While not every CIO may actively seek a board seat, the moment calls for their presence. AI has changed the rules, and it may well be the opening that finally brings CIOs into the boardroom. ■



“While not every CIO may actively seek a board seat, the moment calls for their presence. AI has changed the rules, and it may well be the opening that finally brings CIOs into the boardroom..”

Jatinder Singh
Executive Editor
jatinder.singh@9dot9.in



COVER STORY

18-23

Is AI Going to Catapult the: CIO Into the Boardroom?

As AI rewrites the rules of business, the CIO is stepping up as the visionary architect shaping the enterprise of tomorrow.



Cover Design by:
Shokeen Saifi



Please Recycle This Magazine And
Remove Inserts Before Recycling

COPYRIGHT, Copyright All rights reserved: Reproduction in whole or in part without written permission from 9.9 Group Pvt Ltd (formerly known as 9.9 Group Pvt Ltd (formerly known as Nine Dot Nine Mediaworx Pvt Ltd). Published at 121, Patparganj, Mayur Vihar Phase-1, Near Mandir Masjid, Delhi-110091 and printed at G. H. Prints Private Limited, A-256 Okhla Industrial Area, Phase-I, New Delhi - 110020.



NEWS & VIEWS

06

80% of GenAI apps will use existing data: Gartner



AI: FROM PILOT TO PRODUCTION

11-14

AI success is 30% tech, 70% change management...

DR. TAPAN SAHOO



15-17

AI will automate or assist 80% of enterprise functions...

AMIT PRADHAN



INSIGHT

24-25

Unlocking Business Value through Intelligent Multi-Cloud Management



28-29

How to Bulletproof Your WordPress Site



30-32

The Looming Quantum Threat: Why We Must Act Now to Secure Cryptography



TECH TALK

35-36

The real CX begins before the first contact

SANJAY GUPTA



37-40

AI Arms Race: How India's Tech Hubs Became Cybersecurity...

VISHAL SALVI

CIO&LEADER

www.cioandleader.com

MANAGEMENT

Managing Director: **Dr Pramath Raj Sinha**
Printer & Publisher / CEO & Editorial Director (B2B Tech):
Vikas Gupta
COO & Associate Publisher (B2B Tech):
Sachin Nandkishor Mhashilkar (+91 99203 48755)

EDITORIAL

Group Editor - 9.9 Group: **R Giridhar**
Executive Editor - B2B Tech: **Jatinder Singh**
Correspondent - B2B Tech: **Jagrati Rakheja**
Principal Correspondent: **Musharrat Shahin**

DESIGN

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

SALES & MARKETING

Director - B2B Tech:
Vandana Chauhan (+91 99589 84581)
National Sales Head - B2B Tech:
Hafeez Shaikh (+91 98331 03611)
Head - Brand & Strategy:
Rajiv Pathak (+91 8010757100)

COMMUNITY ENGAGEMENT & DEVELOPMENT

Head - Community Relations: **Dipanjn Mitra**
Head - Databases: **Neelam Adhangale**
Community Manager: **Vaishali Banerjee**
Community Manager: **Snehal Thosar**
Community Manager: **Reetu Pande**
Community Manager: **Nitika Karyet**
Assistant Manager Community Development:
Shabana Shariff

OPERATIONS

General Manager - Events & Conferences:
Himanshu Kumar
Senior Manager - Digital Operations:
Jagdish Bhainsora
Assistant Manager - Events & Conferences:
Sampath Kumar
Video Editor: **Sunil Kumar**

PRODUCTION & LOGISTICS

Senior Manager - Operations: **Mahendra Kumar Singh**

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 Tara Art Printers Pvt Ltd., A-46-47,
Sector-5, NOIDA (U.P.) 201301.

Editor: **Vikas Gupta**



CIOmovements



Vijay Kannan has joined Danone as Vice President – Digital Operations, leveraging two decades of global IT and transformation experience to strengthen the company's digital operations.



Vikas Srivastava has been appointed Interim CTO at Mahindra Holidays & Resorts, bringing 20+ years of experience in enterprise architecture and digital leadership.



Prem Kiran Udayavarma takes over as CIO at Aditya Birla Renewables, leading IT strategy and digital innovation with expertise in cloud, IoT, and SAP transformatio



Burgess Cooper joins Adani Enterprises as CEO – OT Cybersecurity, bringing deep cybersecurity leadership experience from EY, Vodafone, and HSBC.



Rakesh Dhanda has been named Chief Digital Officer at Adani Infra, with 20+ years of experience in large-scale transformation, analytics, and digital twin systems.



Rupesh Vaish has been promoted to Deputy GM – IT at Dwarikesh Sugar, bringing nearly 30 years of in-house IT experience and award-winning leadership.



Anvize Rodrigues has been appointed CIO & SVP at Tata Tele Business Services (TTBS), bringing 25+ years in enterprise IT, analytics, and digital leadership.



Nikesh Tripathi has been promoted to Vice President – Digital Tech at Axis Mutual Fund, where he will lead digital innovation and platform modernization.



Ajay Malgaonkar joins Agivant Technologies as Chief Digital Delivery Officer, bringing 28+ years of global leadership in AI-driven transformation.



Surajit Deb has been appointed CTO – Group Subsidiaries & Private Bank at Kotak Mahindra Bank, with prior leadership roles at HDFC Securities and IBM.



Balaji Alapilla Sampath joins Gorilla Tech as Project Director, leveraging two decades of experience in transformation and program management.



Senthil Kumar Raman has taken over as CIO at Onward Technologies, with 20+ years of experience in IT strategy, analytics, and engineering transformation.



Subram Natarajan has been appointed CTO & Innovation Officer at L&T-Cloudfiniti, following leadership roles at Google and IBM.



Manjunath Kashi has been promoted to EVP & Head – IT Infrastructure at Axis Bank, bringing two decades of infrastructure leadership in BFSI and tech.



Mohan Shah joins ClaimPro Assist as Chief Technology Officer, with 30 years of experience in IT leadership across logistics and infrastructure.



Anjani Kumar has joined Ather Energy as CDIO, bringing digital leadership experience from TATA AIG, Nissan, and Strides Pharma.



Shweta Singh has been appointed SVP & Head – AI & Analytics at Bharti AXA, with 20 years in analytics, customer intelligence, and digital strategy.



Rishav Raj joins Kotak811 as Vice President, driving digital banking and core banking transformation with prior roles at Tata Capital and ICICI Bank.



Dr. Kaushik Majumder joins LyondellBasell as Director – Infrastructure Services, with global IT experience from BASF, Linde, and hubergroup.

80% of GenAI apps will use existing data: Gartner

Gartner forecasts that 80% of GenAI business applications will be built on existing data platforms by 2028, making RAG a critical enabler of faster, safer AI deployment.

By **Musharrat Shahin** | musharrat.shahin@9dot9.in

IN A world racing to embrace Generative AI (GenAI), the question is no longer if businesses will adopt it, but how fast and how wisely. At the Gartner Data & Analytics Summit in Mumbai, the conversation has shifted from hype to how-to. Gartner predicts that by 2028, 80% of GenAI business applications will be developed on existing data management platforms—cutting development time and complexity by half.

This trend signals a pivotal shift: leveraging in-house data systems as a launchpad for GenAI innovation, while reducing the cost and confusion of integrating fragmented tools and frameworks.

Why RAG matters now

A key theme at the summit was the growing adoption of Retrieval-Augmented Generation

(RAG)—a technique that combines large language models (LLMs) with real-time access to business-specific data. According to Prasad Pore, Senior Director Analyst at Gartner, RAG offers “implementation flexibility, enhanced explainability, and composability” for GenAI applications.

Since most LLMs are trained on public data, they often fall short when addressing organization-specific challenges. RAG bridges this gap by feeding LLMs with internal structured and unstructured data, using tools like vector search, metadata tagging, and chunking to boost accuracy and trust.

Recommendations for enterprises

To fully leverage GenAI, Gartner advises organizations to:

- Transform existing data platforms into RAG-ready systems that serve as real-time knowledge sources.
- Adopt RAG technologies such as vector search and graph databases to ensure scalability and resilience.
- Leverage both technical and operational metadata strategically to mitigate privacy risks and misuse.

As India's GenAI ecosystem gains momentum—with major players like Infosys and TCS integrating GenAI into core services—RAG is fast emerging as a foundational capability, not just an optional enhancement. ■



Infosys launches 200+ enterprise AI agents to streamline operations

Infosys aims to run processes smarter, faster, and with less human intervention.

By **Musharrat Shahin** | musharrat.shahin@9dot9.in

INFOSYS HAS launched over 200 enterprise AI agents, developed through its Infosys Topaz AI platform in collaboration with Google Cloud's Vertex AI. These agents are built to manage complex workflows, automate decision-making, and scale operations across industries.

AI agents built for business impact

Targeting key sectors—healthcare, finance, retail, telecom, manufacturing, and agriculture—these agents utilize advanced machine learning and cognitive architectures to:

- Extract and analyze data from diverse sources
- Process varied formats through multimodal capabilities
- Operate over encrypted channels to ensure privacy
- Make autonomous decisions for complex, repetitive tasks

The result: increased efficiency, faster decisions, and reduced operational overhead.

Use cases across key domains

Infosys shared real-world examples:

- **Network operations:** An AI monitoring agent

tracks real-time usage and alerts teams before capacity issues escalate, minimizing downtime.

- **Corporate finance:** Agents assist with accounts payable and receivable, optimizing reporting and improving cash flow.
- **Manufacturing:** A forecasting agent uses live data to predict demand for vehicle parts, manage inventory, and place automated orders—streamlining the supply chain.

A collaboration built on shared strengths

Part of the Infosys–Google Cloud partnership, this initiative is housed under their Cloud Center of Excellence. It combines Infosys Topaz capabilities with Google Cloud's agentic AI framework. According to Balakrishna D. R., EVP at Infosys, the goal is to enhance Human +AI collaboration for better performance and precision.

Victor Morales, Vice President at Google Cloud, added that these agents show how decision intelligence and automation can simplify complex enterprise workflows.

What it means for enterprises

Infosys' launch signifies a shift from isolated AI tools to scalable, multi-agent systems operating in real-world business environments. For IT leaders, it marks a new phase of AI maturity—where enterprise agents become core to enhancing accuracy, streamlining operations, and driving efficiency at scale. ■

These agents are built to manage complete workflows, automate decision making and scale operations across industries.

Only 7% of Indian firms are cyber-ready

The ongoing shortage of skilled cybersecurity professionals remains a challenge for 92% of organizations.

By **Musharrat Shahin** | musharrat.shahin@9dot9.in

ACCORDING TO Cisco's 2025 Cybersecurity Readiness Index, only 7% of Indian organizations have reached a 'Mature' level of cybersecurity readiness. While up from last year's 4%, the vast majority remain unprepared to tackle today's complex and fast-evolving cyber threats.

AI raises the stakes in security

The report highlights how AI is reshaping the threat landscape. Nearly 95% of Indian organizations faced AI-related security incidents in the past year. Yet only 66% believe their employees fully understand these threats, and just 63% are confident their teams grasp how attackers use AI—indicating major awareness gaps.

"AI is creating a whole new class of threats, and many organizations are not moving fast enough to address them," said Jeetu Patel, Chief Product Officer at Cisco.

Shadow AI, device risks, and talent gaps add pressure

With growing usage of generative AI—both sanctioned and unsanctioned—many IT teams lack visibility. Around 45% of organizations report being unable to detect shadow AI usage, and 90% cite risks from unmanaged employee devices.

