VOLUME 2, ISSUE 3 | JULY 2026

Tech Disruptor media.com

techdisruptormedia.com techdisruptormedia

Pg 26
INTERVIEW
Arun Attri
CDIO
Wonder Cement Ltd.

CYBERSECURITY IN THE AGE OF AI

FROM VULNERABILITIES TO EXPOSURE MANAGEMENT

RAJNISH GUPTA
Architecting Modern Cyber Defence

A BRAND OF BNG
bharatnetworkgroup.com

2nd Chapter

CIO HORIZON

Where Vision Becomes Direction

2026

Meet 100+ tech leaders at the industry's most premium summit

3-5 JULY 2026 | RAMADA BY WYNDHAM, HOTEL & CONVENTION CENTER, LUCKNOW

Lucknow

An Initiative of

BNG BHARAT™ NETWORK GROUP

Concept by

Tech Disruptor media.com

For partnership opportunities, please contact

Naman Singhal
naman@thefoundermedia.in
+91 9267933240

Abhinav Chaudhary
abhinav@thefoundermedia.in
+91 8700749849

Tech Disruptor media.com

Your feedback about this magazine is welcomed at

editor@thefoundermedia.com

info@thefoundermedia.com

FOUNDERS
ASHISH SRIVASTAVA
ANUPAM GUPTA

DIRECTOR - IT & DIGITAL STRATEGY
ATUL KUMAR PANDEY

AGM - ART & DESIGNING
VIPIN RAI

DGM - CONFERENCE STRATEGY & PLANNING
ISHA SRIVASTAVA

CONSULTING EDITOR
BALAKA BARUAH AGGARWAL

SENIOR ASSOCIATE EDITOR
AISHWARYA SAXENA

ASSISTANT EDITOR
JEEVIKA SRIVASTAVA

ASSISTANT MANAGERS - SALES & MARKETING
NAMAN SINGHAL
ABHINAV CHAUDHARY
TAPOSHI BOSE
NISHIT SAXENA
DEVIKA GULATI

ASSISTANT MANAGER - EVENTS & BOOTHIFY
ANKUR SRIVASTAVA

HR MANAGER
POOJA SHRIVASTAVA

EVENT ASSOCIATE
NEHA GUPTA

MIS EXECUTIVE
PRAGYA SUMAN

EXECUTIVE - 3D DESIGNER
AJAY TOMER

This magazine is published under/as a part of "HELLO FOUNDER INFOMEDIA PRIVATE LIMITED, an UTTAR PRADESH-based private limited company registered at the Ministry of Corporate Affairs (MCA). The Corporate Identification Number (CIN) of HELLO FOUNDER INFOMEDIA PRIVATE LIMITED is U56210UP2023PTC191833 and registration number is U56210UP2023PTC191833. HELLO FOUNDER INFOMEDIA PVT LTD's registered office address is Flat No 1006 10th Floor, Tulip 3 Gulmohar Garden, Raj Nagar Extension, Ghaziabad, Uttar Pradesh, India, 201017. All rights reserved throughout the world. No part of this magazine may be reproduced.

Copying, whether electronically or otherwise, either wholly or partially, without prior written permission, is strictly prohibited.

VOLUME 2, ISSUE 3 | JULY 2026

Table of CONTENT

50

Ashish Srivastava (L) and Anupam Gupta (R), Founders, Bharat Network Group (BNG)

FROM THE FOUNDERS' DESK

INTELLIGENCE AT SCALE: THE NEXT COMPETITIVE ADVANTAGE

Dear Prime Reader,

Artificial Intelligence is no longer a future ambition. It is rapidly becoming the operating layer of modern enterprises, transforming how businesses innovate, compete, and create value. Yet technology alone is not enough. Success will depend on an organization's ability to combine data, governance, human expertise, and responsible AI practices into a unified strategy.

That is what makes the rise of the AI-native enterprise one of the most significant business transformations of our time. It is not simply about deploying new tools. It is about reimagining how work gets done, how decisions are made, and how intelligence can be scaled across the enterprise.

This edition of **Tech Disruptor Media** places that transformation in focus.

Through the insights of forward-looking technology leaders, we explore how organizations are moving from experimentation to enterprise-wide adoption, embedding AI into core operations, and preparing for a future where intelligence becomes a competitive advantage.

WHETHER YOU ARE AN ENTREPRENEUR OF A SEASONED BUSINESS OWNER, (WHO HAS EMBRACED TECHNOLOGY) WE INVITE YOU TO SHARE YOUR EXPERIENCES AND INSIGHTS WITH OUR COMMUNITY. WE ENCOURAGE YOU TO CONTRIBUTE YOUR STORY, ARTICLES, OR INSIGHTS ON VARIOUS ASPECTS OF YOUR ENTREPRENEURIAL JOURNEY.

Describe the Path

You have Travelled

Inspire, Connect & Empower

We celebrate the entrepreneurial journey and achievements of individuals who dared to dream and toiled hard to make those come true. We believe that every success story is unique and has the potential to inspire and empower others.

SCAN THE QR CODE
& Start Inspiring Everyone Around

At Bharat Network Group, we are a dedicated team of passionate entrepreneurs,storytellers and innovators. We understand the drive, ambition and challenges founders face, because we are founders ourselves.

INDIA'S LEAP FROM DIGITAL TO INTELLIGENCE

Technology conversation has fundamentally changed from digitization to Artificial Intelligence. AI is rapidly transforming itself from a tool that automates processes into one that augments decision-making, predicts outcomes, creates content, and increasingly acts autonomously. We are witnessing the emergence of a new era—one where intelligence itself is becoming a strategic asset. The organizations, industries, and nations that succeed in this transition will not simply deploy AI; they will learn how to embed intelligence into every layer of their operations, services, and ecosystems. This edition of Tech Disruptor explores that transition from multiple perspectives.

In our story, *India's AI Moment: From Digital Public Infrastructure to Global AI Leadership*, we examine why India finds itself at an inflection point in the global AI race. India brings together a rare combination of advantages: digital public platforms operating at population scale, one of the world's largest developer communities, rapidly expanding compute capacity, and a vibrant innovation ecosystem. The world is watching how will India help define the AI revolution.

As AI adoption accelerates, organizations are discovering that compute capacity, data management, and digital resilience are becoming strategic considerations. Our feature on AI-powered data centres explores how these facilities are evolving from back-office utilities into mission-critical assets that power enterprise intelligence. Increasingly, competitive advantage will depend not only on access to AI models but the ability to process, manage, and operationalize intelligence at scale.

At the same time, intelligence without trust is unsustainable. Our cybersecurity feature highlights a reality many organizations are only beginning to appreciate: the traditional security perimeter has disappeared and security has become a business imperative. Governance, privacy, accountability, and security-by-design that will determine whether organizations can harness AI responsibly while preserving trust. The issue also explores one of the most powerful examples of technology-led inclusion anywhere in the world. The story of UPI demonstrates how thoughtfully designed digital platforms can create participation at unprecedented scale. What began as a financial inclusion initiative has evolved into a global blueprint for how technology can democratize access, empower innovation, and drive economic growth.

Taken together, these stories point to a larger transformation underway. The next phase of technology evolution will be defined by the ability to combine intelligence, scale, trust, and inclusion into a cohesive ecosystem. For India, this moment presents a historic opportunity wherein the challenge now is to build intelligent systems that deliver economic value, societal impact, and global competitiveness at scale.

Balaka Baruah Aggarwal
Consulting Editor
balaka.baruah@thefoundermedia.in

COVER STORY

THE FUTURE OF CYBERSECURITY IS EXPOSURE MANAGEMENT

WHY CYBER RESILIENCE DEMANDS A NEW SECURITY MINDSET

India has emerged as one of the world's most dynamic cybersecurity markets, driven by rapid digital transformation, cloud adoption, AI initiatives, and the rise of Global Capability Centers. In a freewheeling interview with **Balaka Baruah Aggarwal,** Consulting Editor, **Rajnish Gupta, Managing Director, India and SAARC at Tenable**, shares his perspective on the evolving cyber threat landscape, the growing importance of exposure management, AI-powered security, and the role India plays in driving innovation, product development, and business outcomes across Tenable's global ecosystem.

Tenable has steadily expanded its footprint in India over the years. How important is the Indian market in Tenable's global growth strategy, and what role does the India team play within the broader organization?

India is absolutely critical to Tenable's global growth strategy. We've witnessed an unprecedented scale of digital transformation across the country, not just in major metros, but increasingly in up-and-coming markets that are rapidly evolving into technology hubs.

The role of the India team extends far beyond regional sales and market penetration. We operate as a strategic hub for the broader organization. Our local operations mirror the mature Global Capability Center (GCC) model. We are tapping into India's unparalleled engineering and cybersecurity talent to drive global product innovation, threat research and customer success. The feedback and complexities we manage for Indian enterprises directly influence our global platform development.

Cybersecurity conversations have evolved from vulnerability management to exposure management. How is Tenable helping organizations gain a more comprehensive view of cyber risk across their environments?

Giving a CISO a list of 10,000 vulnerabilities isn't security—it's homework. Indian enterprises are drowning in fragmented data silos that create dangerous blind spots, and traditional security methods fail to provide insights into how to actually drive down risk. The industry must move away from the reactive "patch everything" mentality and adopt a proactive exposure management approach.

Tenable is leading the shift to exposure management with the Tenable One Exposure Management Platform.

RAJNISH GUPTA
MANAGING DIRECTOR, INDIA
AND SAARC, TENABLE

We help organizations transition from simply identifying flaws to proactive, precise risk reduction.

Tenable One breaks down fragmented data silos by integrating native telemetry from across the entire modern attack surface—IT, AI, cloud, identity and operational technology (OT)—custom data sources and over 330 pre-built integrations. This vast repository of exposure data is normalized and contextualized by Tenable One, delivering the most complete and prioritized view of risk. Instead of chasing 10,000 vulnerabilities, security teams can focus efforts on the exposures that matter most.

What are the most significant cybersecurity challenges Indian enterprises are grappling with today, particularly as they accelerate cloud adoption, AI initiatives, and digital transformation programs?

Indian enterprises are facing a perfect storm of complexity, driven by three major challenges:

- **Securing sanctioned and unsanctioned AI:** The security challenges introduced by AI have skyrocketed along with their adoption. There's vulnerabilities in the models, prompt injections, insider threats inputting sensitive data into the models, and more. AI is deeply connected in enterprises.
- **The Burden of Compliance:** With new regulations like India's DPDP Act, the manual burden of compliance reporting and governance is crushing security teams.
- **CISO Tool Fatigue:** Organizations have deployed dozens of standalone security tools over the years. Managing this fragmented legacy stack leads to operational fatigue and chaotic visibility gaps.

Tenable's portfolio spans vulnerability management, cloud security, identity management, operational technology (OT) security, and cyber exposure management. Which of these areas is seeing the strongest demand in India, and why?

While the overarching demand is for Tenable One, the sharpest spikes in specific demand are in cloud security and AI security. Cloud adoption has been on the rise for years, introducing complexity that makes securing these environments a never-ending battle. AI is deeply embedded and interconnected throughout organizations, and is introducing risk at an unprecedented speed. This has led to an "AI Exposure Gap," a largely invisible form of exposure that emerges across applications, infrastructure, identities, agents and data, and that most security teams are not equipped to manage.

Tenable's key differentiator is delivering a unified platform to see, prioritize and act on all of your exposures. No more looking at risk in a vacuum. Tenable tells you what matters right now and where to focus resources, whether it's in the cloud, an AI environment or anywhere in between.

As AI becomes mainstream, organizations are focused not only on protecting AI systems but also on defending against AI-powered attacks. How is Tenable evolving its offerings to address this emerging threat landscape?

Our strategy addresses both sides of the AI coin: securing AI and defending with AI. With Tenable One, we're equipping organizations with the visibility and insights they need to confidently embrace the transformative potential of AI without compromising security. Tenable One unifies AI protection, discovery and usage governance across the enterprise – including SaaS platforms, cloud services, APIs and agents.

On the other side, attackers are leveraging

AI to accelerate their defenses. The reality is, security teams can't fight AI-powered attackers with manual processes. Tenable Hexa AI, the agentic engine of Tenable One, transforms exposure intelligence into coordinated, automated action, enabling security teams to scale proactive exposure management and proactively defend at machine speed.

Which industries are currently driving cybersecurity investments in India, and are you seeing different priorities emerging across sectors?

While every sector in India is accelerating its cyber investments, investment drivers vary distinctly by sector. Though the underlying need for unified visibility remains constant. In highly regulated spaces like BFSI, investment is heavily defensive, driven by strict compliance mandates and the urgent need to secure identities and consumer financial data. Meanwhile, in manufacturing and healthcare, the game has completely changed due to IT/OT convergence. These industries are highly focused on visibility—discovering legacy physical assets that were never meant to be internet-connected and protecting them from crippling ransomware attacks. India's booming technology sector is prioritizing frictionless, code-to-cloud security that integrates seamlessly into its DevOps pipelines without slowing down innovation.

Many organizations continue to struggle with fragmented security tools and siloed visibility.

How does Tenable help customers move from reactive security operations to a more proactive risk-based approach?

At the core of the Tenable One Exposure Management Platform is the Tenable Exposure Data Fabric, a scalable, cloud-native architecture that ingests, normalizes and connects all exposure data to deliver the most complete view of enterprise risk. In addition to Tenable's native telemetry – IT, AI, cloud, OT, web apps and identity systems – Tenable One ingests data from 330+ partners and custom sources, unifying all security data and enabling customers to see, understand and act on risk all in one place. By proactively identifying, prioritizing and remediating vulnerabilities across the technology stack, organizations can focus efforts on the risks that matter most and reduce risk, rather than chasing potential threats in motion.

India has emerged as a global hub for GCCs, many of which are driving critical digital, cloud, and cybersecurity initiatives for their parent organizations. How do you see the GCC opportunity evolving for Tenable, and what cybersecurity priorities are these organizations focusing on?

India is the nerve center for GCCs globally. For

Tenable, this is a massive strategic opportunity. GCCs are no longer just cost centers; they are tasked with securing multinational, complex infrastructures. The primary focus for GCCs is standardizing global security postures. They need to ensure that their parent organizations maintain consistent, compliant exposure management across borders. GCC leaders are highly focused on code-to-cloud visibility, identity governance, and automated compliance dashboards to meet international regulatory requirements.

GCCs in India have evolved from delivery centers into strategic engines of innovation. How is Tenable leveraging its India operations to drive product innovation, cybersecurity research, and global business outcomes?

Our operations in India play a central role in how we innovate at Tenable. We are actively expanding our R&D capabilities to drive core product developments, particularly in critical areas like cloud security, AI security and AI-powered exposure management. The engineering talent we have built in India shapes how the Tenable One platform evolves to meet the security needs of the modern enterprise in region and across the globe. In addition, feedback and insights from our India-based customers also influence product innovation.

What are your key priorities for Tenable India over the next 12 to 18 months—in terms of market expansion, customer engagement, partner ecosystem development, and talent growth?

Our growth strategy in India is built on three core pillars: Partners, Platform, and Value.

Partner Ecosystem: We've expanded our technology ecosystem partners through Tenable Open Partner Exchange Network (OPEN). This program is designed to help organizations unify security data, accelerate AI-driven workflows and operationalize exposure management across their existing technology stack. In addition, we have a vast network of channel partners that deliver more than simple technology implementation, serving as long-term, strategic security advisors, helping customers build robust exposure management programs.

Platform Innovation: We're deeply committed to R&D and product innovation aimed at delivering a world class exposure management platform designed to meet the customer needs of tomorrow.

Customer Value: We aim to directly address CISO's biggest challenges: highly fragmented security tools, troves of unprioritized data, manual processes that can't keep up with AI-powered attackers. Tenable One is the single source of truth for exposure management, helping organizations proactively reduce risk across the enterprise before attackers strike.

Looking ahead, what will define a cyber-resilient enterprise in the age of AI, and what advice would you offer Indian CIOs and CISOs as they prepare for the next generation of cyber threats?

In the age of AI, cyber resilience hinges on an organization's ability to proactively anticipate and disrupt attack paths before they are exploited. My advice to Indian IT and security leaders is straightforward: shift your thinking from reactive fire fighting to proactive fireproofing.

Exposure management is the way forward. The only way to stop an AI-powered attack is to block all attack paths before an attacker can exploit those weaknesses. Exposure management takes the guesswork out of preemptive security. In a sea of rapidly rising vulnerabilities, exposure management prioritizes exposures based on reachability, exploitability and business impact, unique to your environment.

INTERVIEW

REBUILDING THE DIGITAL CORE: WHY MODERNISATION IS CRITICAL FOR FUTURE-READY ENTERPRISES

Shobhana Lele, CIO, The Bombay Dyeing and Manufacturing Company Ltd, in an exclusive interaction with **Jeevika Srivastava**, discusses the challenges of legacy transformation, the role of cloud and risk management in modernisation journeys, and the emerging technologies that will shape the next generation of enterprise platforms

What are the biggest challenges you face when transitioning from legacy infrastructure to modern digital platforms?

Legacy systems are built with business rules that are not readily available unless and until the organization has very strong documents that define its coding and design. That means that most rules need to be blueprinted and recreated to ensure that the functionality achieves the objectives of the platforms. This often requires extensive collaboration between business users, technology teams, and process owners to identify hidden dependencies and undocumented workflows. In many cases, legacy applications have evolved over years or even decades, making it difficult to fully understand their architecture and operational nuances.

The second challenge is data migration. The data may need a complete transformation before being migrated to modern systems. A number of checks and balances need to be in place to ensure data integrity. Organizations must carefully assess data quality, remove redundancies, standardize formats, and establish validation mechanisms to prevent inconsistencies. Data migration is not just a technical exercise; it is also a business-critical process because inaccurate or incomplete data can impact decision-making and customer experience.

Lastly, one cannot ignore change management. It takes a lot to bring focus on technology upgrades from business teams, which are focused on business deliverables. Employees often need training and guidance to adapt to new platforms and processes. Building stakeholder confidence, communicating the benefits of modernization, and ensuring minimal disruption to daily operations are essential for successful transformation. Ultimately, the transition is as much about people and processes as it is about technology.

In what ways does modernizing core systems accelerate innovation and time-to-market?

Modern core systems provide the agility that are required for innovation and time-to-market. They enable organizations to respond faster to changing business requirements, customer expectations, and market opportunities. With flexible architectures and modern development practices, businesses can introduce new products, services, and features more efficiently than with traditional systems.

Simulations and POCs are much simpler to confirm the requirements and expectations of objectives and output. This allows teams to test ideas quickly, validate assumptions, and reduce the risk associated with large-scale deployments. Faster experimentation encourages innovation because organizations can explore new concepts without committing significant resources upfront.

Lastly, they are easier to maintain, there is enough talent and skill available who bring these skills. Modern platforms benefit from broader ecosystem support, regular updates, and access to a larger pool of skilled professionals. This reduces operational complexity and allows technology teams to focus more on innovation rather than maintaining outdated

Organizations must carefully assess data quality, remove redundancies, standardize formats, and establish validation mechanisms to prevent inconsistencies

infrastructure. As a result, organizations can shorten development cycles, improve collaboration, and significantly enhance their speed of execution.

How are hybrid and multi-cloud strategies enabling scalability and flexibility in your organization?

The very principle of cloud is to bring in the scalability required in operations. Organizations can rapidly scale resources up or down depending on business demand, ensuring optimal performance while controlling costs. This flexibility becomes especially important during seasonal spikes, new product launches, or periods of rapid business growth.

Using hybrid strategies helps us to leverage the clouds as per their USPs. Different cloud providers offer unique strengths in areas such as analytics, AI capabilities, security frameworks, geographic reach, and specialized services. By adopting a hybrid and multi-cloud approach, organizations can align workloads with the most suitable environments and avoid over-dependence on a single provider.

To effectively utilize this strategy, one must consider licenses, is the data of a dynamic or static nature, access frequency, storage media requirements, compute and memory, long-term and short-term roadmaps, etc. Additionally, factors such as compliance requirements, business continuity planning, disaster recovery, and application performance must also be evaluated. A well-designed hybrid and multi-cloud strategy provides organizations with greater resilience, operational efficiency, and the ability to adapt quickly to evolving business needs.

What role does risk management play during large-scale technology transformation?

Risk Management helps organizations take a balanced approach when investing in technology. It ensures that technology decisions are aligned with business objectives while considering potential operational, financial, compliance, and security implications. Effective risk management creates a structured framework for evaluating opportunities and challenges before major investments are made.

Risk Probability and Impact analysis bring out clearly why certain projects can minimize risks in certain cases, justify compliance, regulatory or governance needs vs revenue or productivity related investments. This helps leadership teams understand both the benefits and trade-offs associated with transformation initiatives. It also supports informed decision-making by providing visibility into potential outcomes and mitigation measures.

That way, organizations can also prioritize the initiatives by consciously making decisions. Resources can be allocated more effectively, ensuring that critical projects receive the necessary attention and investment. Finally, having a formal risk management system nudges organizations to think wholistically to identify and build risk mitigation strategies. This proactive approach strengthens resilience, improves stakeholder confidence, and increases the likelihood of successful technology transformation outcomes.

Different cloud providers offer unique strengths in areas such as analytics, AI capabilities, security frameworks, geographic reach, and specialized services

What key trends will shape core system modernization over the next 3–5 years?

Process Automation, AI-led innovations, Security and Governance Frameworks and tools, Blockchain and quantum are the technologies to watch out for in the near future. These trends are expected to redefine how organizations design, operate, and optimize their core systems.

Process automation will continue to streamline operations by reducing manual effort, improving accuracy, and increasing productivity. AI-led innovations will enable smarter decision-making, predictive insights, personalized customer experiences, and enhanced operational efficiency. As AI capabilities mature, organizations will increasingly embed intelligence directly into their business processes and core applications.

Security and Governance Frameworks and tools will become even more critical as digital ecosystems grow more complex and regulatory requirements continue to evolve. Businesses will focus on strengthening cybersecurity, ensuring compliance, and establishing robust governance structures to manage emerging risks.

Blockchain has the potential to enhance transparency, trust, and traceability across various business processes, particularly in areas such as supply chain management, financial transactions, and digital identity. Quantum technologies, although still in the early stages of adoption, could significantly impact computing power, optimization, and cryptography in the years ahead. Together, these advancements will drive the next wave of modernization and help organizations build more intelligent, secure, and future-ready digital foundations. ■

jeevika@thefoundermedia.in

INTERVIEW

FROM EFFICIENCY TO INTELLIGENCE: THE NEXT EVOLUTION OF ENTERPRISE TECHNOLOGY

Manoj Kumar, CIO, Shyam Steel Industries Ltd, in conversation with **Jeevika Srivastava** explores how organizations can prepare for an intelligent and autonomous future while maintaining accountability, ethical oversight, and strategic control.