The report also reveals a 92% talent gap in cybersecurity roles, making it harder to stay ahead of threats. Furthermore, 84% say that



having too many disconnected security tools slows down threat response.

The need for strategic investment and unified security

Despite growing threats, only 54% of organizations allocate more than 10% of their IT budget to cybersecurity. Experts stress the need for unified, AI-powered platforms that can automate threat detection, simplify infrastructure, and reduce risk.

"Cybersecurity is not just about tools—it's about strategy, awareness, and resilience," said Samir Kumar Mishra, Director, Security Business, Cisco India & SAARC ■

Indian enterprises embedding AI into core operations: SAP

The findings, based on SAP customer data from March 2024 to March 2025, were unveiled during the SAP NOW AI Tour held recently in Mumbai.

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

INDIAN BUSINESSES are moving decisively beyond pilot AI programs to integrate artificial intelligence across core functions, delivering measurable outcomes, according to new analysis released by SAP India.

The findings, based on SAP customer data from March 2024 to March 2025, were unveiled during the SAP NOW AI Tour held recently in Mumbai. The study highlights key AI use cases gaining traction in India, including AI-generated visual insights, language translation, sales order creation from unstructured data, process optimization, predictive forecasting, and natural language query capabilities.

“In any organisation, mission-critical operations are driven by the deep insights data can provide,” said Manish Prasad, President and Managing Director, SAP Indian Subcontinent. “SAP is enabling enterprises to evolve into intelligent, optimized businesses by embedding AI agents into their operational backbone.”

SAP, which has had a strong presence in India since 1996, partners with leading enterprises such as Mahindra & Mahindra, Asian Paints, Infosys, and Wipro, as well as fast-growing firms like Vahdam Teas and Wakefit. Its R&D arm, SAP Labs India, is the second-largest outside Germany and contributes significantly to



SAP’s AI-led transformation equips Indian companies to “shift from hindsight to foresight,” enabling sustainable growth, smarter decision-making, and proactive customer engagement- Prasad

SAP’s global goal of embedding 400 AI use cases across its business applications.

Prasad noted that SAP’s AI-led transformation equips Indian companies to “shift from hindsight to foresight,” enabling sustainable growth, smarter decision-making, and proactive customer engagement. ■

AMD launches EPYC 4005 Series CPUs



The series offers affordable, high-performance solutions for small businesses and hosted service providers.

By **Musharrat Shahin** | musharrat.shahin@9dot9.in

A **AMD HAS** launched its EPYC 4005 Series processors, designed to provide enterprise-grade performance in a cost-effective and easy-to-deploy platform. Aimed at small and medium businesses as well as hosted IT service providers, these chips offer powerful computing without the high cost or complexity of traditional enterprise solutions.

The new processors use AMD's proven AM5 socket and are compatible with multiple form factors—servers, blades, and tower systems. AMD claims its 16-core EPYC 4565P outperforms Intel's 6th-gen Xeon 6300P by up to 1.83x, according to Phoronix benchmark tests.

Tailored for virtualized environments, enter-

prise apps, and 24/7 cloud workloads, the EPYC 4005 series aims to balance efficiency, scalability, and reliability.

Partner support and global adoption

The series has received backing from leading system builders such as Lenovo, Supermicro, OVHcloud, Vultr, and Gigabyte.

Lenovo's Senthil Reddy stated that the new processors enable small businesses to "prepare for the AI era."

The AMD EPYC 4005 Series positions itself as a workload-optimized, affordable choice for enterprises seeking powerful yet flexible computing infrastructure. ■

AI: From Pilot to Production

AI success is 30% tech, 70% change management and alignment

By **Jatinder Singh & Sachin Mhashilkar** | jatinder.singh@9dot9.in

Dr. Tapan Sahoo, Head of Digital Enterprise, Information & Cyber Security, on scaling innovation, translating AI pilots into impact, securing connected vehicles, and empowering the future.



A **AS INDIA'S** largest carmaker, Maruti Suzuki has long been synonymous with accessible mobility and engineering excellence. But in today's hyperconnected, software-defined era, the company is aggressively reinventing itself—not just as an automaker, but as a leader in mobility and technology innovation. At the heart of this transformation lies a bold digital enterprise vision powered by AI, open innovation, and customer-centric design.

In an exclusive interaction with Jatinder Singh, Executive Editor at CIO&Leader, and Sachin Mhashilkar, COO and Associate Publisher – B2B Tech at 9.9 Group, Dr. Tapan Sahoo, Executive Officer – Digital Enterprise at Maruti Suzuki, discusses how the New Delhi headquartered company is reimagining business and customer experiences through deep tech and ecosystem collaboration.

AI: From Pilot to Production

With over three decades of experience spanning vehicle engineering, product development, and program management, Dr. Sahoo now leads the automaker's Digital Enterprise Vertical—anchored in AI/ML, AR/VR, Industry X.0, and open Innovation Programs under the umbrella of Maruti Suzuki Innovation such as Nurture, Incubation, Accelerator and Mobility Challenge. In this wide-ranging conversation, he shares insights on building innovation at scale, navigating AI's pilot-to-production challenges, preparing for agentic AI, strengthening cybersecurity in connected vehicles, and what it takes for CIOs in traditional industries to lead with impact.

Excerpts from the interview:

CIO&Leader: Maruti Suzuki Innovation has emerged as a flagship initiative in your open innovation journey. What inspired its creation, and how is it enabling Maruti Suzuki to tap into external ecosystems and drive scalable digital transformation?

DR. TAPAN SAHOO: The Maruti Suzuki Innovation was conceptualized with a clear vision to create a structured and sustainable approach to open innovation within Maruti Suzuki. We wanted to create a space—not just physical but also intellectual—where innovation could thrive through collaboration with startups, academia, and industry partners.

The primary goal was to tap into external innovation and integrate it with our internal capabilities to solve real business challenges. To achieve this, we launched several strategic initiatives under the Maruti Suzuki Innovation umbrella. These include the Nurture Program, which is our gateway to engaging with very early stage startups & incubation program for early stage startups, our

We've screened nearly 5,000+ startups, with 165+ actively engaged. Over 45+ pilots are underway, and more than 25+ have become full-fledged tech partners.

own accelerator program and Maruti Suzuki Mobility Challenge.

We have also formed deep partnerships with leading academic institutions such as IIM Bangalore and IIM Calcutta, and with ecosystem enablers like T-Hub and NASSCOM. Our model is systematic: we invite startups working on advanced technologies like AI, ML, IoT, EV charging, drones, and micromobility to apply. After a rigorous evaluation process, short-listed startups are onboarded for paid pilot projects. If the PoCs prove successful in business terms, we graduate these startups into long-term partnerships.

To date, we have screened close to 5,000+ startups, and 165+ are actively engaged with us. We have over 45+ pilots currently in progress and have converted more than 25+ of these into full-fledged technology partners. This program has helped Maruti Suzuki stay agile, future-ready, and continuously aligned with emerging customer expectations.

CIO&Leader: That's impressive. AI clearly plays a key role here—can you share some examples of AI projects that have successfully moved from pilot to production?

DR. TAPAN SAHOO: Indeed, AI is one of the most transformative technologies we are leveraging across various functions. One notable use case is how we are improving the post-sale customer experi-

ence. Traditionally, every car comes with an owner's manual, but we observed that very few customers actually read them unless there's a problem. In real situations—say a warning light appears on the dashboard—customers often panic and don't know what steps to take.

To address this, we deployed an AI-based visual recognition feature through the Maruti Suzuki mobile app. It allows users to simply take a picture of the issue, such as a dashboard symbol. The AI model instantly identifies the symbol, explains the issue in layman's terms, and guides the user on the next steps. It even gives the option to directly contact customer care or schedule a service if needed.

This solution replaces the static owner's manual with a dynamic, intuitive, and accessible AI assistant. It reflects how we're blending AI into the real customer journey—making it more proactive, responsive, and engaging. And this is not an isolated initiative—we are scaling similar solutions across quality control, preventive maintenance, and supply chain functions as well.

CIO&Leader: Studies show that 75% of AI projects remain stuck in pilot mode. Why does this happen, and what can CIOs do to move them into full-scale deployment?

DR. TAPAN SAHOO: That's a very relevant observation. Many AI initiatives falter in the transition from proof of concept to enterprise-wide deployment. One primary reason is the lack of readiness when it comes to data. AI models require clean, contextual, and representative datasets to train effectively. But many organizations still have fragmented or siloed data architectures, making it difficult to extract consistent value.

Secondly, there's often a mismatch between the AI solution and a well-articulated business prob-



AI models need clean, contextual, representative data—but many organizations still operate with fragmented, siloed architectures, limiting consistent value.

lem. If there's no clear value proposition—whether it's cost saving, efficiency improvement, or revenue generation—then the initiative won't find traction beyond the pilot phase. CIOs need to co-create use cases with business stakeholders, ensuring alignment with organizational priorities.

Also, AI models need to be explainable, transparent, and free from systemic biases. The presence of risks, hallucinations in generative models, incorrect outputs due to flawed data, must be managed through robust governance frameworks. Selecting the right language models (SLMs or LLMs), investing in continuous learning, and setting KPIs tied to business impact will help bridge the gap between experimentation and scale.

In my experience, successful AI implementation is 30% about technology and 70% about change

management and stakeholder alignment.

CIO&Leader: With growing digitization and connected vehicles, cybersecurity is a critical concern. What steps has Maruti Suzuki taken to mitigate cyber risks?

DR. TAPAN SAHOO: Absolutely, cybersecurity is foundational in today's connected automotive ecosystem. With vehicles increasingly becoming software-defined, the attack surface has expanded significantly—from IT and OT infrastructure to in-vehicle networks and customer-facing digital touchpoints.

Our cybersecurity strategy rests on several pillars. The first is internal awareness—ensuring all employees, from factory workers to senior leaders, understand the importance of cybersecurity hygiene. Regular training, phish-

ing simulations, and workshops are part of this effort.

The second pillar is system-level security—ensuring that our applications are secure by design. We follow secure coding practices, conduct regular vulnerability assessments, and maintain strict version control across all deployed software.

Third, we have robust monitoring through our Security Operations Center (SOC), which allows us to detect, analyze, and respond to threats in real-time. We also conduct red teaming exercises to simulate attacks and test our preparedness.

Fourth, we stay aligned with national advisories from CERT-In and NCIIPC. These guidelines help us benchmark our posture against evolving threats.

Cybersecurity, however, is an ongoing journey—it requires constant vigilance and smart investment. We must strike a balance between security robustness and cost efficiency. While no system can be 100% secure, the aim is to minimize risk exposure and recover quickly in the event of a breach.

CIO&Leader: A futuristic question—agentic AI and autonomous agents are becoming mainstream. Are Indian enterprises ready for this shift?

DR. TAPAN SAHOO: Agentic AI is definitely on the horizon, and it promises to redefine work processes by introducing autonomous decision-making capabilities. However, its adoption in India—or anywhere—depends largely on organizational maturity.

Enterprises that have standardized processes and clearly defined workflows are in a better position to benefit from agentic AI. These agents require structured inputs and outcomes. If the enterprise landscape is chaotic or process-



Enterprises that have standardized processes and clearly defined workflows are in a better position to benefit from agentic AI.

heavy with human dependencies, AI agents will struggle to deliver value.

I often reference the Harvard framework for AI adoption: AI as a tool, as a companion, as a manager, and as a potential replacement. Indian enterprises need to map their use cases across these levels. For instance, AI as a tool is already in use—data analytics, chatbots, diagnostics. AI as a companion might assist humans in complex decision-making. AI as a manager—where agents autonomously handle workflows—is the next leap but requires high trust, regulatory clarity, and process discipline.