Having witnessed multiple waves of technological change throughout your career, where do you see the current AI revolution differing from previous transformations, and what excites you most about its potential?

Over the last 25 years, I have witnessed several major technology shifts, from ERP and enterprise digitization to cloud computing, mobility, and cybersecurity. What makes the AI revolution fundamentally different is its ability to augment human intelligence rather than just automate processes. Unlike previous transformations that primarily improved efficiency, AI has the potential to enhance decision-making, innovation, and business outcomes at an unprecedented scale.

What excites me most is AI's ability to democratize knowledge, accelerate problem-solving, and create new opportunities across every function of an organization. For CIOs, it is not just a technology upgrade; it is a strategic enabler that can redefine how businesses operate, compete, and deliver value in the digital era.

The impact of AI extends beyond technology departments and is rapidly becoming a boardroom-level priority. Organizations are increasingly exploring how AI can improve customer experiences, optimize operations, and uncover new business models. Unlike previous technology shifts that required significant process redesign before benefits could be realized, AI has the ability to generate value across multiple business functions simultaneously. This broad applicability is accelerating adoption and making AI one of the most transformative technologies enterprises have encountered in recent decades.

Autonomous systems are increasingly being trusted with decision-making and execution. In your view, what are the key business processes that are ready for this shift, and where should human judgment continue to play a central role?

Autonomous systems are best suited for repetitive, data-driven, and rule-based processes such as IT operations, cybersecurity monitoring, supply chain optimization, predictive maintenance, customer service, and financial processing. In these areas, AI can improve speed, accuracy, and efficiency while reducing operational risks.

However, human judgment must remain central to strategic decision-making, risk management, governance, ethics, crisis response, and people-related decisions. While AI can provide valuable insights and recommendations, it cannot fully replicate human qualities such as contextual understanding, empathy, creativity, and ethical reasoning.

The future lies in human-AI collaboration, where autonomous systems handle routine execution and humans focus on strategy, innovation, and leadership. Organizations that achieve this balance will realize the greatest business value while maintaining trust and accountability.

As autonomous systems continue to mature, organizations will need to establish clear frameworks that define the boundaries between machine-driven execution and human oversight. Success will depend on ensuring transparency, accountability,

and governance throughout the decision-making process. Businesses that thoughtfully integrate autonomous technologies into their operations will be able to improve productivity while maintaining the trust of customers, employees, and stakeholders.

Many organizations are still working to unlock value from data and automation. What foundational capabilities should enterprises build today to prepare for a more intelligent and autonomous future?

To prepare for a more intelligent and autonomous future, organizations must first establish a strong digital foundation. This includes high-quality and governed data, scalable cloud infrastructure, robust cybersecurity, and integrated enterprise platforms that enable seamless data flow across the organization.

Equally important is building AI and analytics capabilities, strengthening data governance frameworks, and ensuring responsible AI practices. Organizations should also invest in workforce upskilling so employees can effectively collaborate with AI-driven systems.

Ultimately, enterprises that focus on data quality, digital agility, security, and a culture of continuous learning will be best positioned to unlock the full value of AI, automation, and future autonomous technologies.

Building foundational capabilities is not a one-time initiative but an ongoing journey. Organizations must continuously modernize their technology landscape, improve data quality standards, and strengthen governance practices to keep pace with evolving business needs. A strong foundation enables enterprises to scale innovation confidently, reduce complexity, and ensure that future AI-driven initiatives can deliver sustainable and measurable outcomes.

Technology adoption often comes with cultural and organizational challenges. From your experience,

how can leaders foster trust and readiness among employees as AI becomes a more active participant in day-to-day operations?

Successful AI adoption is as much about people as it is about technology. Leaders must create trust through transparent communication, clearly explaining how AI will augment employees' capabilities rather than replace them. Employees need to understand the purpose, benefits, and expected outcomes of AI initiatives.

Organizations should also invest in continuous learning and upskilling programs to help employees confidently work alongside AI-powered tools. Involving teams early in the transformation journey, encouraging experimentation, and celebrating success stories can significantly improve adoption.

Most importantly, leaders must establish clear governance and ethical guidelines for AI use. When employees see AI being implemented responsibly and as a tool to enhance productivity and decision-making, they are more likely to embrace it as a valuable partner rather than view it as a threat.

Trust is built when employees feel empowered rather than threatened by technological change. Creating an environment where people can learn, experiment, and adapt without fear is critical for successful transformation. Leaders who actively engage with employees, address concerns openly, and demonstrate the practical benefits of AI can accelerate adoption while fostering a culture of innovation and collaboration across the organization.

A strong foundation of data quality, governance, security, and scalability is equally critical for long-term success

As AI capabilities continue to evolve at an unprecedented pace, what advice would you give to technology leaders who are trying to distinguish between short-term hype and innovations that can create long-term strategic value?

My advice to technology leaders is to focus on business outcomes rather than technology trends. Every new AI innovation should be evaluated based on its ability to solve real business problems, improve efficiency, enhance customer experience, reduce risk, or create new revenue opportunities.

While experimentation is important, organizations should avoid pursuing AI initiatives simply because they are popular. Instead, prioritize use cases that align with strategic business objectives and deliver measurable value. A strong foundation of data quality, governance, security, and scalability is equally critical for long-term success.

Technology trends will continue to evolve, but the innovations that create lasting value are those that address genuine business needs, can be scaled across the enterprise, and contribute to sustainable competitive advantage. Leaders who balance innovation with business discipline will be best positioned to separate lasting transformation from short-term hype.

Technology leaders should also recognize that successful innovation requires patience and long-term commitment. While emerging technologies often generate significant excitement, their true value is realized only when they are integrated into business processes and supported by the right operating models. By maintaining a disciplined approach to evaluation and execution, organizations can maximize returns on innovation investments while avoiding unnecessary risks associated with short-lived trends.■

jeevika@thefoundermedia.in

INTERVIEW

THE NEW BLUEPRINT FOR TECHNOLOGY-DRIVEN ENTERPRISES

In this insightful interaction, **Chitti Babu Atreyapurapu, Group CIO, Aurobindo Pharma Ltd.**, discusses with **Jeevika Srivastava** the leadership lessons that have shaped his career, the growing impact of AI across enterprise functions, the importance of building a strong data culture

Having spent decades leading technology initiatives across industries, what has been the most valuable leadership lesson you've learned about driving change in large and complex organizations?

The most defining lesson I have learned is that sustainable transformation is never a technological challenge; it is fundamentally , predominantly a cultural and alignment challenge. In large enterprises, it is remarkably easy for initiatives to get accepted by fragmented across depaartmental silos.

True transformation requires leaders to anchor every technological roadmap in a clear, shared vision, defining the comprehensive "why" before engineering the "how." When teams across disparate functions understand how a new system serves a unified corporate purpose, resistance drops significantly. This is what I have learned practically.

Beyond vision, change must be anchored in the people executing it daily, rather than being imposed as a top-down mandate. Sometime top-down mandate also works. Empowering frontline teams to co-design workflows transforms the narrative from "mandatory process changes" to "organic operational improvement."

Finally, leaders must build psychological safety by practicing transparency through both milestones and setbacks, while systematically celebrating incremental wins.

AI is rapidly moving from experimentation to enterprise adoption. Which business functions do you believe will see the greatest transformation from AI in the next three to five years, and why?

While AI will impact the entire corporate landscape, the most profound mid-term structural shifts will occur within operational and quality data-heavy environments.

In Supply Chain and Logistics, the shift from reactive execution to predictive orchestration is revolutionary. By leveraging AI and ML for real-time monitoring and autonomous routing, enterprises can mitigate global volatility and minimize asset downtime. Similarly, Product Development and R&D are expected to experience compressed timelines especially in the areas of document intelligence and laboratory testing. AI/ML will be helpful in Drug Discovery provided unified bio-data bank is available in India. Furthermore, operational backbone functions like Finance, Risk, and Human Resources are moving toward hyper-efficiency. AI compresses financial decision cycles through real-time anomaly detection and dynamic risk scoring, while transforming HR from an administrative function into a predictive talent platform, optimizing retention and mitigating bias in career progression.

The pharmaceutical sector depends on precision, quality, and compliance. How can technology leaders foster innovation while ensuring these critical standards remain uncompromised?

In the pharmaceutical sector, innovation and compliance are often viewed as opposing forces. However, a modern technology leader must view them as symbiotic. The key is moving away from retrospective quality assurance and

By running parallel "innovation" and "compliance" squads that continuously cross-review outputs (Human in the Loop), breakthroughs are vetted rigorously without stalling developmental momentum

shifting toward a "compliance-by-design" architecture. This can be achieved by embedding regulatory compliance directly into core technology stacks, utilizing advanced Laboratory Information Management Systems (LIMS), electronic batch records, and immutable ledgers to guarantee absolute data integrity from raw material to the final product. This is what any regulatory auditor looks into.

To maintain velocity, organizations should implement a dual-track operating model. By running parallel "innovation" and "compliance" squads that continuously cross-review outputs (Human in the Loop), breakthroughs are vetted rigorously without stalling developmental momentum. Furthermore, by feeding historical audit points and deviations back into predictive quality models, automated learning loops can be built that flag potential anomalies on the factory floor before they escalate into regulatory challenges.

As organizations become increasingly data-driven, what steps should they take to build a culture where employees at all levels are empowered to make better decisions using data?

Along with AI Governance, Data governance is most critical now every organization should concentrate. Building a data-empowered culture requires moving past the concept of data as an IT asset and treating it as a core organizational capability. Governance framework must secure corporate assets through clear ownership and rigorous data quality metrics

Once governance is established, organizations must democratize access. Providing intuitive, self-service analytics tools and centralized dashboards allows business units to independent extract insights without relying heavily on technical teams. However, access without literacy breeds misinterpretation. Companies must invest in role-specific data literacy programs that teach teams how to critically evaluate sources and practice meaningful data storytelling.

Ultimately, culture follows accountability. Leaders must formalize data metrics as a prerequisite for capital allocations, project kick-offs, and executive reviews, while actively recognizing and rewarding teams that successfully leverage data to eliminate operational waste or unlock new revenue streams.

Looking ahead, what emerging technology or industry trend do you believe is currently underestimated but has the potential to significantly reshape businesses in the coming decade?

While the corporate world remains heavily focused on the immediate horizons of generative AI, Quantum Computing for Optimization and Materials Discovery represents a profoundly underestimated paradigm shift with massive, decade-long implications. Because quantum hardware is still in its nascent stages, many leaders dismiss it as a distant milestone. This is a strategic oversight. Quantum algorithms possess the unique capability to compute extremely complex combinatorial optimization problems exponentially faster than classical supercomputers.

In highly complex or regulated spaces like pharmaceuticals, this creates an extraordinary competitive advantage. Quantum systems can compress the timeline for molecular simulation and initial drug discovery from years down to mere weeks (Possibility). Enterprises that wait for the hardware to fully mature before building hybrid classical-quantum data pipelines, cultivating talent, or participating in early software ecosystems will find themselves at disadvantage against who are quantum-ready today.■

jeevika@thefoundermedia.in

INTERVIEW

AI LITERACY IS THE NEW WORKFORCE ESSENTIAL

Arun Attri, CDIO, Wonder Cement Ltd., speaks with **Aishwarya Saxena** on why technology transformations succeed through people and value, and how Agentic AI is reshaping enterprise infrastructure strategy

Technology transformations often fail because of organizational resistance rather than technical limitations. What approaches have proven most effective in driving adoption and cultural change?

Technology transformations often fail due to organizational resistance rather than technical gaps. What works best in driving adoption and cultural change is a strong focus on people and value. At Wonder Cement, we start by clearly linking every digital initiative to measurable business outcomes such as productivity, cost optimization, profit maximization or customer experience, ensuring teams understand the "why."

We emphasize co-creation, engaging business teams & relevant stake holders early, so solutions are built with users, not for them. Pilot led deployments that demonstrate quick wins help build trust and momentum, while structured capability building programs remove fear and improve confidence. Sustained adoption is then driven through governance mechanisms, leadership sponsorship, and aligning performance metrics with digital usage. Ultimately, successful transformation is less about enforcing change and more about building ownership and belief.

With industry rapidly switching towards Agentic AI systems, in your opinion how are CIOs rethinking infrastructure strategies to support AI workloads, particularly around GPUs, edge computing, hybrid cloud environments, and data sovereignty requirements?

With the rise of Agentic AI, CIOs are rethinking infrastructure strategies from a compute centric to a workload centric approach. AI is no longer just about GPU scaling; it requires a balanced architecture where CPUs, GPUs, and specialized accelerators work together, with CPUs increasingly orchestrating complex agentic workflows. Organizations are moving toward hybrid models that combine cloud, on-premises, and edge computing to optimize latency, cost, and resilience. Edge computing is gaining prominence for real-time industrial use cases, while robust data platforms are becoming critical to manage data flow, governance, and AI economics.

Additionally, evolving data sovereignty requirements are pushing enterprises toward localized processing and stricter governance. The future is not 'cloud-first' but 'right-workload-on-right-platform,' enabling scalable and secure AI adoption.

Cement logistics involve complex coordination between plants, grinding units, and distribution. How has real-time data changed decision-making in your company's supply chain?

In the cement industry, real-time data has fundamentally transformed supply chain decision making from reactive to predictive. At Wonder Cement, integrating production, inventory, dispatch, and logistics data into a unified view has enabled end-to-end visibility across plants, grinding units, and distribution networks. This allows dynamic decision making, such as optimizing dispatch planning, balancing inventory across locations, and proactively managing fleet movements. Real-time


We emphasize co-creation, engaging business teams & relevant stake holders early, so solutions are built with users, not for them

tracking enhances delivery reliability and customer transparency, while digital workflows accelerate financial processes like invoicing and reconciliation. The result is a supply chain that not only improves service levels but also drives significant cost efficiencies, turning logistics into a strategic lever rather than just an operational necessity.

With operations spanning multiple grinding units across Rajasthan, Maharashtra, Madhya Pradesh, Haryana, Uttar Pradesh, and Gujarat, how do you ensure consistent digital adoption and data standards across geographically dispersed sites?

Ensuring consistent digital adoption and data standards across geographically dispersed operations requires a strong foundation of governance and standardization. We follow an enterprise-wide model where core systems, data definitions, and processes are standardized, while execution remains locally adaptable. Unified platforms such as ERP, CRM, IBPS/SCM, Data Lake and Analytics Systems etc. ensure a single source of truth, supported by clearly defined data ownership and quality standards. Implementations are typically executed through a "pilot-and-scale" approach, where successful deployments are templated and replicated across sites. Continuous monitoring through adoption metrics and governance reviews ensures alignment is sustained. This disciplined approach allows us to operate as a digitally integrated enterprise despite geographical diversity.

At Wonder Cement, integrating production, inventory, dispatch, and logistics data into a unified view has enabled end-to-end visibility across plants, grinding units, and distribution networks

What skills do you believe will become most critical in technology organizations over the next five years, and how are you preparing teams for an AI-first operating model?

Looking ahead, the most critical skills in technology organizations will combine deep technical expertise with business and cognitive capabilities. Skills in AI/ML, Data Engineering, Cloud and Edge Architectures, and Cybersecurity will be essential, but equally important will be system thinking, problem framing, and human-AI collaboration.

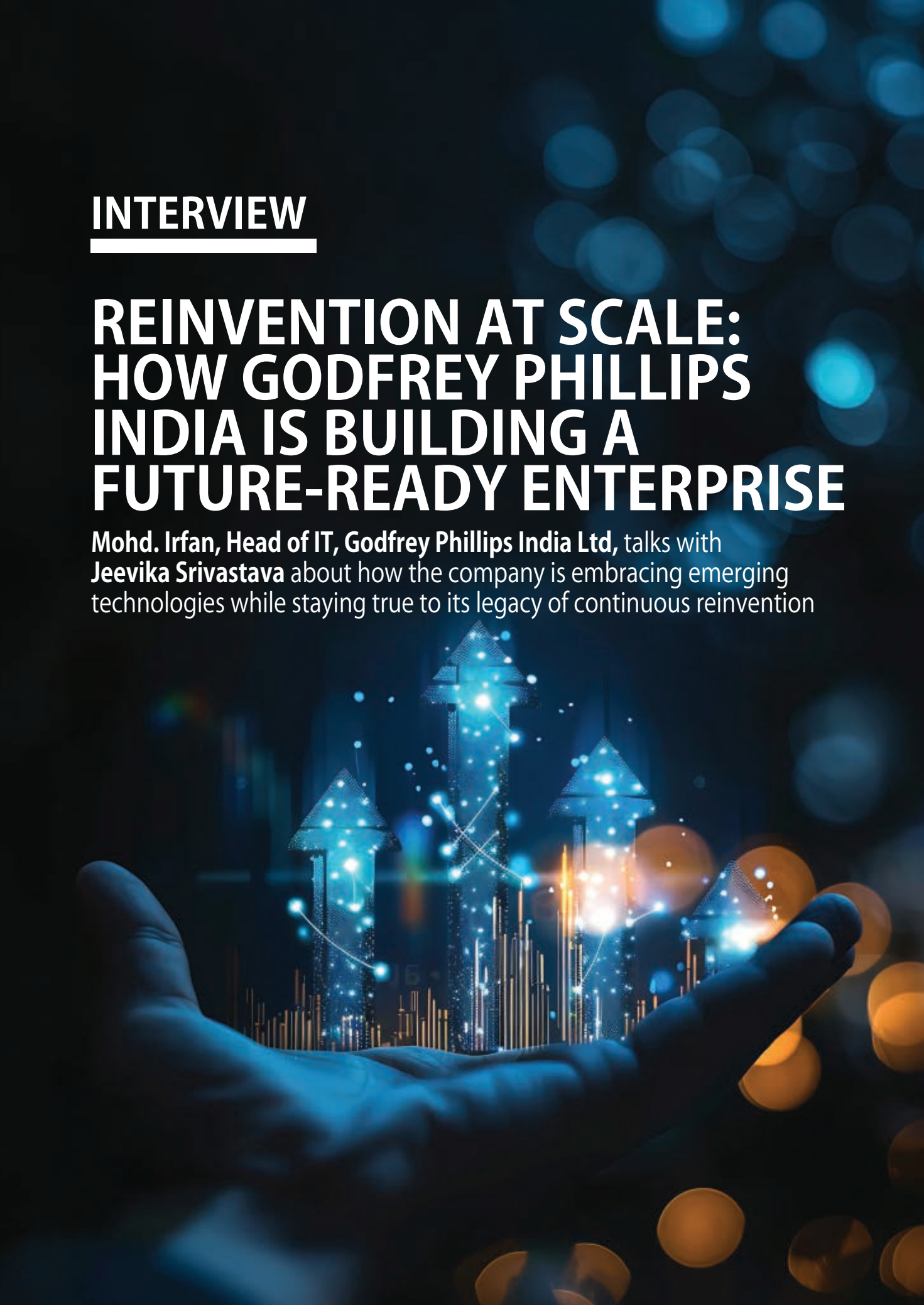
At Wonder Cement, we are preparing for this shift through structured AI literacy programs across roles, role-based capability frameworks, and cross-functional exposure between IT and operations. We prioritize upskilling internal talent to build institutional knowledge, while fostering a culture of continuous learning and experimentation. As AI becomes embedded in operations, the focus will shift from task execution to intelligent orchestration, where technology teams design, govern, and continuously optimize human-machine collaboration.■

editor@thefoundermedia.com

INTERVIEW

REINVENTION AT SCALE: HOW GODFREY PHILLIPS INDIA IS BUILDING A FUTURE-READY ENTERPRISE

Mohd. Irfan, Head of IT, Godfrey Phillips India Ltd, talks with **Jeevika Srivastava** about how the company is embracing emerging technologies while staying true to its legacy of continuous reinvention



Godfrey Phillips India has a rich legacy, yet it continues to embrace new technologies and ways of working. How do you view innovation in the context of such a well-established organisation?

One of the philosophies that continues to inspire us comes from our founder, KK Modi, who firmly believed that "to stagnate is to die." He often spoke about the importance of constantly learning, evolving, and adopting ideas from the best minds and institutions around the world. That mindset remains deeply embedded in GPI's DNA even today.

Innovation, for us, is about continuously reinventing ourselves while staying true to our values. Under the leadership of our Chairperson and Managing Director, Dr. Bina Modi, we have continued to invest in technology, sustainability, people, and operational excellence to build a resilient and future-ready organisation. From cloud-first architecture and advanced analytics to cybersecurity, intelligent automation, and AI readiness, technology today is helping us become more agile, data-driven, and responsive. We actively learn from peers, technology partners, and global best practices, and as we continue to evolve, we also hope to contribute back to the ecosystem by sharing our own experiences and learnings. That's how innovation sustains itself.

AI is reshaping every industry. How is GPI preparing for an AI-driven future?

Long before AI was the buzzword, our CMD, Dr. Bina Modi, and CEO and Whole-Time Director, Sharad Aggarwal, had a keen interest and understanding of its potential to change businesses for better. The conversation around AI has rapidly moved from experimentation to enterprise value creation. Our approach has been to focus first on building strong digital foundations before scaling AI-led innovation.

Over the last few years, we have invested heavily in cloud infrastructure, data governance, analytics capabilities, and integration frameworks. These foundational investments are creating an AI-ready enterprise where data is structured, accessible, and usable at scale.

We have already begun introducing Generative AI capabilities within controlled enterprise environments and are actively evaluating opportunities across forecasting, knowledge management, employee productivity, cybersecurity, and intelligent automation.

At the same time, responsible AI remains a critical priority. Governance, privacy, security, and ethical use are integral to our AI strategy. The future belongs to organisations that can combine innovation with trust, and that is exactly the balance we are working to achieve.

Employee experience is increasingly becoming a key pillar of digital transformation. How is GPI leveraging technology to empower its people?

Our core value is People-First. So, any digital transformation at GPI can only be truly successful when it improves the experience of the people using it. Technology should simplify work, remove friction, and help employees focus on what matters most.

One of our most impactful

The transformation involved consolidating systems, standardising data, automating workflows, and creating a unified platform accessible across locations

initiatives in this area has been the rollout of MyHR, our integrated digital HR platform built on Oracle Fusion. Developed in close partnership with our CHRO, Sakshi Anand, the initiative was designed to create a seamless and intuitive employee experience across multiple HR processes. Leveraging a globally recognised cloud-based HR platform has enabled us to build a solution that is not only robust and scalable, but also continuously evolving through regular enhancements and new capabilities.