So yes, agentic AI is coming. But the focus should be on identifying the right domains within the enterprise where autonomy adds value without introducing unacceptable risks.

CIO&Leader: From being India's dream car in 1983 to a premium experience today—how is Maruti

Suzuki continuing to innovate on the customer experience front?

DR. TAPAN SAHOO: The evolution of Maruti Suzuki from a value-driven carmaker to a premium experience brand has been deliberate and continuous. Customer experience (CX) is a key differentiator today, and we have made concerted efforts to digitize and elevate it.

Currently, 26 out of our 28 key customer touchpoints are digitally enabled. These include everything from online booking, financing, servicing, insurance, to loyalty programs. The only parts that still require physical interaction are the test drive and vehicle delivery.

The next phase is about orchestrating these digital touchpoints into a seamless and hyper-personalized journey. We are integrating AI, data analytics, and real-time engagement tools to ensure that every customer interaction is relevant, timely, and frictionless.

For example, predictive servic-

ing, AI-based recommendation engines, and dynamic pricing models are being tested and deployed. The idea is to create a 'phygital' ecosystem—where digital and physical touchpoints merge to create a consistent brand experience across the customer lifecycle.

CIO&Leader: You have led multiple transformation journeys. What's your advice to CIOs from traditional industries looking to leapfrog through AI?

DR. TAPAN SAHOO: The CIO role today is mission-critical. Gone are the days when CIOs were confined to infrastructure or back-office automation. In the digital era, they are strategic partners in shaping the organization's future.

My first piece of advice is to build a compelling case for change. Whether it's AI or digital transformation, it must be tied to business outcomes. That sense of urgency needs to permeate across the C-suite and operating layers.

Second, drive transformation as a team sport. The best CIOs are also great collaborators—they listen to business leaders, co-create solutions, and ensure alignment across functions. They balance short-term wins with long-term vision.

Third, resilience and focus are critical. The journey will be fraught with challenges—W constraints, resistance to change, technology failures. But if you keep your eye on the destination, you will find ways to navigate the obstacles.

Lastly, keep learning. The tech landscape is evolving rapidly—AI, quantum computing, cybersecurity, digital twins. CIOs must continuously upgrade their own understanding to lead with confidence.

In summary: instill urgency, build strong collaborations, maintain focus, and keep evolving. That's the formula for transformative success. ■

AI will automate or assist 80% of enterprise functions by 2027

By **Jatinder Singh** | jatinder.singh@9dot9.in

Amit Pradhan,
Vice President – IT
and CIO at Dixon
Technologies on scaling AI from pilot to production, building digital manufacturing capabilities, and preparing Indian enterprises for the future of autonomous operations



ONE OF the biggest challenges enterprises face today is not adopting AI—but scaling it. As companies move from small pilot projects to enterprise-wide AI adoption, they face a host of challenges, including data readiness, system integration, change management, and aligning with business goals. Amit Pradhan, Vice President – IT and Chief Information Officer (CIO) at Dixon Technologies (India) Ltd., has been leading this transformation from the front.

Dixon Technologies is one of India's leading electronics manufacturing services (EMS) companies, partnering with top global and Indian brands across segments such as consumer electronics, home appliances, mobile phones, lighting, and wearables. As a key contributor to the "Make in India" initiative, Dixon is actively building digital capabilities

AI: From Pilot to Production

to scale smart manufacturing and foster innovation.

Amit brings over 20 years of cross-industry experience in electronics, telecom, energy, and consumer durables. At Dixon, he heads the company's IT strategy, digital initiatives, and innovation-led transformation agenda. Prior to joining Dixon, he held senior leadership roles at Mahindra Group, Sterlite Power, Adani Enterprises, and Videocon, where he drove several large-scale technology initiatives. A NEXT100 awardee (2019), Amit combines deep enterprise leadership with entrepreneurial agility.

In this exclusive conversation with Jatinder Singh, Executive Editor, CIO&Leader, and Vikas Gupta, Editorial Director, 9.9 Group, Amit shares how Dixon is scaling AI, strengthening digital manufacturing, and preparing for the future of autonomous enterprise operations.

CIO&Leader: What are some of the unique challenges that companies like yours face in operationalizing AI? And what best practices have emerged from your experience?

AMIT PRADHAN: AI as a concept is not new. What has changed is the maturity of the ecosystem, especially for enterprise-scale deployment. A few years ago, AI was limited to isolated use cases, often inspired by Big Tech, but rarely scalable across traditional industries like manufacturing. The rapid pace of change and frequent model updates made it difficult to stabilize.

Today, the ecosystem is far more mature. At Dixon, we have built and tested nearly 20 AI proof-of-concepts (POCs). Of these, 5–6 are now being scaled across the organization.

Being a manufacturing-intensive company, our AI focus is largely on production, supply chain, qual-

At Dixon, we have developed and tested close to 20 AI proof-of-concepts (POCs). Of these, 5–6 are now being scaled across the organization, including global operations.

ity and testing. Some key examples include:

- **Dixon answer platform:** We are building an internal platform layered over our DMS, CMS, and other systems to create a bot that serves as a central knowledge assistant. Employees no longer need to sift through long documents—they simply ask the bot and receive precise, contextual answers on policies, quality checks, or procedures.
- **Defect detection and prevention:** We use AI models to detect product defects and recommend corrective actions. This enables continuous learning and prevention, improving product quality.
- **Supply chain optimization:** We are using AI-driven video-based training solutions. Traditional classroom sessions or lengthy training videos are often ineffective in such environments. So, we have created short, targeted training clips—like step-by-step guides—that help operators quickly learn how to handle specific tasks or machines. These are focused on ensuring quality and efficiency on the production floor.
- **AI-Powered Video Summarization & Surveillance System:** We are building Automated Video Summarization. Continuous video feeds from hundreds of factory cameras. custom AI models summarize 8 hours of foot-

age into 2–3 minutes. Smart tags (e.g., "idle machine," "worker absence," "manual intervention") auto-generated.

CIO&Leader: How are you approaching data governance to ensure AI implementations are effective and sustainable?

AMIT PRADHAN: AI is only as good as the data that feeds it. That's why data governance is a foundational part of our AI strategy. We have transitioned from Excel-based planning to an integrated IT platform, which ensures master data is accurate and consistently maintained—especially important for our supply chain planning.

We have also implemented a maker-checker model that started manually but has now evolved into an intelligent system. It automatically flags anomalies and discrepancies, allowing us to act before issues escalate.

A key goal has been to establish a single source of truth, which is critical in a complex setup with multiple data streams. This ensures reliability and trust in our AI outputs and supports better decision-making.

CIO&Leader: What are your key priorities for AI and technology in the next couple of years?

AMIT PRADHAN:

- **AI strategy – maker, shaker, and taker:**
 - Maker:** Build custom AI models for our unique business needs.
 - **Shaker:** Leverage and refine existing internal models.
 - **Taker:** Integrate SaaS platforms with pre-built AI capabilities.
- **Edge-to-cloud strategy:**
 - Our fast-paced production lines require minimal latency. We are exploring Edge-to-Cloud architectures that combine local responsiveness with cloud scalability.



At the CIO&Leader Annual Conference, I am especially looking forward to engaging with fellow CIOs, OEM leaders, and ecosystem partners to explore how AI is being practically deployed across industries. Of particular interest is the evolution of India-built AI stacks—how they're being scaled in real-world enterprise environments, especially in manufacturing, supply chain, and field operations.

■ **Transitioning from Industry 4.0 to 5.0:**

- We are deploying technologies like intelligent UIs, advanced automation, camera-based quality checks, and AI-guided workstations.
- A strong focus is on workforce skilling—we use AI-driven video tutorials and short, gamified training clips that are process-specific and sometimes even certified. In industries like ours, where skilled manpower (e.g., SMT operators) is limited, this makes a big difference.
- We've also introduced digital displays at workstations with real-time, interactive instructions—significantly improving both quality and productivity.

CIO&Leader: Is there growing pressure from global brand partners to include AI in your manufacturing lines, or are these initiatives led purely by Dixon?

AMIT PRADHAN: It's a mix of both. On one hand, we are internally driving AI as part of our KPIs—to make manufacturing more efficient, sustainable, and smarter.

On the other hand, global customers are increasingly expecting their partners to be tech-enabled. One of our largest clients recently adopted an AI-powered logistics quality solution we developed and told us, "This is the first time any supplier worldwide has done this." They're now looking to roll it out with other vendors too. That's a big validation of our efforts.

CIO&Leader: From your vantage point, do you think fully autonomous enterprises will be a reality in India within the next two years?

AMIT PRADHAN: I believe we are moving in the right direction. Many Indian enterprises have already set up dedicated AI teams and are integrating AI across departments.

Of course, for some companies, it's still a journey—especially where digital maturity or foundational data infrastructure is lacking. But the momentum is strong. For enterprises that are still building AI foundations—like working on surrounding technologies, developing new skills, and scaling data infrastructure—it's definitely a journey. It will take a bit more time for them to fully adopt and integrate AI. But as I said, AI is a powerful game-changer. In just a couple of years, I believe around 80% of our work will be either AI-assisted or entirely bot-driven.

CIO&Leader: What kind of topics would you personally like to see covered at CIO&Leader's upcoming conference on "AI: From Pilot to Production"?

AMIT PRADHAN: There are three areas I'd like to learn more about, especially given the challenges CIOs are currently facing:

- **Agent-based AI:** There is significant promise here—where AI agents can connect multiple systems, data sources, and actions to replicate decision-making.
- **Responsible AI:** As more models are deployed, trust, bias mitigation, and transparency become critical. We need frameworks to ensure ethical and accountable AI use.
- **India-specific AI innovations:** I would love to see how India-built AI stacks and where they can be practically applied. Understanding local innovation will help contextualize global trends. ■

Is AI Going to Catapult the CIO into the Boardroom?

As AI rewrites the rules of business, the CIO is stepping up as the visionary architect shaping the enterprise of tomorrow.

By **Gagandeep Kaur** | editor@cioandleader.com





Today's CIOs are not only orchestrating enterprise-wide digital transformation but also driving innovation, accelerating time-to-market, anticipating market shifts and customer behavior, optimizing operations through real-time insights, and even spearheading the creation of new revenue streams. The CIO's role is no longer just about supporting the business—it's about shaping its future.

With technology now central to both customer experience and operational agility, CIOs are increasingly stepping into roles that require a combination of deep technology leadership and sharp business acumen. From leading AI adoption and enabling data-driven decision-making to co-owning digital initiatives that directly impact revenues, CIOs are emerging as pivotal architects of enterprise growth.

Many are taking on hybrid roles such as Chief Digital Officers (CDOs) and Chief Product & Technology Officers (CPTOs)—often seen as stepping stones to the CEO's chair. "Now, only 60% of the CIO's responsibilities remain traditional—focused on IT infrastructure and systems management," says Suresh Karnati, Senior Executive Vice President at Bajaj Allianz Life. "The remaining 40% is shifting towards business-focused responsibilities."

Traditionally, CIOs were expected to ensure uptime, manage infrastructure, and reduce operational costs through technology. That is rapidly changing. "Today, their role has expanded to include driving digital transformation, enabling innovation, shaping business strategy, and delivering customer-centric solutions," says Arun Chandrasekaran, Distinguished VP Analyst at Gartner.

How has the CIO role evolved?