The transformation involved consolidating systems, standardising data, automating workflows, and creating a unified platform accessible across locations. Employees today have greater visibility, transparency, and control over key HR services, while managers benefit from faster access to insights, analytics, and decision-support tools. The platform's cloud-native architecture also ensures that we can continuously introduce new features and innovations without disrupting the user experience.

Beyond efficiency gains, MyHR represents something larger. It reflects our commitment to building a workplace where technology empowers people, strengthens engagement, and supports the OneGPI culture that connects employees across the organisation. As the platform continues to evolve, it will play an increasingly important role in creating a more connected, agile, and employee-centric workplace.

Cybersecurity has become a boardroom priority. How are you securing an increasingly digital enterprise?

Cybersecurity today is a business resilience discussion. As our digital footprint expands, we continue to strengthen our security posture through a comprehensive zero-trust architecture, where every user, device, and application is continuously authenticated and validated before access is granted. This is supported by

advanced threat monitoring, AI-powered detection capabilities, identity governance controls, vulnerability management programs, and continuous security assessments. Our objective is to move from reactive defence to proactive risk management.

Equally important is the human dimension. We conduct regular awareness programs, phishing simulations, and security training sessions to ensure cybersecurity becomes part of everyday behaviour across the organisation. Technology, processes, and people must work together. When those three elements align, organisations become significantly more resilient against emerging threats.

Technology is evolving faster than ever. How do you ensure GPI stays ahead of the curve while remaining grounded in practical business value?

One of the realities of modern technology leadership is that technology is evolving faster than any single organisation can predict. Staying ahead therefore requires a combination of continuous learning, strong partnerships, and a willingness to adapt.

At GPI, we place significant emphasis on capability building across the organisation. Our IT teams regularly participate in certification programs, technology workshops, partner-led training sessions, and knowledge-sharing forums to stay abreast of developments in areas such as cloud computing, cybersecurity, AI, analytics, and enterprise applications. Equally important, we invest in digital literacy and awareness programs for employees across functions, ensuring that new tools and technologies are understood, adopted, and used effectively. Whether it is cybersecurity awareness, AI-enabled productivity tools, or new digital platforms, continuous learning has become an integral part of our culture. We also actively engage with technology partners, industry peers, cloud providers, and cybersecurity specialists to understand emerging trends and best practices. These interactions often provide valuable insights into how technology can solve business challenges in new and innovative ways. At the same time, every technology decision must ultimately create measurable business value. We evaluate initiatives through the lens of business outcomes, employee experience, operational efficiency, risk reduction, and long-term scalability. The goal is not to adopt technology because it is new. The goal is to adopt technology because it solves a real problem, creates meaningful impact, and helps the organisation move forward.

Looking ahead, what will define the next chapter of GPI's digital journey?

Dr. Bina Modi, has consistently championed the role of technology as a catalyst for business growth and organisational agility. Her belief that technology should drive smarter decisions, faster execution, and stronger collaboration aligns closely with our vision for the future.

Over the next five years, I expect AI, advanced analytics, intelligent automation, connected operations, and predictive decision-making to become deeply embedded across the organisation. Technology will increasingly move beyond enabling processes to actively shaping business strategy.

We are building towards a future where data flows seamlessly across functions, decisions are powered by real-time intelligence, and employees have access to smarter digital tools that enhance productivity and innovation. Our aspiration is not simply to become more digital. It is to become more intelligent, connected, and adaptive as an enterprise. Technology will continue to be the thread that brings together our people, processes, and ambitions, helping us create sustainable value in an increasingly dynamic world.■

jeevika@thefoundermedia.in

FEATURE

CYBERSECURITY IN THE AGE OF AI: NAVIGATING A WORLD WITHOUT BOUNDARIES

As enterprises become increasingly AI-driven and distributed, traditional security boundaries are disappearing, making AI-driven cybersecurity central to enterprise resilience and trust.

- **Balaka Baruah Aggarwal**, Consulting Editor, Bharat Network Group

The modern enterprise is no longer confined to office walls, corporate networks or centralized data centers. Businesses today operate in a connected ecosystem where employees work remotely, applications run across multi-cloud environments, AI systems make autonomous decisions, and data flows seamlessly between platforms, partners, customers, and intelligent agents. While this transformation has accelerated innovation and operational efficiency, it has also created extremely complex environments for organizations to design and manage security and defence strategies.

Artificial intelligence has fundamentally altered the cyber threat landscape. Global cyber attacks have reached an all time high, averaging 2090 incidents weekly and costing the organization an average of US4.88 million per breach. Needless to say, AI-powered phishing has been a primary tool for ingression, along with supply chain compromises and exploitation of third-party vendors.

While AI is helping organizations automate workflows, strengthen threat detection, and improve business decision-making, AI is also enabling cybercriminals to launch faster, smarter, and more sophisticated attacks at unprecedented scale. Enterprises are now confronting a future where cybersecurity is no longer about defending systems from hackers; it is about protecting a borderless digital enterprise in which AI has become both an enabler and a threat vector.

Industry experts believe that traditional cybersecurity models are rapidly becoming obsolete. Avinash Tiwari, CISO and Head IT at Pidilite Industries, believes the biggest shift organizations must recognize is that the traditional security perimeter has effectively disappeared. “Today, security is shaped by identity, data, and continuous authorization rather than a fixed network boundary,” he observed. “Organizations must move from protecting a physical perimeter to securing every access request, wherever the user, device, or AI agent may be.”

This changing reality is forcing enterprises to rethink not just security technologies, but the

entire approach toward governance, trust, infrastructure, and digital operations.

AI Has Become the New Cyber Weapon

The rise of generative AI has dramatically increased the sophistication of cyberattacks. AI-driven phishing campaigns can now generate highly personalized emails that mimic executive communication styles, organizational hierarchies, and employee behavior patterns. Deepfake technologies can convincingly clone voices and videos to impersonate senior leaders. Autonomous malware can adapt dynamically to bypass conventional security tools.

Cybersecurity professionals warn that attackers are now operating at machine speed. "The primary risks stem from rapidly expanding attack surfaces, undocumented shadow AI usage, and compromised credentials across fragmented multi-cloud environments," said Avinash Tiwari. "Without centralized visibility and continuous exposure management, these vulnerabilities invite rapid, machine-speed exploitation."

This marks a significant shift from traditional cyber threats. Earlier attacks largely targeted networks, endpoints, or applications. Modern attacks increasingly target AI systems themselves through techniques such as model poisoning, prompt injection, and data manipulation. AI-powered attackers can automate reconnaissance, generate malicious code faster, and execute hyper-personalized social engineering attacks at a scale previously unimaginable.

"The primary risks stem from rapidly expanding attack surfaces, undocumented shadow AI usage, and compromised credentials across fragmented multi-cloud environments. Without centralized visibility and continuous exposure management, these vulnerabilities invite rapid, machine-speed exploitation."

AVINASH TIWARI
CISO AND HEAD IT
PIDILITE INDUSTRIES

The challenge is compounded by the fact that AI adoption inside enterprises is accelerating rapidly. AI is no longer an experimental technology being tested in isolated environments. It is increasingly embedded into enterprise applications, manufacturing systems, analytics platforms, financial operations, customer engagement systems, and workplace productivity tools.

"AI is already embedded everywhere. The experimentation is over and the results are there for organizations that are ready to adopt it," noted Naresh Kumar Pathak, Vice President IT and CDIO, Dampur Bioorganic Limited. "The question is not whether AI works, but how quickly organizations can adopt it meaningfully and derive measurable value."

But while organizations are aggressively deploying AI to improve productivity and innovation, governance frameworks often lag behind deployment. This gap is becoming one of the most significant risks for enterprise while deploying AI.

The Borderless Enterprise Has Expanded the Attack Surface

The widespread

adoption of remote work, cloud platforms, SaaS applications, AI copilots, and distributed digital ecosystems has fundamentally changed the nature of enterprise security. Organizations are no longer protecting a centralized infrastructure. They are defending a constantly shifting digital ecosystem spanning employees, devices, APIs, cloud workloads, third-party applications, and autonomous AI systems.

According to Avinash Tiwari, enterprises are now confronting a dual challenge where AI is simultaneously reshaping cyber defense and cyber threats. "AI is a double-edged sword," he explained. "Threat actors use it to launch autonomous attacks and hyper-personalized phishing, while defenders must leverage it for real-time threat hunting and automated remediation."

Harish Arora, CISO and Data Protection Officer at Singhi and Co adds, "AI is a double-edged sword. If we use it ethically, it can help us enormously. If not, it can hurt us."

Arora adds that many organizations are still unprepared for the scale and speed of this transformation. Enterprises now require AI-augmented security platforms capable of responding in real time to threats that evolve dynamically.

"The AI conversation has fundamentally shifted. The question is no longer whether AI works, but how quickly organizations can move from experimentation to meaningful adoption. As AI becomes embedded across enterprise applications, operations, and decision-making, success will depend on an organization's ability to balance innovation, governance, and measurable business outcomes."

NARESH KUMAR PATHAK
VP IT AND CDIO
DAMPUR BIOORGANIC LTD.

Traditional perimeter-based security frameworks are proving inadequate because attackers no longer need to breach corporate networks physically. Compromised identities, unsecured APIs, poorly governed AI models, and vulnerable cloud configurations now offer multiple entry points into enterprise systems.

This has accelerated the shift toward Zero Trust architectures where organizations continuously verify users, devices, workloads, and AI agents before granting access.

A modern Zero Trust architecture moves beyond basic network segmentation to dynamic trust verification and continuous anomaly detection at every transaction level. "A modern Zero Trust architecture assumes a breach by default," Tiwari explained. "It requires stringent, contextual authentication for both human users and AI workloads before granting least-privilege access." The emphasis is no longer on trusting users because they are inside the network, because now trust must be continuously validated.

AI Is Also Becoming the Defender

Ironically, the same technology making cyberattacks more dangerous is also becoming the enterprise's most powerful defense mechanism.

Organizations are increasingly deploying

AI-powered Security Operations Centers (SOCs) capable of monitoring massive volumes of telemetry data generated across cloud systems, firewalls, endpoints, applications, and networks. AI-driven systems can identify anomalies, detect zero-day attacks, correlate threats across environments, reduce false positives, and automate incident response far faster than human analysts.

Arora emphasized that if AI is used responsibly and ethically, it can significantly strengthen cybersecurity operations and improve enterprise resilience. Experts believe the next phase of cybersecurity will increasingly revolve around Agentic AI — autonomous AI systems capable of independently monitoring, analyzing, and responding to threats in real time. These systems can process enormous volumes of security data continuously and adapt to emerging attack patterns without waiting for manual intervention.

But this growing reliance on AI also raises concerns around governance, accountability, and ethical implementation. Organizations are now realizing that AI systems themselves must be governed carefully because vulnerabilities within AI can quickly become enterprise-wide risks.

"One of the most overlooked cybersecurity risks is the growing tendency of employees to adopt AI tools without fully understanding its security implications. Convenience is becoming one of the biggest drivers of AI adoption. Employees routinely use AI-powered note-taking tools during Zoom or Teams meetings. But very few stop to ask where that information is being stored, how it is being processed, or who may ultimately have access to it."

SUBROTO KUMAR PANDA
CIO
ANAND AND ANAND

The Hidden Risks Inside Everyday AI Usage

As organizations rapidly embrace AI tools to improve speed, collaboration, and efficiency, the boundary between productivity and risk is becoming blurred. What appears to be a harmless attempt to automate routine work — summarizing meetings, generating reports, analyzing documents, or querying enterprise data — can inadvertently expose sensitive information beyond the organization's control. Often, adoption of AI tools is outpacing governance frameworks, security awareness, and policy enforcement, creating new blind spots for CISOs and IT leaders.