Increasingly, there is a growing expectation from senior management that CIOs will play a role in building new revenue streams. They are expected to work closely with the Chief Executive Officer (CEO) and other C-suite executives

on growth strategies and lead enterprise-wide Artificial Intelligence (AI) and data initiatives.

Globally, there are several examples of CIOs who have transitioned from a CIO role to a business role and even CEO. A well-known example is Chris Lofgren, who transitioned from Schneider National's National's CIO to its CEO. There are also a few examples in India. For instance, Vijay Sethi, former CIO of Hero Moto-corp, is now the Chairman and Chief Mentor at MentorKart.

"While CIOs have always tried to generate value for the organization using technology, AI is amplifying these capabilities and bringing them directly into the strategic limelight of the boardroom," says Vijay Sethi, Chairman and Chief Mentor, MentorKart; Advisory Board Member to multiple organizations; and former CIO, Chief Human Resource Officer, and Head of CSR at Hero MotoCorp.

This shift underscores the growing weight of AI in business conversations. It is not just reshaping operational workflows, but also altering the strategic posture of CIOs. With AI moving to the center of boardroom discussions, CIOs are stepping up as key decision-makers.

"AI has shifted the conversation from 'How can IT support the business?' to 'How can AI transform the business?' This fundamental change has made the CIO's role more strategic.

"Though most board members are increasingly aware of AI's disruptive potential and the opportunities it presents, they still look to the CIO to provide strategic guidance on AI—thus bringing CIOs closer to a seat at the board."

—Vijay Sethi
Chairman and
Chief Mentor,
MentorKart



“The CIO role today is mission-critical. Gone are the days when CIOs were confined to infrastructure or back-office automation. In the digital era, they are strategic partners in shaping the organization’s future.”

—Dr. Tapan Sahoo

Head of Digital Enterprise (DE) and Information & Cyber Security, Maruti Suzuki India



“We are increasingly seeing CIOs and CTOs evolve into hybrid roles such as Chief Product and Technology Officer (CPTO) in digital-native firms or take on additional roles like Chief Digital Officer (CDO) and Chief Operating Officer (COO) in sectors like financial services.”

—Vamsi Krishna Ithamraju

Chief Technology Officer, Axis Mutual Fund



Though most board members are increasingly aware of AI's disruptive potential and the opportunities it presents, they still look to the CIO to provide strategic guidance on AI—thus bringing CIOs closer to a seat at the board,” he adds.

Anand Deodhar, Group Chief Information Officer at Force Motors adds that in the automotive industry, for example, CIOs no longer manage internal IT systems; they lead efforts to create connected vehicles, integrate telematics platforms, and develop customer-facing mobile applications. This evolution reflects a broader shift; IT has transitioned from a back-office support function to a critical enabler of business growth, customer engagement, and competitive differentiation.

This expansion of roles enables CIOs to take on additional responsibilities. “The time is right for CIOs to step into a more strategic role, as enterprises increasingly expect to leverage technology to drive business at citizen scale. We are increasingly seeing CIOs and CTOs evolve into hybrid roles such as Chief Product and Technology Officer (CPTO) in digital-native firms or take on additional roles like Chief Digital Officer (CDO) and Chief Operating Officer (COO) in sectors like financial services,” says Vamsi Krishna Ithamraju, Chief Technology Officer at Axis Mutual Fund.

“We have seen CIOs across industries lead initiatives that have transformed operations, launched new digital products, and delivered measurable business growth. The impact is clear,” says Daniel-Zoe Jimenez, Vice President of Digital Innovation, CX & Software, DNB/Start-ups, SMBs, Consumer and Channels Research, IDC Asia/Pacific.

IDC predicts that by 2027, 50% of CIOs will be accountable for embedding sustainability goals into every technology project, measuring outcomes to refine investments and align with environmental objectives.

“CIOs are emerging as key figures in driving enterprise business growth – but not just as enablers, but increasingly as catalysts. Forward-looking CIOs are stepping beyond traditional IT to actively orchestrate value across the organization, effectively partnering with business leaders to drive innovation, new sources of value across the business, as well as achieve the organization's sustainability goals,” says Daniel-Zoe Jimenez of IDC APAC.

This view is echoed by other industry members who emphasize the growing influence of CIOs in shaping strategic direction and unlocking enterprise-wide value. “CIOs and CISOs are now seen as visionary leaders and key architects of business growth, empowered by their ability to integrate technology, data, and strategy across the organization. They have become central to driving business growth, given the rapid pace of digital transformation that has made technology a core enabler of business. CIOs have evolved into critical business leaders who are no longer confined to just operational roles,” says Sharat Sinha, Director and CEO of Airtel Business.

The growing ubiquity of technology across business functions means that CIOs are active-

ly involved in the processes and operations of various departments. This cross-functional engagement broadens their perspective and positions them as strategic leaders beyond the realm of technology. "CIOs are championing transformative projects across various functions, including procurement, supply chain, sales and marketing, HR, manufacturing, and quality management. Initiatives across functions demonstrate the CIO's ability to transcend traditional IT boundaries and deliver measurable financial gains alongside innovation," says Deodhar of Force Motors.

This shift has also elevated CIOs into strategic technology advisors to senior management. "CIOs are also emerging as digital coaches and trusted strategic advisors to senior leadership, significantly expanding both the scope and influence of their roles," says Vamsi.

"While forward-looking enterprises are transforming their business processes, the CIO is emerging as the primary internal influencer and driver. Increasingly, the new-age CIO is not just well aligned with an organization's business strategies and goals; they are actively involved in screening and identifying technologies that can help augment existing revenue streams and create new ones, apart from optimizing costs and improving efficiency and productivity," says Deepak Kumar, the founder analyst and chief research officer at BMNxxt Business and Market Advisory.

What are the factors driving this shift?

Several forces are driving this shift, but the most significant one is the growing strategic role of technology in business. Once limited to supporting back-end operations, technology has now become a critical differentiator, and CIOs are expected to lead that transformation. As digital channels, AI, data analytics, and cloud computing reshape how companies engage with customers and optimize operations, CIOs are moving from the sidelines to the center of strategic decision-making.

"They are leading the adoption of cloud, AI, IoT, and 5G to build smarter, more agile enterprises and unlock new revenue streams. Also, the shift to hybrid work and digital-first customer engagement has increased the demand for seamless, scalable, and secure IT infrastructure," says Sinha of Airtel Business.

5 Key Takeaways

- **CIOs are stepping beyond tech:** No longer limited to managing infrastructure, CIOs are driving digital transformation, innovation, and revenue growth initiatives.
- **Tech is now business-critical:** With AI, data, and digital platforms central to customer experience and value creation, CIOs are influencing core business decisions.
- **CIOs are taking on hybrid roles:** Titles like CPTO, CDO, and even COO reflect how CIOs are blending technology leadership with operational and other core business areas.
- **AI adoption is a game-changer:** CIOs play a crucial role in ensuring the success of AI initiatives and aligning them with business goals, enabling them to grow their profiles.
- **The mindset shift is key:** The future belongs to CIOs who embrace business KPIs, take ownership of non-IT initiatives, and act as catalysts for growth.

The role of new-age technologies is undeniable in the evolving role of CIOs. "This expansion is fuelled by the rise of digital transformation, AI, and data analytics, which position the CIO as a key enabler of transformation. Their ability to align tech initiatives with business goals, enhance customer experience, and drive agility is critical," says Chandrasekaran of Gartner.

In the cloud era, customers expect solutions to be available at all times and seamlessly integrated across all platforms. It has, in effect, become part of the product and service itself.

"Now, only 60% of the CIO's role remains traditional, which is focusing on IT infrastructure and systems management, among others. The remaining 40% is shifting towards business-focused responsibilities."

—**Suresh Karnati**
Senior Executive Vice
President, Bajaj Allianz Life



This has played a role in CIOs becoming business enablers by driving the transformation of new business models.

Additionally, there has been a shift in employee demand, driven partly by the COVID-19 pandemic. A new generation of workers is transforming the way we work, and CIOs must create a digital workplace that not only addresses business requirements but also appeals to employees. The digital transformation of enterprises, coupled with workplace evolution, typically means close collaboration between CIOs and different departments, broadening their perspective.

"This shift is being driven by the rapid pace of technological change and the critical role technology now plays in enterprise success. As a result, CIOs are no longer seen as technology leaders or business enablers but are now contributing significantly to the overall business growth," says Vamsi.

Visionary CIOs are grabbing this opportunity to grow their profile by building new revenue streams or taking ownership of new technology-driven business initiatives. They are leveraging new-age technologies, including AI, cloud, and data, to create new products, reinvent services, and establish digital business models that drive new revenue streams.

"By embedding technology into every aspect of the business value chain, CIO-led projects are redefining what it means to drive growth and create competitive advantages," says Deodhar of Force Motors.

"In the automotive industry, for example, CIOs no longer just manage internal IT systems; they lead efforts to create connected vehicles, integrate telematics platforms, and develop customer-facing mobile applications."

—Anand Deodhar
Group Chief
Information Officer,
Force Motors



Technology is also helping CIOs by providing them with tools to manage their technology infrastructure and teams more effectively, making it easier for them to transition from technology-driven to business-focused roles. "CIOs now have more capacity and tools to contribute to strategic business goals," says Karnati of Bajaj Allianz.

AI: A defining moment for the CIO

As AI becomes a transformative force in enterprise IT, it is reshaping the role of the CIO in profound ways. CEOs are under pressure to ensure that AI investments deliver tangible results, which remains elusive for many organizations. While there is a broad consensus on AI's potential to transform business processes and models, unlocking this requires the expertise of a CIO who can anchor AI initiatives in business goals.

IT leaders are leveraging AI to automate routine tasks—such as infrastructure monitoring, ticket resolution, and incident management—while simultaneously enhancing user experiences through intelligent chatbots and other AI-driven tools. This shift not only optimizes resource utilization but also frees up valuable time for IT leaders and their teams to focus on high-impact initiatives and channeling their efforts into building platforms and services that directly generate new revenue streams. This marks a clear evolution—from IT being viewed as a cost center to becoming a strategic growth enabler.

IDC's 2024 Future Enterprise Resiliency and Spending (FERS) Survey, wave 4, reveals that organizations in the Asia/Pacific region have conducted an average of 24 Gen/AI proofs of concept (POCs) over the past 18 months, with only three reaching production. In this scenario, CIOs play a crucial role in the successful adoption of AI by enterprises, working closely with business leaders to identify opportunities where technology can directly generate revenue.

"CIOs are instrumental in orchestrating this shift and must work with key business stakeholders in setting the enterprise AI agenda, defining KPIs, establishing governance frameworks, building AI Centers of Excellence, and indeed, rethinking talent strategies to drive real impact for the AI-fueled enterprise," says Daniel Zoe-Jimenez of IDC.

Not Without Challenges

While the path for CIOs to evolve into strategic business leaders is becoming more visible, the journey is anything but straightforward—and such transitions are still relatively rare. A senior CIO at a major Indian conglomerate, requesting anonymity, puts it bluntly: “We must ask ourselves, how many CIOs have truly moved beyond their traditional role as technology custodians to take on direct business responsibilities? Too often, CIOs are still seen as service providers or enablers rather than as co-drivers of business strategy.”

One key reason for this is inertia—many CIOs operate within a familiar comfort zone. Moving beyond it requires embracing ambiguity, making bold decisions, and taking ownership of business outcomes—all of which come with risk. The fear of failure, organizational resistance, and a lack of exposure to P&L responsibilities make the transition daunting for many.

Seizing the opportunity to step into broader business roles demands not just technical expertise but a fundamental shift in mindset. As Daniel Zoe-Jimenez of IDC notes, “Many traditional CIOs still focus on maintaining infrastructure and meeting legacy IT KPIs. They’re measuring system uptime when they should be measuring customer lifetime value or revenue per digital transaction. The CIOs who rise to the challenge are those who strategically align AI and emerging technologies with the organization’s top business goals.”

Today’s forward-thinking CIOs are already showing what’s possible. They are:

- Anticipating market trends and shifting customer expectations through predictive analytics
- Driving hyper-personalized customer experiences using AI and data platforms
- Transforming supply chains and operations through automation and real-time decision-making

By aligning technology initiatives with core business strategies, these CIOs are no longer playing a supporting role—they are becoming architects of enterprise value and key contributors to shaping the organization’s future.

In closing

As digital transformation and growing AI adoption reshape business processes and models, they provide an opportunity for CIOs to step

"CIOs have become central to driving business growth given the rapid pace of digital transformation that has made technology a core business enabler. CIOs have evolved into critical business leaders, who are no longer confined to just operational roles."

—**Sharat Sinha**
Director and CEO,
Airtel Business



"The rise of digital transformation, AI, and data analytics has positioned the CIO as a pivotal driver of enterprise change. Their ability to align technology with business strategy, elevate customer experience, and foster organizational agility is now more critical than ever."

—**Arun Chandrasekaran**
Distinguished VP Analyst,
Gartner



into boardrooms as strategic growth leaders.

Enterprises are giving CIOs a bold new mandate: to step beyond traditional boundaries and lead with confidence. In turn, CIOs must rise to the challenge: pushing past their comfort zones, aligning deeply with business strategy, and driving meaningful change. The future will not favor those who simply maintain systems, but those who reimagine them. The next generation of enterprise leaders won’t just enable the business—they will redefine it. ■



Unlocking Business Value through Intelligent Multi-Cloud Management

Enterprises are embracing multi-cloud strategies to enhance resilience, scalability, and operational control.

By **Rahul S Kurkure** | editor@cioandleader.com

IN TODAY'S digital-first era, multi-cloud adoption across SMBs and large enterprises is considered a smart investment strategy. Organizations are increasingly opting for multi-cloud strategies to enhance operational efficiency, ensure resilience and scalability, avoid vendor lock-in, and tailor service offerings. This approach involves leveraging cloud services from two or

more providers, extending the organization's private cloud capabilities, and distributing workloads across diverse cloud platforms. According to Precedence Research, the global multi-cloud management market size is calculated at USD 16.02 billion in 2025 and is forecasted to reach around USD 147.2 billion by 2034, growing at a CAGR of 27.94% from 2025 to 2034.

Strategic approach for multi-cloud success

As organizations are increasingly leveraging services from multiple cloud providers, the complexity of the multi-cloud environment, such as operational and technical challenges, is growing, too, making it rather difficult to manage. This drives the need for a comprehensive multi-cloud management strategy for organizations to achieve success.

Define clear objectives

Before starting a multi-cloud journey, organizations must identify business needs and set clear objectives. Determine which workloads benefit most and define desired outcomes—whether performance, compliance, security, or scalability. These goals guide the process and ensure cloud initiatives align closely with overall business strategy for meaningful results.

Choose the right service provider

Cloud service providers should be evaluated based on their strengths and alignment with organizational needs. Choose providers suited for specific workloads and consider their geographic reach. Review contracts for cost transparency, flexibility, and regulatory compliance. Assess security practices and certifications to ensure data protection. Defining key performance metrics helps select the provider that best supports business goals and operational efficiency.

Establish a strong governance framework

A strong governance framework is key to multi-cloud success, ensuring effective risk management and compliance. Consistent, automated policies and processes guide operations across environments. Clear governance is essential for work-



Rahul S Kurkure
Founder and Director
Cloud.in

load placement, access control, data management, and security protocols. Without it, organizations risk losing control, leading to higher costs and security or compliance issues.

Invest in Cloud Management Platform

Workloads spread across multiple cloud service providers have introduced significant operational and management complexities. Without the right set of tools and a single pane of glass view, organizations will have to face challenges of managing resources across several cloud environments, ensuring security and compliance, and optimizing costs at the same time. By investing in a multi-cloud management platform, organizations can gain an integrated view for monitoring and managing resources across all cloud environments. AI-driven systems and open-source standards for multi-cloud management can support interoperability between different cloud service providers.

Adopt Zero-trust Architecture

Using multiple cloud environments increases security risks by expanding attack surfaces and vectors.

This complexity demands a new approach like Zero Trust Architecture (ZTA), where no user or system is trusted by default. ZTA enforces strict access controls and verification, ensuring consistent security across multi-cloud setups.

Implement monitoring

Organizations adopting multi-cloud strategies must ensure these environments are functionally well and are secure. By leveraging monitoring and analytics tools, organizations can gain insights into the performance, availability, resource use, cost, and condition of the applications and services across all cloud service providers. By doing so, timely detection and resolution of issues are possible, and the multi-cloud environments can be constantly optimized with cost-saving measures and right-sized resources.

Cost Control

It is necessary to strike the right balance between cost and performance with multi-cloud environments. This can be achieved by ensuring cloud resources are rightly sized. Organizations can leverage spot instances for less important tasks as they cost less than on-demand or reserved instances, thereby keeping costs in check while ensuring smooth operations across all cloud environments. Optimization of cloud expenses is possible by leveraging automation in resource administration.

Organizations adopting multi-cloud strategies must ensure these environments are secure and function efficiently. Monitoring and analytics tools provide insights into performance, availability, resource usage, cost, and overall health across all providers. This enables timely issue detection, resolution, and continuous cost optimization. ■

Data in the Age of AI: Why Enterprises Must Rethink Security Now



GenAI, quantum threats, and app complexity demand radical change in enterprise data strategy.

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

THE 2025 Thales Data Threat Report paints a striking picture of an enterprise world on the edge of technological transformation—and exposed to unprecedented risk. As generative AI (GenAI) integrates into core business functions and quantum computing edges closer to cracking classical encryption, data has never been more powerful or vulnerable.

Drawing on insights from 3,163 IT and security professionals across 20 countries and 15 industries, the report reveals a digital landscape where the pace of change is outstripping preparedness. One-third of organizations are already in GenAI adoption's "integration" or "transformation" stages. However, Thales notes that enterprises are rushing ahead without securing foundational safeguards, making the GenAI ecosystem the top security concern for 69% of respondents.

GenAI Races Ahead—but Security Isn't Keeping Up

While data availability and confidentiality have long been security cornerstones, the report highlights growing concern for data integrity and trustworthiness. Attacks targeting these dimensions—such as AI model poisoning or deepfakes—threaten information accuracy and organizational credibility. The explosive growth in API usage, particularly in manufacturing and financial services, adds another layer of vulnerability, as only 16% of organizations prioritize secrets management, despite it being the top DevSecOps challenge.

The rapid spread of GenAI capabilities in SaaS applications and enterprise systems is also creating blind spots. Enterprises are adopting GenAI tools without fully understanding their architectures or assessing the long-term implications of adversarial input, model theft, or data misuse. As the report warns, some enterprises are moving forward without getting their "security or technology houses in order," lured by the urgency to stay competitive.

Some organizations do not wait to get their security or technology houses in order before departing on their AI journey, as the urgency to move into transformation supersedes improvements to organizational readiness.

Quantum Computing and Digital Sovereignty Reshape Data Protection Priorities

Quantum computing, once theoretical, is now a real and rising threat. With successful experiments already cracking 50-bit RSA keys, more than 60% of respondents fear that today's encrypted data could be exposed shortly. Yet, only a third plan to rely on third-party providers for post-quantum cryptography solutions, pointing to a broader industry need for internal crypto-agility.

As regulatory scrutiny intensifies, digital sovereignty is emerging as a strategic differentiator. Half the surveyed organizations are refactoring applications to meet sovereignty mandates, especially in jurisdictions with strict data residency laws. From encryption strategies to software portability, sovereignty is central to cloud adoption decisions.

Despite progress, like improved encryption rates for sensitive cloud data, gaps remain. Only 28% of respondents have formal ransomware response plans, and compliance audit failures continue to correlate strongly with data breaches. Fragmentation of tools and siloed security approaches further complicate unified risk management.

Thales concludes that enterprise security must evolve with AI and cloud innovation. Consolidated platforms, unified data controls, and a proactive stance on sovereignty and cryptography are no longer optional—they are foundational for securing the future of enterprise data. ■



IF YOU run a WordPress website, it's not the time to think that all is well simply because everything appears okay on the surface. Recent research has highlighted that more than 50,000 WordPress sites are vulnerable to hijack and has already breached—many of them without their owners ever realizing it. The problem lies not with WordPress itself, which hosts more than 40% of all websites in the world, but with its vast plugin ecosystem. Hackers are specifically looking for outdated or abandoned plugins and employing a less commonly used feature called the “mu-plugins” directory to add malicious code that runs quietly in the background.

Mu-plugins autoload every time WordPress runs and go unnoticed by administrators in regular maintenance on the site, so it makes them an optimal hiding ground for resilient malicious code. With inside access, attackers can divert visitors to phishing websites, add spam content, or tamper with SEO rankings. Their aim is usually profit—via affiliate scams, ad revenue from fake clicks, or information theft.

How to Bulletproof Your WordPress Site

Think your WordPress site is safe? Think again. Hackers are silently targeting outdated plugins and hidden directories to hijack sites undetected.

By **Shibu Paul** | editor@cioandleader.com

These aren't boisterous or flashy attacks; they're stealthy, ongoing intrusions intended to take over your site, manipulate traffic, and make your digital property a money machine for someone else.

Real-World Exploits

In February 2025, top critical WordPress CVEs vulnerabilities were discovered:

- **CVE-2025-1128:** It was a highly critical security discovered, an unrestricted file upload vulnerability in “The Everest Forms” plugins that allowed attackers upload unrestricted and dangerous files.
- **CVE-2025-0181, CVE-2025-0316, CVE-2025-1061:** These critical authentication bypass vulnerabilities which affected the WP Foodbakers, Nextend Social Login Pro, and WP DirectoryBox Manager plugins for WordPress, which allowed attackers to bypass authentication using an alternate path or channel and gain unauthorized access. These vulnerabilities highlight the importance

of regular updates and vigilant monitoring.

Why Is This So Dangerous?

The fact that these attacks continue to happen is what makes them so worrying. Even when you clean up your plugins and upgrade your WordPress installation, the malware in the mu-plugins directory can go undetected. This means that hackers can have long-term access and control of your site, essentially making it part of a botnet or a scam business without your even knowing.

The damage to reputation can be extreme. An infected WordPress site can be blacklisted by Google, flagged by browsers, and lose the trust of its users in no time.

Here's how attackers are hijacking WordPress sites:

So how, exactly, are the hackers doing this? It's not a quick smash-and-grab—it's a multi-layered plan meant for long-term domination. Here's what happens typically:

1. Exploiting Vulnerable plugins

Hackers scan the webpages for WordPress websites that are using out-of-date or poorly protected plugins. Once they discover a known vulnerability, they use it as a jumping-off point—loading malicious code and gaining entry without triggering alarms. That's why plugin updates aren't simply a best practice; it's a frontline defense.

2. Hiding in Plain Sight (mu-plugins abuse)

After they get in, attackers don't want to be booted out any time soon. That's where the mu-plugins directory is useful. Dubbed "must-use plugins," this unique directory loads its contents automatically on each WordPress initialization—but doesn't appear on the admin dashboard. It's cryptic, tenacious,



Shibu Paul

Vice President – International Sales
Array Networks

and rarely visited by site owners. In other words: it's a great place to hide.