One of the most underestimated cybersecurity risks today comes from employees themselves. The widespread use of AI-powered note-taking tools, collaboration assistants, public generative AI models, and AI-driven productivity applications has created a new category of enterprise exposure. Employees often upload confidential business information into AI systems without fully understanding where the data is being stored, processed, or reused.

Subroto Kumar Panda, CIO at Anand and Anand, warned that convenience is driving risky AI adoption behaviors inside enterprises.

"People use AI note-takers during Zoom or Teams meetings because it is convenient," he said. "But nobody asks where that confidential information is being stored and who has access to it."

For industries handling sensitive legal, financial, healthcare, or intellectual property data, these risks are particularly severe. Many enterprises are increasingly exploring private AI ecosystems and closed AI environments trained only on proprietary datasets to ward of security vulnerabilities. "The opponent counsel could use the same public AI model that we use," Panda explained while discussing legal sector concerns. "That is why we are extremely cautious."

The age of AI has transformed data governance from a compliance issue into a strategic cybersecurity priority.

Healthcare Illustrates the Complexity of AI Security

The promise of AI is compelling across every industry, but nowhere are the stakes higher than in sectors where data sensitivity, regulatory compliance, and human outcomes intersect. Few sectors demonstrate the challenges of AI governance more clearly than healthcare. The cost of breach in the healthcare industry is the highest with an average breach pegged at USD 12.5 million, according to industry estimates.

"AI is a double-edged sword. If we use it ethically, it can help enormously. If not, it can hurt us. Many organizations are still unprepared for the scale and speed of this transformation. Enterprises now require AI-augmented security platforms capable of responding in real time to threats that evolve dynamically."

HARISH ARORA
CISO AND DATA PROTECTION OFFICER
SINGHI AND CO

Sushil Kumar Meher, Head IT and CISO at AIIMS, believes organizations must approach AI adoption with extreme caution because AI systems directly impact patient privacy, ethical accountability, and healthcare outcomes.

"Blindly using AI models in the organization is very dangerous," he warned. Healthcare organizations operate in hybrid environments where manual and digital systems coexist, making governance significantly more complex. At the same time, AI systems processing sensitive patient information become highly attractive targets for attackers.

Meher also highlighted emerging risks such as model poisoning and data poisoning, where attackers manipulate AI systems themselves rather than simply stealing data. These attacks could potentially compromise clinical decisions, patient diagnosis, or healthcare operations.

His observations underline a larger enterprise reality: cybersecurity in the age of AI is not just about protecting infrastructure anymore. It is about protecting trust, data integrity, ethical governance, and AI accountability.

Critical Infrastructure Is Becoming a Cybersecurity Battleground

The rise of AI is also transforming operational environments such as smart cities, transportation networks, telecom operations, utilities, and command centers.

Sharun Seth, Assistant General Manager, Government Vertical, India

"Today's control rooms are mission-critical environments where cybersecurity and operational resilience are inseparable. As AI strengthens threat detection, it is also helping attackers scale and automate cyber threats. This makes security-by-design—through zero-trust architectures, strong access controls, encryption, and continuous monitoring—a business imperative rather than a technology choice."

SHARUN SETH
ASSISTANT GENERAL MANAGER, GOVERNMENT VERTICAL, INDIA & NEPAL
BARCO CONTROL ROOMS

and Nepal at Barco Control Room, explained that control rooms today are no longer passive display environments. They have evolved into mission-critical operational centers where cybersecurity and operational resilience are inseparable.

Organizations across government, defense, transportation, utilities, and enterprise operations increasingly depend on secure, real-time visualization and monitoring systems. These environments require highly secure architectures capable of supporting continuous operations while defending against sophisticated cyber threats.

Seth emphasized that modern control room environments are now being built around security-by-design principles including zero-trust architecture, multi-factor authentication, end-to-end TLS encryption, role-based access controls, and real-time monitoring systems.

He also pointed out how AI is simultaneously enabling predictive threat monitoring while helping attackers automate phishing campaigns, generate malicious code faster, and exploit vulnerabilities more effectively.

"Cybersecurity can no longer be treated as an afterthought or an add-on feature," Seth stressed. "Modern enterprise infrastructure must be built with security embedded

into the architecture from the outset."

Data Privacy Is Now a Boardroom Imperative

As cyber risks intensify, data privacy is rapidly moving beyond IT departments into corporate boardrooms. Regulations such as India's Digital Personal Data Protection (DPDP) Act are significantly increasing accountability for enterprises that fail to protect customer data. Organizations now face the risk of substantial penalties, reputational damage, and regulatory scrutiny.

"Data privacy or data protection is not an IT function anymore," said Harish Arora. "It has become a board-level accountability."

This growing accountability is forcing enterprises to adopt "privacy by design" strategies where governance, security controls, compliance frameworks, and AI guardrails are embedded directly into systems from the beginning rather than added later.

Avinash Tiwari believes AI governance must become the starting point for enterprise cybersecurity modernization. "You cannot effectively modernize your security posture to defend a borderless enterprise without first defining the rules, guardrails, and compliance standards that govern how AI is safely consumed and deployed," he noted.

"AI can significantly improve healthcare outcomes, but its adoption must be guided by strong governance and oversight. Healthcare organizations manage highly sensitive patient data, and emerging threats such as data poisoning and model manipulation are critical concerns. As AI becomes embedded in healthcare workflows, organizations must focus not only on cybersecurity, but also on ensuring data integrity, ethical accountability, and patient trust."

SUSHIL KUMAR MEHER
HEAD IT AND CISO
AIIMS

The Future May Become AI Versus AI

Cybersecurity is entering an era where intelligent systems will battle other intelligent systems in real time. Attackers are already leveraging AI to automate attacks, exploit vulnerabilities, bypass human filters, and scale cybercrime operations globally. Defenders are simultaneously deploying AI-driven analytics, automated remediation systems, and intelligent monitoring platforms to keep pace. Defending against AI-driven threats will require equally advanced AI-powered behavioral analysis capable of detecting anomalies across the entire attack chain. The future of enterprise cybersecurity will be a continuous battle between AI-powered attackers and defenders.

Clearly, cybersecurity is no longer a standalone IT function. As in other areas, AI will play a crucial role in ensuring enterprise trust, resilience, governance, compliance, and business continuity. Organizations that fail to modernize security frameworks, govern AI responsibly, and build resilient digital architectures will struggle to survive in an increasingly borderless organization.

FEATURE

AI-POWERED DATA CENTRES: THE NEW NERVE CENTRES OF ENTERPRISE INTELLIGENCE

- **Balaka Baruah Aggarwal**, Consulting Editor, Bharat Network Group

HOW AI IS TURNING DATA CENTRES INTO STRATEGIC BUSINESS ASSETS

Data Centres Are Becoming the Decision Layer of the Enterprise

Artificial intelligence is rapidly transforming the way enterprises operate, compete, and innovate. But behind every AI model, predictive engine, digital workflow, and real-time analytics lies an infrastructure layer that is becoming increasingly strategic — the modern data centre. Once viewed largely as passive repositories for storage and computing, data centres are now evolving into intelligent, dynamic ecosystems that power enterprise decision-making, automation, and digital experiences.

The explosive growth of AI workloads has fundamentally changed enterprise expectations from infrastructure. Organizations today demand scalability on demand, ultra-low latency, high-performance computing, real-time analytics, advanced cybersecurity, and sustainable operations — all at once. Traditional enterprise data centres, designed primarily for predictable workloads and standard compute requirements, are struggling to keep pace with these new realities. As AI adoption accelerates, businesses are increasingly shifting toward cloud-based, AI-ready data centres that supports GPU-intensive environments and distributed operations.

At the same time, the role of the data centre is expanding far beyond infrastructure management. It is becoming central to enterprise intelligence—from powering fintech lending decisions to enabling AI-driven manufacturing operations, modern data centres are shaping how businesses process data to deliver differentiated services and create competitive advantage.

"Today, the data centre concept has changed. It is no longer a back-office affair. It has become an intelligence layer," observed Arnab Sarkar, Co-Founder and COO, eFunds. "Businesses now expect data centres to support decision-making, vigilance, security, and real-time outputs."

This transformation

is especially visible as enterprises embrace AI at scale. Organizations are no longer asking whether they need AI infrastructure — they are asking how quickly they can access, scale, secure and optimize it for business outcomes.

From Traditional Infrastructure to AI-Ready Platforms

One of the biggest shifts emerging today is the redesign of data centres themselves. AI workloads require a fundamentally different architecture compared to conventional enterprise applications.

"As you know now, when it comes to looking at data centres from an AI standpoint, the data centres need to be designed differently," said Suresh Vijayaraghavan, CTO, The Hindu Group Media.

Unlike conventional applications that rely primarily on CPU-based computing, AI training and inference models demand GPU-heavy environments capable of handling massive parallel processing tasks. This has created new challenges around energy consumption, cooling efficiency, compute density, and infrastructure resilience.

"The shift from traditional CPU-based computing to GPU-intensive AI workloads is fundamentally transforming data centre design. GPUs demand significantly higher power and advanced cooling capabilities, forcing organizations to rethink the entire data centre architecture."

However, Vijayaraghavan also emphasized an important distinction often overlooked in the AI excitement cycle. "We get confused many times that if we are adopting AI, we need GPUs ourselves," he explained. "But 70 to 80 percent of enterprises actually do not require GPUs because they are consuming LLMs through APIs. Unless you are building and training your own models, you do not need that high-end infrastructure."

"The shift from traditional CPU-based computing to GPU-intensive AI workloads is fundamentally transforming data centre design. GPUs demand significantly higher power and advanced cooling capabilities, forcing organizations to rethink the entire data centre architecture."

SURESH VIJAYARAGHAVAN
CTO
THE HINDU GROUP MEDIA

This distinction is becoming increasingly important for enterprises planning their AI strategy. Most organizations are not building foundational models from scratch. Instead, they are integrating AI services from providers such as OpenAI or Gemini into their applications and workflows. This allows enterprises to consume AI capabilities on demand without investing heavily in expensive infrastructure.

"It becomes an OPEX model for me," Vijayaraghavan added. "I consume tokens and only pay for usage. I do not have to worry about the CAPEX of building large infrastructure."

This shift toward consumption-based AI infrastructure is fundamentally altering enterprise economics. Businesses can now scale compute resources dynamically, deploy AI faster, and experiment with innovation without committing to large infrastructure investments.

Data Centres as Business Enablers

The impact of AI-powered data centres is particularly visible in industries undergoing rapid digital transformation. For sectors like fintech, logistics, manufacturing, and mobility, infrastructure agility has become directly linked to business growth.

At TVS Mobility, changing business dynamics and growing digital operations forced a rethink of traditional infrastructure models. "Earlier, we were known to be a traditional company with a brick-and-mortar model," said Manjunath Prasad, Head IT, TVS Mobility Private Limited. "But with digital adoption happening across the organization, our internal data centre would not have been sufficient to support the scale of growth." The company increasingly adopted public and private hosted data centre models to support scalability, operational flexibility, and AI workloads.

"There are two major advantages," Prasad explained. "First, we can ramp up and ramp down as per our requirement because everything comes with a pay-per-use model. Second, these platforms help us roll out products faster to the market."