3. Staying Put for the Long Haul

Cleaning out a compromised plugin or even reinstalling WordPress won't necessarily do the trick—because the compromised code cached in mu-plugins remains after the cleanup. It provides hackers with constant access to your site, lying in wait silently as you believe everything is okay.

4. Redirects, Spam, and Botnets

With control secured, attackers can do a lot of damage. They might redirect your visitors to phishing pages, inject spammy links to game search rankings, or even use your server as part of a botnet. You might not notice until your site slows down, traffic drops, or worse—your domain gets blacklisted by Google.

Steps to Protect Your WordPress Site

Securing your WordPress site doesn't have to be a hassle, but it does require attention. Here are the key steps:

- **Update Plugins Regularly:** Most vulnerabilities stem from outdated software. Keep your WordPress core, themes, and plugins up to date. Timely security patches shut down common attack vectors.
- **Remove Unused Plugins and Themes:** Even inactive ones can be exploited.
- **Use Trusted Security Plugins:** Download themes and plugins only from official sources like the WordPress repository. Avoid nulled or pirated plugins—they're often laced with malware.
- **Scan Your Site Regularly:** Use tools like Wordfence, Sucuri, or iThemes Security to run malware scans and detect unauthorized changes.
- **Install a Web Application Firewall (WAF):** A WAF blocks malicious traffic before it reaches your site and helps prevent known exploits.
- **Backup Often:** Automated, regular backups ensure quick restoration if your site is compromised.
- **Audit File Structure:** Check wp-content/mu-plugins for suspicious files and delete anything unusual.
- **Strengthen Admin Access:** Use multi-factor authentication, avoid the default username "admin," and limit admin users. Always follow secure login practices.

Conclusion

Although WordPress provides a solid foundation for creating websites, it is an open platform means that owners must take initiative to ensure security. One needs to be updated, monitor regularly or potential issues, and cleaning up old tools will greatly minimize the likelihood of your site being hacked. Keep in mind, when it comes to cybersecurity, an ounce of prevention is worth a pound of cure. ■

The Looming Quantum Threat: Why We Must Act Now to Secure Cryptography



Quantum computing won't wait. With encryption at risk, organizations must migrate to post-quantum cryptography now—or risk future exposure.

By **Dr. Sandeep K. Shukla** | editor@cioandleader.com

F

FOR YEARS, IBM and other global technology leaders have been making steady progress toward the realization of quantum computing. Alongside them, countries such as China have also claimed moderate success in developing quantum capabilities. While these advancements represent a significant milestone in computing, they also pose a critical security threat that cannot be ignored.

The Quantum Computing Security Challenge

Much of today's cryptographic security infrastructure relies on the hardness of certain mathematical problems. These include integer factorization (which underpins RSA encryption) and the discrete logarithm problem (used in Diffie-Hellman key exchange). The security of these cryptographic systems is based on the assumption that no efficient algorithm exists to solve these problems in polynomial time. If quantum computing reaches a level where these problems can be solved efficiently, most of our existing public-key cryptography will become obsolete.

The ramifications are severe. The entire security framework used to protect financial transactions, government communications, and personal data would be at risk. We have become deeply dependent on these cryptographic methods, and without viable replacements, our ability to secure digital information would be in jeopardy.

The State of Quantum Computing

Some experts argue that practical quantum computing capable



Dr. Sandeep K. Shukla
Chair Professor in Cybersecurity at
IIT Kanpur

of breaking encryption is still 10 to 20 years away. Even Google's recent announcement of its Willow quantum processor, which boasts 123 qubits, is still far from the threshold needed to break modern asymmetric cryptographic systems. Experts estimate that to pose a real threat, quantum computers would need thousands of stable qubits. However, the possibility of a "quantum surprise"—a sudden breakthrough in secrecy—remains a major concern.

Even without an immediate threat, the long-term implications demand urgent action. Many governments and enterprises need their confidential data to remain secure for decades. If an adversary intercepts encrypted communications today, they could store the data and decrypt it later when quantum computing reaches maturity. This is known as the "record now, decrypt later" strategy, and it presents a significant threat to national security, banking, and sensitive corporate information.

Preparing for the Quantum Threat

The U.S. National Institute of Standards and Technology (NIST)

and the Department of Homeland Security (DHS) have already issued guidelines urging federal agencies to prepare for quantum-safe cryptography. India's Ministry of Electronics and Information Technology has circulated similar documents, though they have yet to be mandated. Enterprises and governments must begin transitioning to quantum-resistant cryptographic methods now, rather than waiting until quantum computers become a clear and present danger.

The first step in quantum preparedness is identifying all instances where vulnerable cryptography is being used. This includes software, embedded systems, secure communication protocols, and digital certificates. Organizations must create a comprehensive cryptographic inventory—often referred to as a cryptographic bill of materials (CBOM)—to understand their exposure.

Once vulnerabilities are identified, organizations need to assess the risk associated with each use case. Some legacy systems may be decommissioned before quantum threats materialize, while others may need urgent upgrades. The next crucial step is achieving cryptographic agility, which allows organizations to swiftly replace existing cryptographic algorithms with quantum-safe alternatives without requiring extensive system overhauls.

The Role of Post-Quantum Cryptography (PQC)

NIST has been leading a global effort to standardize post-quantum cryptographic algorithms since 2015. The process has involved multiple rounds of rigorous evaluation and testing. In 2024, NIST finalized its selection of three quantum-safe algorithms:

- **Crystal Kyber** – A key encapsulation algorithm based on lattice-based cryptography.
- **Crystal Dilithium** – A digital signature algorithm that is also lattice-based.
- **SPHINCS+** – A stateless hash-based signature scheme.

Lattice-based cryptography is believed to be quantum-resistant due to its reliance on complex geometric problems that quantum algorithms struggle to solve efficiently. However, these algorithms are not mathematically proven to be quantum-safe; they have merely withstood all known quantum attacks so far. This underscores the need for continued monitoring and adaptability in cryptographic implementations.

Challenges in Implementing PQC

Transitioning to PQC is not as simple as swapping out one algorithm for another. Public key infrastructure (PKI) systems, which issue digital certificates, will need to be updated to support these new algorithms. Given that the current PKI ecosystem took decades to establish, integrating quantum-safe alternatives will require significant effort and time.

Moreover, real-world implementation poses challenges. Cryptographic algorithms often have vulnerabilities not in their theoretical design but in their software and hardware implementations. The infamous OpenSSL Heartbleed vulnerability in 2014 serves as a reminder that flawed implementations can render even the strongest algorithms ineffective. Side-channel attacks, where adversaries extract cryptographic keys by analyzing system behavior, remain a pressing concern. Ongoing research is needed to develop hardened implementations resistant to these threats.

“We’re not just preparing for the future—we’re defending the present from the possibility of a quantum surprise.”

India’s Role in Quantum Security

India has recently launched a national quantum mission aimed at fostering indigenous quantum technology development. As part of this initiative, research institutions such as IIT Kanpur are actively working on implementing and testing PQC algorithms. While India currently follows NIST’s guidelines, there is a possibility that it will develop its own quantum-safe standards tailored to its unique security needs.

For Indian enterprises and government agencies, waiting for a government mandate may be too late. The financial sector, in particular, should start planning its quantum transition now. The Reserve Bank of India (RBI) and other regulatory bodies must issue clear directives on PQC adoption timelines, mirroring efforts by NIST and DHS.

The Urgency of Quantum Preparedness

Despite the 10- to 20-year horizon for large-scale quantum computing, organizations cannot afford to delay. The process of migrating to quantum-safe cryptography will take years, and the threat of retrospective decryption is real. The Moskowitz Theorem underscores this urgency: if the time required to deploy quantum-safe algorithms (Y) plus the number of years data must remain confidential (X)

exceeds the estimated time to practical quantum computing (Z), then organizations are at risk.

Governments and enterprises must take proactive steps now:

- **Identify Quantum-Vulnerable Cryptography** – Conduct a cryptographic inventory to locate weak algorithms in use.
- **Assess Risks and Prioritize Migration** – Determine which systems need immediate transition to quantum-safe alternatives.
- **Achieve Cryptographic Agility** – Develop flexible cryptographic frameworks that allow for seamless algorithm replacement.
- **Adopt PQC Algorithms** – Begin implementing NIST-approved quantum-resistant cryptography.
- **Upgrade PKI Infrastructure** – Ensure that digital certificates support quantum-safe key exchanges and signatures.
- **Monitor Cryptographic Advances** – Stay informed about new vulnerabilities and advancements in PQC.

Conclusion

The threat of quantum computing to modern cryptography is no longer theoretical—it is a matter of when, not if. Organizations must start planning their transition to quantum-safe cryptography today. Regulatory bodies must enforce mandates to accelerate migration, and enterprises must embrace cryptographic agility to future-proof their security frameworks. Waiting until quantum computers become powerful enough to break today’s encryption will be too late. The time to act is now.

(This article is inspired by a talk given by Dr. Sandeep K. Shukla, Chair Professor in Cybersecurity at IIT Kanpur, at the CISO Forum in December 2024. Some content has been edited for brevity.) ■

Powering the Future of AI with Governance, Intent, and Human Oversight

Nishant Rathi, Co-Founder of NeoSOFT, emphasizes that success will depend on thoughtful implementation, cultural readiness, and a clear focus on long-term impact.

By **Nishant Rathi** | editor@cioandleader.com

IN TODAY'S hypercompetitive landscape, organizations everywhere are betting large on artificial intelligence (AI) to give them a transformative edge. Even as innovation accelerates, companies recognize the crucial role of ethics and regulation in AI development, with 88% of C-level executives reporting their organizations as taking measures to communicate the ethical use of AI to their workforces.

Why are ethics and regulation so important in the race to put AI innovations to market?

New AI innovations introduce new ethical concerns

Advances in AI have meant that we have moved from building systems that make decisions based on human-defined rules to automated rule definition, content creation and decision-making by complex models trained on huge data sets. An unconstrained AI system will prioritize optimizing their inputs according to the defined objectives, often without regard for broader societal impacts or ethical considerations, eroding public trust.

Despite advancements, AI today continues to encounter issues including bias and hallucinations, which have resulted in some controversial outcomes. For instance, a 2025 report by MeitY

highlights cases of biased hiring algorithms and facial recognition errors in India, emphasizing the need for diverse and transparent training data. Addressing these issues is crucial to ensure AI systems are fair, reliable, and beneficial for all users.

Similar controversies have emerged worldwide, from unfair loan disbursements due to gender discrimination, to the use of privacy-breaching facial recognition technologies to process insurance claims.

Many of these events can largely be attributed to issues with explainability. AI, especially deep learning models, learn in a way that does not follow the straightforward rules humans use. These models are often seen as a “black box” because of the inhumanely complex layers of calculations they use to arrive at decisions. Thus, many experts find it a challenge to understand how AI comes to conclusions. Without appropriate human supervision and understanding, these biased decisions could spiral into negative outcomes like the ones above.

Keeping the focus on ethics has never been more important, especially as new generative AI innovations, like Phenomenal AI's text-to-video platform developed in India promise to accelerate productivity at the workplace and

enable organizations to sharpen their competitive edge. Despite their great potential, these generative tools can introduce issues like copyright infringement – and worse still, open the doors to misuse and misinformation.

Need for public and private sectors to work together to embed ethics and regulations into AI

While many generative AI tools, like ChatGPT, have rules to prevent abuse, many users have found ways to break these safeguards. Cybercriminals have even created their own generative pre-trained transformers (GPTs) to code malware and create highly convincing phishing emails at scale.

There are currently few tools and laws which can effectively detect and deter the production of such harmful outputs. As such, the public and private sectors need to tighten collaboration to better regulate AI to reduce the risks of misuse, and ensure that models are created with ethics in mind.

Ethical AI involves integrating core ethical principles, accountability, transparency, explainability, and good governance into AI models. Improving explainability and strengthening ethics in models can help organizations address AI's shortcomings today. It also can greatly improve the accuracy and effectiveness of decision-making.

Many public and private sector entities are working together to advance ethical AI. For example, in India, the government is taking an increasingly active role in shaping responsible AI development. A publicly funded AI compute infrastructure, AI Kosha, with a total capacity of over 10,000 GPUs, is being established to support innovation across startups, research institutions, and enterprises. This AI Compute Network is designed to accelerate the



Mayank Baid

Regional Vice President, India & South Asia, Cloudera

safe and scalable adoption of AI and foster a robust ecosystem rooted in trust and responsibility. As regulations and initiatives continue to roll out, organizations can play their part to advance ethical AI by ensuring the data they use is trusted.

Designing ethical enterprise AI systems requires trusted data

Building AI systems that people trust requires organizations to have trusted information sources. With accurate, consistent, clean, bias-free, and reliable data as the foundation, an ethically designed enterprise AI system can be relied on to consistently produce fair and unbiased results. Here are some tips for organizations looking to develop better ethical AI systems:

- **Focus on intent:** An AI system trained on data has no context outside of that data. There is no moral compass, no frame of reference of what is fair unless we define one. Designers, therefore, need to explicitly and carefully construct a representation of the intent motivating the system's design. This involves identifying, quantifying, and measuring ethical considerations while bal-

ancing these with performance objectives.

- **Consider model design:** Well-designed AI systems are created without bias, causality and uncertainty in mind. Organizations should remember that apart from data, model designs can also be a source of bias. Organizations should regularly audit them for model drift – when a model starts to become inaccurate over time due to outdated data.
- **Ensure human oversight:** AI systems can reliably make good decisions when trained on high-quality data. However, they lack emotional intelligence and cannot deal with exceptional circumstances. The most effective systems are ones that intelligently bring together both human judgment and AI. Organizations must always ensure human oversight, especially in situations where AI models produce outputs with low confidence.
- **Enforce security and compliance:** Developing ethical AI systems centered on security and compliance will strengthen trust in the system and facilitate adoption across the enterprise, while ensuring adherence to local and regional regulations.
- **Harness modern data platforms:** Leveraging advanced tools, like data platforms that support modern data architectures, can greatly boost organizations' ability to manage and analyze data across the entire data and AI model lifecycle. Ideally, the platform should have built-in security and governance controls that allow organizations to maintain transparency and control over AI-driven decisions – even as they deploy data analytics and AI at scale. ■



Sanjay Gupta
VP & MD, South Asia & Middle East,
NICE

The real CX begins before the first contact

Sanjay Gupta, VP & MD at NICE, on how early understanding of customer intent is redefining CX—shifting it from reaction to intelligent anticipation.

By **Mushrrat Shahin and Jatinder Singh** | jatinder.singh@9dot9.in

CUSTOMER EXPERIENCE (CX) is fast becoming the primary yardstick by which organisations are measured. In industries such as banking, telecom, e-commerce, and digital services, customers increasingly judge businesses not just by what they offer, but by how quickly, intelligently, and seamlessly they respond to their needs.

This shift has placed pressure on organisations to engage in real time, across multiple channels, and with a level of personalisation and empathy that feels natural to the customer. AI and automation, once seen as efficiency tools, are now central to enabling this shift—from reactive service to proactive, predictive engagement.

NICE, a long-time player in the enterprise technology space, has

focused its efforts on this evolving front. Known for its work in customer analytics, contact centre operations, and automation, the company has increasingly built its capabilities around cloud-based, AI-driven platforms aimed at helping organisations make their customer interactions more contextual and anticipatory.

In this interview, Sanjay Gupta, who oversees NICE’s business across South Asia and the Middle East, dis-

cusses what it means to rethink CX in an AI-first environment—and how enterprises can design systems that understand customer intent from the outset.

CIO&Leader: How do you see customer experience transforming over the next 3–5 years with AI and automation gaining momentum?

SANJAY GUPTA: We’re witnessing a fundamental shift in how organisations view and deliver CX. AI is moving from the periphery to the centre. Over the next three to five years, I expect this transformation to accelerate—with AI driving changes across self-service, agent-assisted support, and fully automated interactions.

The focus is shifting from transactional efficiency to intelligent orchestration. Whether through AI agents or augmented human agents, success will depend on

Structured, accessible knowledge isn’t optional anymore—it’s the foundation for deploying effective AI across channels.

how well a business understands customer intent in real time and responds with contextually relevant, emotionally aware service. CX is no longer a back-end function—it's becoming a strategic differentiator led by insight and automation.

CIO&Leader: What approaches are enterprises adopting to move from reactive service models toward more proactive and predictive customer engagement—and how is NICE supporting this shift?

SANJAY GUPTA: Our approach rests on three pillars: agents, workflows, and knowledge. These are the essential elements for building intelligent and anticipatory service experiences.

Let's start with agents—both human and AI-powered. We're enabling them to access real-time guidance, sentiment cues, and knowledge insights right when they need them. This not only improves accuracy but ensures agents are empathetic and proactive in resolving issues.

Next, knowledge. Today, knowledge must be accessible at the very start of the customer journey—even before the customer reaches out. Whether a user enters a query via search, app, or website, the system must anticipate what they're looking for and guide them immediately.

Finally, workflows. Front-end automation is just the tip of the iceberg. Unless the back-end is automated with intelligent workflows—from fulfillment to resolution—you can't deliver consistent, scalable CX. At NICE, we provide a platform that unifies these three layers, helping organisations transition from reactive firefighting to proactive service delivery.

CIO&Leader: What are the key challenges and opportunities in

The ability to understand customer intent—often before a direct interaction—will separate leaders from laggards in the next phase of CX.

delivering a unified, omnichannel customer journey—and how is NICE addressing them?

SANJAY GUPTA: The challenge lies not just in being present across channels, but in orchestrating coherent, context-aware experiences across them. Today, the journey may begin with a web search, continue on a mobile app, and end with a conversation via chat or voice. Each of these interactions needs to be connected, with full context transferred seamlessly.

The opportunity is in engaging customers at the point of intent emergence—when they're searching, exploring, or browsing. If you can fulfill their need right there—through intelligent self-service or routing to the right agent—you not only solve their problem faster but also increase loyalty.

Our solutions ensure that the context of every interaction is preserved, sentiment is understood, and journeys are completed intelligently. We also equip agents with tools that help them manage complex omnichannel flows efficiently, without losing the human touch.

CIO&Leader: Looking ahead, which three trends do you believe will shape the future of CX?

SANJAY GUPTA: Three trends stand out.

First, knowledge-powered self-service. The more accurately

you can anticipate and address common issues through intuitive self-service, the fewer escalations you'll see—and the more empowered your customers will feel. This isn't just about deploying chatbots; it requires structured knowledge, real-time updates, and integration with conversational AI to ensure relevance and accuracy. It's about meeting customers at their point of intent—whether through voice, search, or app—and resolving their needs without requiring human intervention.

Second, next-generation agent enablement. As simpler queries are handled by self-service, the interactions that reach agents are increasingly high-stakes—often emotionally charged or complex. Agents must evolve from process executors to trusted advisors. This demands dynamic access to knowledge, real-time guidance, and visibility into customer sentiment and journey context. AI must act as a co-pilot—helping agents personalise responses while reducing cognitive load.

Third, the emergence of unified, AI-ready knowledge frameworks. Every successful CX deployment will depend on the strength of its knowledge architecture. Generative AI models can only perform well when drawing from a clean, curated, and centralised pool of organisational intelligence. Enterprises must treat knowledge not as a byproduct of operations but as a core strategic asset—one that informs automation, training, service design, and analytics.

Ultimately, CX over the next twelve months—and beyond—will be shaped by how intelligently organisations combine self-service, empowered agents, and AI-fed knowledge to deliver seamless, context-aware, and proactive engagement—often before customers even realise they need it. ■



Vishal Salvi
Chief Executive Officer,
Quick Heal Technologies Ltd

AI Arms Race: How India's Tech Hubs Became Cybersecurity Battlegrounds

Vishal Salvi, Chief Executive Officer of Quick Heal Technologies Ltd discusses India's evolving cyber threats, emphasizing AI-driven security solutions, behavior-based detection, and the need for zero-trust frameworks as organizations combat increasingly sophisticated attacks in 2025.

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

A **AS INDIA** battles an unprecedented wave of cyber attacks, with a staggering 369 million malware detections across the nation, organizations face increasingly sophisticated threats designed to evade traditional security measures. In this exclusive interview with CISO Forum, Vishal Salvi, Chief Executive Officer of Quick Heal Technologies Ltd, reveals the alarming reality behind these statistics and shares how his company's Seqrite solutions are leveraging artificial intelligence to transform cyber defense. From the 974% surge in behavior-based

malware to the targeting of critical sectors like healthcare and finance, Salvi provides a sobering assessment of India's cybersecurity landscape while offering strategic insights on how enterprises can build resilience against the next generation of AI-powered threats. As regional technology hubs become prime targets and hacktivism escalates alongside geopolitical tensions, Salvi explains why conventional security approaches are failing and how Quick Heal is pioneering AI-driven solutions to stay ahead in this evolving digital battlefield.

CIO&Leader: India is witnessing a surge in cyber threats, with over 369 million detections. What are the primary reasons behind this increase, and how has the threat landscape evolved in recent years?

VISHAL SALVI: India's cyber threat landscape has intensified dramatically, as highlighted in our India Cyber Threat Report 2025, prepared by our researchers at Seqrite Labs, India's largest malware analysis facility, in association with DSCI. Their in-depth analysis revealed 369.01 million malware detections across 8.44 million installations,

emphasizing the alarming rise in cyber threats from four primary factors; first, rapid digital transformation has expanded the attack surface, particularly in healthcare, hospitality, and financial sectors, which experienced detection rates of 21.82%, 19.57%, and 17.38% respectively per endpoint.

Second, we're witnessing regionalization of threats, with technology corridors in Telangana (15.03%), Tamil Nadu (11.97%), and Delhi (11.79%) facing the highest concentration of attacks. Third, attack methodologies have evolved significantly, with behavior-based malware detections increasing by 974.6% since 2021, jumping from 5 million to 53.73 million. Geopolitical tensions are fueling cyber warfare, as 150+ hacktivist groups targeted Indian entities in 2023, with daily attacks exceeding 50 incidents, often linked to the Israel-Palestine and Russia-Ukraine conflicts. These findings highlight the urgent need for AI-driven threat intelligence and stronger cybersecurity measures to protect India's digital infrastructure.

CIO&Leader: With Trojans accounting for 43.38% of all detections, what risks do they pose to enterprises, and how can organizations effectively protect themselves against such targeted attacks?

VISHAL SALVI: When we look at Trojans, the danger lies in their versatility. These aren't simple viruses. They create backdoors that persist in your systems, move laterally across networks, and steal valuable credentials. Let me give you a real example we've investigated. We've tracked variants like Trojan.Sys scan that brute-forces their way into systems to create hidden administrator accounts. Recently, in Karnataka, attackers used this exact approach. They gained initial

“Looking ahead at India's cybersecurity landscape over the next five years, several critical trends are emerging that business leaders should prepare for today.”

access and then pivoted to extract entire sensitive databases.