This agility is critical in the AI era, where infrastructure needs can fluctuate dramatically depending on training cycles, experimentation, or seasonal demand.

"As TVS Mobility's digital operations expanded, we realized that traditional infrastructure could not support the scale and agility required for growth. Hosted and cloud-based data centres give us the flexibility to scale on demand, accelerate product rollouts, and efficiently support AI workloads without significant upfront investments. In the AI era, infrastructure agility is just as important as computing power."

MANJUNATH PRASAD
HEAD IT
TVS MOBILITY PRIVATE LTD

"AI workloads may only require infrastructure for a specific targeted duration," Prasad noted. "It will not always be a 24x7 requirement. AI-powered data centres help us meet objectives without unnecessary investments."

For fast-growing digital businesses, this flexibility is becoming indispensable. For instance, in fintech, the role of intelligent infrastructure is even more central. Real-time lending decisions, customer onboarding, risk assessment, fraud detection, and underwriting all depend on high-speed data processing and scalable compute capabilities.

"Fintech would not have been possible without the digital public infrastructure of India," Sarkar said. "The cost of acquisition and processing has become extremely efficient because these systems are backed by powerful data centre ecosystems."

The Sustainability Challenge

As AI adoption grows, so do concerns around energy consumption and environmental impact. AI-ready data centres consume significantly higher power than conventional facilities, especially when supporting GPU-intensive workloads. This has made sustainability a core priority for infrastructure providers.

"The new buzzword is

AI-ready data centres," said Suman Chandra, AVP Sales, Techno Digital. "To support AI workloads, you need specialized infrastructure."

Techno Digital has adopted advanced cooling technologies to improve energy efficiency while supporting high-density AI environments. "We use water-cooled chillers, which improve energy efficiency by 35 to 45 percent," Chandra explained. "But then the question becomes — what about water usage?"

To address this, the company implemented adiabatic cooling systems designed to reduce water consumption significantly. "This technology helps reduce water usage to nearly one-fifth of conventional consumption," he said.

Renewable energy is also becoming central to modern data centre strategies. "Eighty percent of our data centre operations use renewable energy," Chandra added. "Environment-friendly infrastructure is becoming essential for future-ready AI deployments."

Sustainability is no longer simply a compliance requirement. Increasingly, enterprises are evaluating infrastructure partners based on energy efficiency, renewable energy adoption, and environmental responsibility.

The New Security Imperative

As data centres become the operational core of AI-driven enterprises, cybersecurity and data governance have emerged as critical concerns. The migration to cloud and AI-powered environments has created a shared responsibility model where both service providers and enterprises must work together to secure infrastructure and data.

"The moment you are using cloud, security becomes a shared responsibility," Vijayaraghavan emphasized. "Physical security lies with the service provider, but logical security is shared."

Organizations still remain responsible for securing applications, access controls, passwords,

workloads, and data governance. “If something goes wrong, management will ask me — not the cloud provider,” he remarked.

This reality is driving enterprises to demand stronger compliance frameworks, certifications, and security controls from infrastructure partners. “I will ensure the provider has all the certifications and independent audits in place,” Vijayaraghavan said. “At the same time, I must ensure all my logical controls are implemented properly.”

Data privacy concerns are particularly acute in industries handling sensitive information such as financial services and healthcare. “In financial services, trust is everything,” Sarkar said. “The PII data of individuals is highly sensitive. Customers are very concerned about where their data goes and how it is protected.”

India’s Digital Personal Data Protection (DPDP) Act has further intensified enterprise focus on governance and compliance. “Organizations are now worried about fines up to ₹250 crore in case of data breaches,” Sarkar pointed out.

As enterprises increasingly rely on multiple third-party integrations, APIs, and distributed cloud environments, maintaining visibility and governance over data flows is becoming more complex.

“You never know at which layer the compromise happens,” Sarkar warned.

“In financial services, trust is everything. As organizations handle increasingly sensitive customer data across multiple platforms, cloud environments, and third-party integrations, maintaining visibility and control becomes critical. With stricter regulations such as the DPDP Act and significant penalties for breaches, data governance is no longer just a compliance requirement—it is a business imperative."

ARNAB SARKAR
CO-FOUNDER AND COO
EFUNDS

AI Inside the Data Centre

Interestingly, AI is not just powering enterprise applications — it is also transforming data centre operations themselves. Infrastructure providers are increasingly using AI-driven analytics, automation, and monitoring systems to improve security, operational efficiency, and predictive maintenance.

“We have implemented video analytics systems inside our data centres,” Chandra explained. “If a person enters a server hall, we monitor the entire movement from entry to exit. Suspicious activities can be identified using AI tools.”

AI is also helping providers optimize cooling systems, monitor power utilization, predict equipment failures, and automate incident responses. The convergence of AI with infrastructure management is creating what many describe as “self-optimizing” data centres — environments capable of adapting dynamically to workload demands while minimizing operational inefficiencies.

Regaining Control in the AI Era

As enterprises increasingly depend on hyperscale providers and cloud-based AI platforms, questions around control and ownership are becoming more prominent.

Are organizations

losing control over their applications and data as they rely more heavily on external infrastructure ecosystems? According to Vijayaraghavan, the answer depends largely on how enterprises architect their AI strategies. “The control still lies with us because the data belongs to us,” he explained. “The model works on the data we provide.”

Organizations today have multiple deployment options — from consuming AI services through APIs to hosting large language models within their own infrastructure environments. “We can always bring the LLM back into our premises if we want complete control,” he said.

Prasad echoed similar sentiments, emphasizing that enterprises can implement “guardrails” to ensure data remains within controlled boundaries. “Technology today supports these controls,” he said. “You can ensure that your data stays within your tenant and does not leak outside.”

However, experts agree that governance, monitoring, and continuous oversight remain essential. “Monitoring is absolutely necessary,” Prasad cautioned. “A small mistake somewhere can lead to data exposure.”

From Infrastructure to Intelligence

Data centres are no longer just processing enterprise intelligence — they are becoming the origin point of intelligence itself. With AI workloads demanding massive GPU compute, real-time data streaming, and ultra-low latency processing, the modern data centre is evolving into a live decision engine for the enterprise.

The key shift is this: enterprises are no longer just running applications in data centres; they are running intelligence through them. Every customer interaction, fraud detection event, supply chain optimization, and predictive insight is increasingly dependent on AI models executing inside or across

distributed data centre ecosystems.

This transforms the data centre into a “nerve centre” in the truest sense — not just connecting systems, but continuously sensing, analyzing, and responding to business signals in real time.

At the same time, AI is reshaping the architecture of data centres themselves. GPU-intensive computing, edge integration, and hybrid cloud deployments are forcing a rethink of power, cooling, and workload distribution. Sustainability pressures add another layer, making energy efficiency and intelligent workload orchestration as critical as raw compute capacity.

Another important dimension is governance. As AI models increasingly operate within data centres, issues of data privacy, model security, and responsible AI governance move closer to the infrastructure layer. The data centre is no longer neutral — it has become a control point for trust, compliance, and risk management.

This convergence of compute, intelligence, and governance is what makes AI-powered data centres fundamentally different. They are not just supporting enterprise intelligence — they are actively shaping it.

In the age of AI, competitive advantage will not come only from better models or applications, but from how intelligently and efficiently an enterprise can convert data centre capacity into real-time decision-making power.

"AI is fundamentally reshaping data centre design. Supporting AI workloads requires specialized infrastructure, from high-density compute environments to advanced cooling systems that improve energy efficiency while reducing resource consumption. As demand for AI grows, sustainability has become just as important as performance, making renewable energy and efficient cooling technologies critical components of future-ready data centres."

SUMAN CHANDRA
AVP SALES
TECHNO DIGITAL

The Future of Enterprise Intelligence

The rise of AI-powered data centres signals a much larger transformation underway in enterprise technology. Infrastructure is no longer an invisible backend utility. It is becoming central to innovation, resilience, customer experience, and competitive strategy.

Traditionally, data centres were viewed as passive infrastructure — places where data was stored and applications hosted. In the cloud era, they became more elastic and scalable, but still largely remained “back-end enablers.”

As enterprises embrace AI at scale, data centres are evolving into intelligent digital ecosystems enabling real-time decision-making, scalable innovation, and secure digital operations. The future enterprise will not simply run on applications — it will run on intelligent infrastructure. And in that future, data centres will no longer be measured merely by uptime or storage capacity. They will be evaluated by how effectively they enable intelligence, trust, agility, and sustainable growth.

FEATURE

BUILT FOR SCALE: INDIA IS POISED AS GLOBAL AI POWER HOUSE

India's AI story is not being built in laboratories alone. It is taking shape across digital platforms serving billions of transactions, developer communities creating the next generation of applications, and a rapidly expanding ecosystem of compute, data, and innovation.

- Balaka Baruah Aggarwal, Consulting Editor, Bharat Network Group

For decades, India was seen as the back office of the world, then as a technology talent powerhouse, and more recently as one of the fastest-growing digital economies. Today, a new opportunity is redefining India's position in the global technology landscape.

Artificial Intelligence is emerging as the next engine of economic transformation, and India is uniquely positioned to influence its future. A combination of world-class engineering talent, a thriving startup ecosystem, expanding cloud and data centre infrastructure, growing enterprise adoption, and increasing government support is creating the conditions for large-scale AI innovation.

More importantly, India offers something few countries can match: the ability to develop, deploy, and scale AI solutions across industries and populations of unprecedented size and diversity. As organizations and technology providers accelerate investments in AI, the real question is whether India can convert its unique advantages into global leadership.

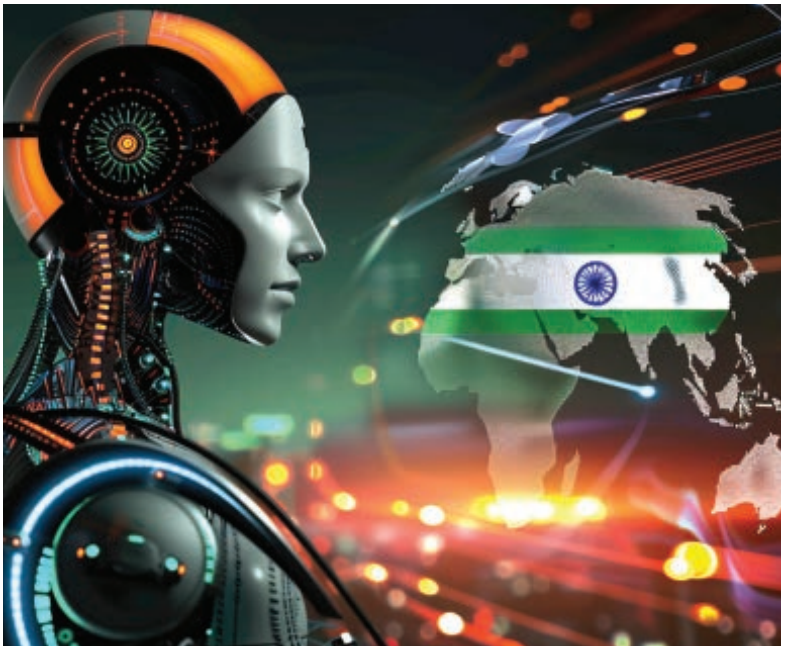
India's advantage is rooted in a decade-long investment in Digital Public Infrastructure (DPI) which is transparent, accountable and built on government frameworks. Platforms such as Aadhaar, UPI, DigiLocker, Account Aggregator, ONDC, and CoWIN have created interoperable digital rails that connect identity, payments and data at population scale.