Enterprises can adopt a multi-layered approach to cybersecurity. First, behavior-based detection is essential. It accounts for about 14.5% of our detections and catches threats that traditional signature-based systems miss. We also strongly advocate for zero-trust security frameworks. At Seqrite, we've integrated these principles with our advanced threat detection and network access tools to validate every access request. Combine this with good email filtering and network segmentation, and you'll significantly limit the impact of any breach.

CIO&Leader: Many organizations still struggle with cybersecurity preparedness. In your view, what are the key gaps in enterprise security strategies, and how should companies address them?

VISHAL SALVI: AI-powered cyber threats like the BlackMamba keylogger represent a paradigm shift in security. They use AI for evasion and payload generation to create polymorphic malware that adapts to defenses in real-time. To combat these threats, organizations must move beyond signature-based detection, which represents 85% of current detections but cannot keep

pace with evolving attack patterns.

To counter this, organizations must prioritize behavior-based detection, which identifies malicious activity based on patterns rather than static signatures. Our data shows a 974.6% surge in behavior-based detections since 2021, highlighting its growing necessity. AI-driven predictive analytics further strengthen security by detecting emerging risks before they escalate.

The human element remains critical, with awareness training evolving to counter AI-generated social engineering attacks. At Seqrite, our XDR solutions leverage machine learning (ML) models to effectively detect and neutralize AI-driven cyber threats. Beyond this, we are developing unsupervised ML models that learn autonomously from vast datasets of malicious activity, enabling real-time anomaly detection.

Looking ahead, we are advancing "AI for AI" — experimental AI models designed to detect and neutralize AI-generated attacks, ensuring proactive defense against the next generation of cyber threats.

CIO&Leader: Seqrite is leveraging AI and ML for threat detection and response. Can you share insights on how AI-driven automation enhances cybersecurity resilience?

VISHAL SALVI: At Seqrite, we are making substantial investments in AI and machine learning. These technologies hold immense potential for transforming how we protect our customers. Our research team analyzes threat patterns across our base of 10 million endpoints. This gives us incredible insight into emerging threats and helps us dramatically reduce false positives, a huge pain point for security teams. More importantly, it allows us to identify zero-day

threats before they have been widely recognized.

Seqrite's comprehensive security solutions, powered by the self-aware malware-hunting technology GoDeep.AI, auto-remediate threats in real-time, shrinking response windows from hours to seconds. Furthermore, our Malware Analysis Platform combines static, dynamic, and manual analysis to neutralize suspicious files preemptively. AI in cybersecurity also alleviates alert fatigue by prioritizing critical incidents, freeing SOC teams to focus on strategic work rather than sifting through endless alerts.

CIO&Leader: Given the increasing sophistication of cyberattacks, what are the primary cybersecurity trends you foresee in India over the next five years?

VISHAL SALVI: Looking ahead at India's cybersecurity landscape over the next five years, several critical trends are emerging that business leaders should prepare for today. First and most concerning of all is how generative AI will transform threats. We already see early signs of hyper-personalized phishing attacks and deepfake-driven social engineering. This is why we're heavily investing in AI-augmented defense capabilities at Seqrite.

For India specifically, we expect cryptojacking to remain a persistent threat. As our country expands its computing infrastructure, these attacks will follow the resources. Similarly, ransomware will continue targeting our critical sectors, with healthcare being particularly vulnerable because of its essential nature and often limited security resources.

The perimeter-based security model is rapidly becoming obsolete. We advise all our enterprise customers to move toward identity-

centric security and zero-trust frameworks. Also, compliance will drive significant investment as India continues to evolve its data protection laws. Companies that prepare early will have an advantage. To help our customers adhere to the new, strengthened laws, we have ensured that all our products comply with the recently released DPDP Draft Rules.

CIO&Leader: Employee training and awareness are critical in mitigating cyber threats. What initiatives does Quick Heal Technologies Limited undertake to help enterprises build a stronger cybersecurity culture?

VISHAL SALVI: We have always believed that technology alone can't solve cybersecurity challenges at Quick Heal Technologies Limited. It's the human element that makes all the difference. That's why we have invested heavily in building Quick Heal Academy as a cornerstone of our cyber education initiatives. We have also developed specialized corporate training programs for enterprises that combine technical depth with real-world scenarios.

We are also addressing the talent pipeline challenge through our industrial training course. To that end, we have also joined forces with Chitkara University and Quantum University to offer long-term cybersecurity courses. We have introduced short-term learning modules for enterprises looking to build continuous learning cultures that employees can access from anywhere, anytime. These daily drills cover everything from spotting deepfake videos to secure BYOD practices. We introduce new courses to help organizations update their employees with the latest technical know-how and cybersecurity best practices.

CIO&Leader: How does Seqrite balance global threat intelligence with localized insights to provide enterprises with tailored cybersecurity solutions?

VISHAL SALVI: At Seqrite, our approach to threat intelligence balances global insights with deep local understanding, which gives us a unique advantage in protecting Indian businesses. We collect telemetry from our global sensor network and combine it with India-specific data from over 10 million nationwide endpoints. This combination is powerful because threats often have regional variations or targeting patterns.

Let me share a concrete example. We recently conducted an in-depth threat study in Karnataka that revealed that Bengaluru experienced approximately 9.5 million threat detections - four times higher than the state average. This granular, localized insight helps us tailor our protections for businesses in different regions.

We have also established valuable partnerships with Indian and international organizations like the DSCI and the NIST, which significantly enriches our understanding of the local threat landscape. At the same time, we ensure our threat intelligence uses standardized protocols that easily integrate with the security tools our customers already have in place. This dual focus lets us predict global threat waves while preempting region-specific campaigns, like cryptojacking surges targeting Indian enterprises.

CIO&Leader: What innovations are you currently working on, and how do they address the pressing concerns faced by CISOs today?

VISHAL SALVI: We take immense pride in the several innovations we have developed at Seqrite. First, there's our Malware Analysis Plat-



"AI-powered cyber threats like BlackMamba represent a paradigm shift in security. They use AI for evasion and payload generation to create polymorphic malware that adapts to defenses in real-time."

form (SMAP). We built this to solve two critical problems: the risk of zero-day threats and the overwhelming volume of alerts security teams face. SMAP performs deep analysis of suspicious files and combines this with real-time threat data to identify previously unknown threats.

Our unified EDR-ZTNA security solutions combine advanced threat detection with zero-trust network access. This is particularly important now that most organizations operate in hybrid environments with employees working from anywhere. I'm particularly proud of our work with AI and machine learning models that automatically prioritize security incidents. This addresses the alert fatigue problem I mentioned earlier and helps

security teams focus on what truly matters, significantly reducing response times.

We understand that organizations have different infrastructure needs, so we have designed our solutions to be flexible. They can be deployed in the cloud, on-premises, or hybrid configurations. This flexibility ensures that security doesn't hinder your preferred IT strategy. Another pain point we're addressing is compliance reporting. We've built automated reporting capabilities that significantly reduce the burden during audits.

The common thread across all these innovations is our focus on simplifying complexity, enhancing visibility, and aligning security with business outcomes. We firmly believe that security shouldn't be

an obstacle to business – it should be an enabler.

CIO&Leader: What should be the top priorities for CISOs in 2025?

VISHAL SALVI: First and foremost, security leaders need to translate cyber risks into business terms better. Quantifying risks using metrics like 'time-to-contain breaches' or 'potential financial impact' dramatically improves leadership buy-in and funding support. At Seqrite, we also strongly advocate for the adoption of behavioral analytics. As credential theft becomes increasingly sophisticated, traditional password protections aren't enough. Systems that automatically flag anomalous login patterns – like an employee suddenly accessing systems at 3 AM from an unusual location – provide an essential layer of protection.

Zero Trust security frameworks are gradually becoming non-negotiable as remote and hybrid work becomes permanent. We need to validate every access request regardless of where it originates. Automation should also be a top priority. Security teams are overwhelmed, and automation of routine SOC workflows increases efficiency by creating the capacity to address more strategic security challenges. At the same time, we must shift focus from prevention to ensuring business continuity during and after attacks. This means regular drills and clear recovery protocols.

Lastly, identity security—protecting human and machine identities—will become increasingly critical as organizations expand their use of SaaS applications and IoT devices. By focusing on these priorities, CISOs can better align security efforts with organizational growth objectives, turning security from a perceived obstacle into a business enabler in this challenging threat environment. ■

Where CIOs Lead, Conversations Thrive

Join the exclusive **CIO&Leader LinkedIn Group**-a vibrant community where IT leaders like **YOU** come together to connect, collaborate, and share insights. With engagement levels higher than all our leading competitors combined, this is the ultimate platform to keep you informed, inspired, and ahead of the curve.

Discover curated content, leadership Insights, and thought leadership tailored for today's CIOs. Be part of the conversations that matter, learn from industry pioneers and network with the best minds in the industry.

The CIO&Leader community is your gateway to thought-provoking dialogue, cutting-edge tech & trends and actionable strategies.

**Join the CIO&Leader
LinkedIn Group today
and elevate your
leadership journey.**

Follow us on **LinkedIn**
@CIOandLeader

Scan the QR Code to follow



Source: LinkedIn Analytics | Time range: 1 April 2025 - 29 June 2025.
Total engagement metrics: Reactions, comments & shares.
Percentage shows change from the previous 90 days.

Total engagement metrics		
Last 90 days		
1	CIOandLeader Your Page	47,730 ▲ 69.5%
2	ETCIO	26,972 ▲ 53.8%
3	ETCISO	16,269 ▲ 30.4%
4	Information Security Media Group (ISMG)	15,485 ▲ 233.6%
5	CISO FORUM	6,125 ▲ 118%
6	Express Computer	5,833 ▲ 11.8%
7	Dataquest	4,785 ▲ 9.9%
8	ETTelecom	983 ▼ 84.4%

You can also visit us at:
www.cioandleader.com

For more information, write to:
editor@cioandleader.com

AMD PRESENTS



26th Annual Conference

CIO&LEADER

AI: From Pilot to Production
1st-3rd August, 2025 • Ritz Carlton, Pune

CO-PRESENTED BY **NxtGen⁷**

#CIOandLeaderConference

The 26th Annual CIO&Leader Conference is not just another tech gathering. It is a curated leadership experience where India's most forward-thinking CIOs converge to discuss, debate, and drive the transition of AI from experimentation to enterprise-wide impact.

Over three dynamic days, the conference will bring together 200+ top CIOs and IT leaders, global AI experts, and many more.

Eminent Speakers @26th Annual CIO&Leader conference

Guest of Honour

**Shri Adv
Ashish Shelar**

Minister for Information
Technology & Cultural Affairs,
Government of Maharashtra



Partha Iyengar

Ex-Gartner Fellow, Country
Manager Research (India), Gartner,
HBR Author, Ex Board Member
SBI, Speaker, Advisor



Prof Balaraman Ravidran

Head: Wadhvani School of Data
Science & AI / Robert Bosch
Centre for Data Science & AI /
Centre for Responsible AI
IIT Madras



Janhavi Chitale

Chief Information Officer
CIO, Chitale Bandhu Mithaiwale
Co-founder of Intelligente
Solutions, an analytics start-up

Know more: <https://annualconference.cioandleader.com/> Follow us:  @CIOandLeader

For partnership inquiries, write to **Hafeez Shaikh, hafeez.shaikh@9dot9.in, +91 9833103611**