As AI moves from experimentation to real-world deployment, these platforms provide entrepreneurs with the ability to integrate intelligence directly into the economic and social fabric. DPI has provided a solid footing for India's AI leadership with a unique ability to operationalize AI at scale.

India is no longer preparing for the AI era. It is building the conditions to lead it.

India's Infrastructure Advantage: Foundation Powering India's AI Ambitions

While much of the global AI



conversation is dominated by large language models, GPUs, and billion-dollar investments, India's has focused on building a robust digital foundation and a sophisticated ecosystem that few countries can match.

The significance of this infrastructure lies in that AI operations require trusted digital identities, interoperable data flows, authenticated records, real-time transactions, and large-scale citizen participation.

India has many of these building blocks in place. UPI, for instance, demonstrated India's ability to build and operate a digital platform capable of handling billions of transactions every month. Aadhaar created a digital identity layer that can securely verify individuals, while DigiLocker has established a framework for authenticated digital documents, while the Account Aggregator ecosystem introduced consent-based data sharing that gives citizens greater control over their financial information. ONDC is now extending similar principles to digital commerce by creating an open network that connects buyers, sellers, logistics providers, and service platforms.

These platforms create fertile ground for AI-driven innovation. For instance, financial institutions can leverage AI to expand credit access, assess risk more intelligently, and deliver personalized financial services to underserved populations. Healthcare providers can build AI-powered diagnostic, triage, and patient engagement systems on top of digital health records and identity frameworks. Governments can deliver citizen services through conversational AI interfaces while farmers can benefit from AI-powered advisory services that combine satellite imagery and market intelligence to improve agricultural outcomes.

INDIA STACK: DIGITAL RAILS POWERING AI FUTURE

India Stack is a set of open digital platforms and APIs that enable:

- Digital identity
- Real-time payments
- Paperless documentation
- Consent-based data sharing
- Digital commerce
- Citizen service delivery

Key Building Blocks

- Aadhaar
- UPI (Unified Payments Interface)
- DigiLocker
- Account Aggregator Framework
- ONDC (Open Network for Digital Commerce)
- CoWIN

What makes India's position stand out is the scale at which these systems operate. India has created interoperable digital rails that connect identity, payments, data, documents, commerce, and public services for more than a billion people. The next phase of India's digital journey may therefore be less about building new infrastructure and more about infusing intelligence into the infrastructure that already exists. In that sense, DPI is not merely a technology achievement, but a foundation to lead in AI innovation.

India's Developer Ecosystem Driving AI Momentum

As AI moves from research labs into industries and public services, the countries that possess large communities of developers capable of building, customizing, and scaling AI solutions will have a competitive advantage.

As per global data on GitHub AI projects by geographic distribution, India was the second-largest contributor worldwide in 2024, accounting for 19.9% of all AI projects. India's position as the world's second-largest contributor to AI projects on GitHub is more than a measure of developer activity. It reflects the country's software engineering ecosystem

THE COMPUTE ADVANTAGE

- 4 GW+ projected data centre capacity by 2030
- US$25 Billion+ expected investments
- AI workloads require up to 10x more compute power
- Multiple hyperscaler cloud regions operational in India
- Growing focus on GPUs, high-density computing, and advanced cooling

and ability to translate AI breakthroughs into real-world applications.

This is because AI is fundamentally a software technology as most organizations will not build their own foundation models. Economic value will be created by building AI-powered products, integrating AI into workflows, developing industry-specific applications, creating agents, fine-tuning models, building APIs, automating processes, and deploying AI solutions at scale—all of which will require software engineering capabilities.

Second, countries that have strong software ecosystems tend to adapt to new technology waves faster. India has expertise in enterprise applications, cloud, data engineering, cybersecurity, digital platforms, and product development, and AI is increasingly becoming an extension of these capabilities.

Third, GitHub AI activity suggests that developers are moving beyond learning AI and are actually building with it. A developer creating an AI-powered customer support tool, an intelligent workflow engine, a healthcare copilot, or an AI agent is contributing to the practical application layer of AI. This is where most business value will eventually be created.

AI leadership will not be determined only by who builds the best foundation models. It will also be determined by who can build the largest ecosystem of AI-powered applications, products, services, and business solutions. India's strong software development ecosystem gives it a significant advantage because AI adoption ultimately happens through software.

The Compute Race: Why Capacity May Define AI Leadership

While headlines often focus on breakthrough models and AI applications, there is another race unfolding behind the scenes—one that will determine which countries emerge as long-term AI leaders. AI is an extraordinarily compute-intensive technology wherein every AI model must be trained, deployed, monitored, and continuously improved, requiring vast amounts of processing power, energy, storage, and connectivity. In many ways, AI is as much a capacity challenge as it is a software challenge. India is rapidly positioning itself

to meet that challenge. In the Union Budget FY27, the Government announced a major step to boost India's digital infrastructure. Since cloud computing, AI data centres and advanced electronics are essential for economic growth, the Government has introduced a tax holiday up to 2047 for foreign cloud service companies that operate through data centres located in India.

Favorable data center policies are attracting investments by global data centre providers to provide high-performance computing and AI-ready facilities. The total data centre capacity has increased from about 375 MW in 2020 to around 1500 MW by 2025. According to the Ministry of Electronics and IT, about 38,231 GPUs have been onboarded through 14 empanelled data centres under the AI compute capacity framework.

Few countries can combine digital scale, software talent, and real-world deployment opportunities the way India can.

These are being provided to startups, researchers, academia at a subsidised average rate of ₹65 per hour which is about one-third of the global average cost.

Data centres in India are located in Mumbai, Chennai, Hyderabad, Bengaluru, Noida and Jamnagar. Global technology giants including Google, Microsoft, Amazon Web Services, Oracle, and IBM are expanding their cloud presence in India, while domestic players such as Reliance, Adani, CtrlS, Yotta, NTT Data, STT GDC India, and Sify are building large-scale capacity to support the next generation of AI workloads.

This surge in investment reflects an awareness that AI innovation cannot rely only on overseas compute resources. Countries seeking leadership in the AI must possess the ability to process, store, and manage massive volumes of data within their own ecosystems. As AI adoption accelerates demand for computing power is expected to grow exponentially.

India's ambitions are also being supported by a broader push into semiconductor manufacturing, electronics production, and advanced computing capabilities. Together, these investments are creating the foundational capacity required for AI research, model training, enterprise deployment, and large-scale innovation. The significance extends beyond technology. Compute capacity increasingly represents economic competitiveness, national capability, and digital sovereignty. The AI race is largely dependent on computing power, energy resources, connectivity networks to bring algorithms to life. India is moving aggressively to ensure that it is not merely a consumer of AI innovation but a destination where AI can be built, scaled, and deployed for the world.■

HOW UPI BECAME INDIA'S MOST SUCCESSFUL DIGITAL PUBLIC PLATFORM

From Financial Inclusion to Global Inspiration. UPI has done more than digitize payments—it has expanded economic participation, accelerated innovation, and created a blueprint for digital economies worldwide.

- Ashish Srivastava, Co-Founder & Director, Bharat Network Group

Undoubtedly, the most remarkable success story in India's Digital Public Infrastructure is the Unified Payment Interface (UPI) which is the world's largest real-time digital payment system. According to data from National Payment Corporation, UPI transactions registered a record high of Rs 29.90 lakh crore in value, and 23.2 billion transactions in May 2026.

Even as nations are racing to build digital economies, India has established a real-time payment infrastructure that serves everyone, from metropolitan professionals and digital-first enterprises to rural farmers and street vendors.

UPI has not only redefined how money moves across the world's most populous nation, but it has also demonstrated how a robust DPI can become a powerful catalyst for inclusive economic growth.

The Government's initiative as early as 2009 by setting up National Payment Corporation of India (NCPI) has given India a headstart in one of the most critical digital infrastructure capabilities.

Processing 23.2 billion transactions worth ₹29.9 lakh crore in a single month, UPI has become the world's largest real-time payments platform and a global case study in digital public infrastructure.

In 2016, the NCPI released the first version of the UPI which is built on an open-source API and allows inter-bank peer to peer and person to peer transactions from mobile phones using a unique UPI ID. Today that system has become a global success story that facilitates UPI transactions across eight countries.

Engineering Inclusion at Population Scale

For decades, financial inclusion remained one of India's biggest challenges as millions lacked access to formal banking systems. To address this challenge, India adopted a platform-based approach instead of building isolated solutions.

The Government of India, in collaboration with the banking ecosystem and the NPCI, laid the foundation for a DPI stack comprising Aadhaar, Jan Dhan accounts, mobile connectivity, and UPI. The result was a digital framework that could operate at national scale while remaining accessible to the smallest participant in the economy.

Today, a fruit seller in Varanasi, a handicraft entrepreneur in Assam,

From street vendors and rural entrepreneurs to fintech innovators and global payment networks, UPI has transformed how India transacts, participates, and grows.

and a startup founder in Bengaluru all operate on the same payment rails, something few countries have achieved.

The Rise of India's Digital Public Infrastructure

Globally, digital payment ecosystems are often dominated by private networks. India's approach has been fundamentally different. UPI was designed as public digital infrastructure - open, interoperable, and accessible to every bank, fintech, and technology innovator. This approach has unleashed a wave of innovation wherein fintech startups, banks, digital wallets, and merchants have built customer experiences on top of a common infrastructure layer. The outcome is a thriving digital economy with innovative applications on top of a universally accessible infrastructure layer. Today, UPI has become a case study in how governments can create foundational digital platforms to encourage innovation.

- **23.2 Billion** UPI transactions in May 2026
- **₹29.9 Lakh Crore** Value processed in a single month
- **8 Countries** Now support UPI-enabled transactions
- **Millions of Merchants** Connected to India's digital payments ecosystem

Beyond Payments: Creating Economic Identity

The true disruption of UPI is the empowerment of millions of people. Every digital transaction creates data trails that help individuals and businesses build financial identities. For millions of micro-entrepreneurs and small businesses, this digital footprint has become an entry point to formal credit, insurance, and financial products. This represents a significant shift from traditional lending models that relied heavily on collateral and extensive documentation. By transforming transaction data into trust, UPI has extended financial institutions to serve underserved segments.

At the same time, UPI has bolstered the start-up ecosystem. It has lowered customer acquisition costs, accelerated digital adoption, and created opportunities for entrepreneurs to

develop innovative financial products. From embedded finance and merchant solutions to lending platforms and digital banking experiences, India's startup ecosystem has leveraged UPI to build solutions at unprecedented scale.

The most significant achievement of the UPI infrastructure is the ability to penetrate rural areas. Government-led initiatives focused on digital literacy, smartphone adoption, banking access ensured that digital payments reach rural and semi-urban regions. Innovations such as offline payments, voice-enabled transactions, vernacular interfaces, and lightweight payment solutions are expanding accessibility.

From Domestic Success to Global Blueprint

Countries across the world are increasingly studying India's digital public infrastructure model. The government's efforts to expand UPI's international acceptance and establish cross-border payment partnerships are positioning India as a global exporter of digital innovation.

What began as a solution to domestic financial inclusion is now emerging as a blueprint for nations seeking to build resilient, scalable, and inclusive digital economies. India's UPI journey offers a compelling lesson in that a robust public technology infrastructure triggers inclusion and economic participation becomes more equitable.

More than a payments platform, UPI has become the foundation for financial inclusion, digital innovation, and economic empowerment at unprecedented scale.

The Next Frontier

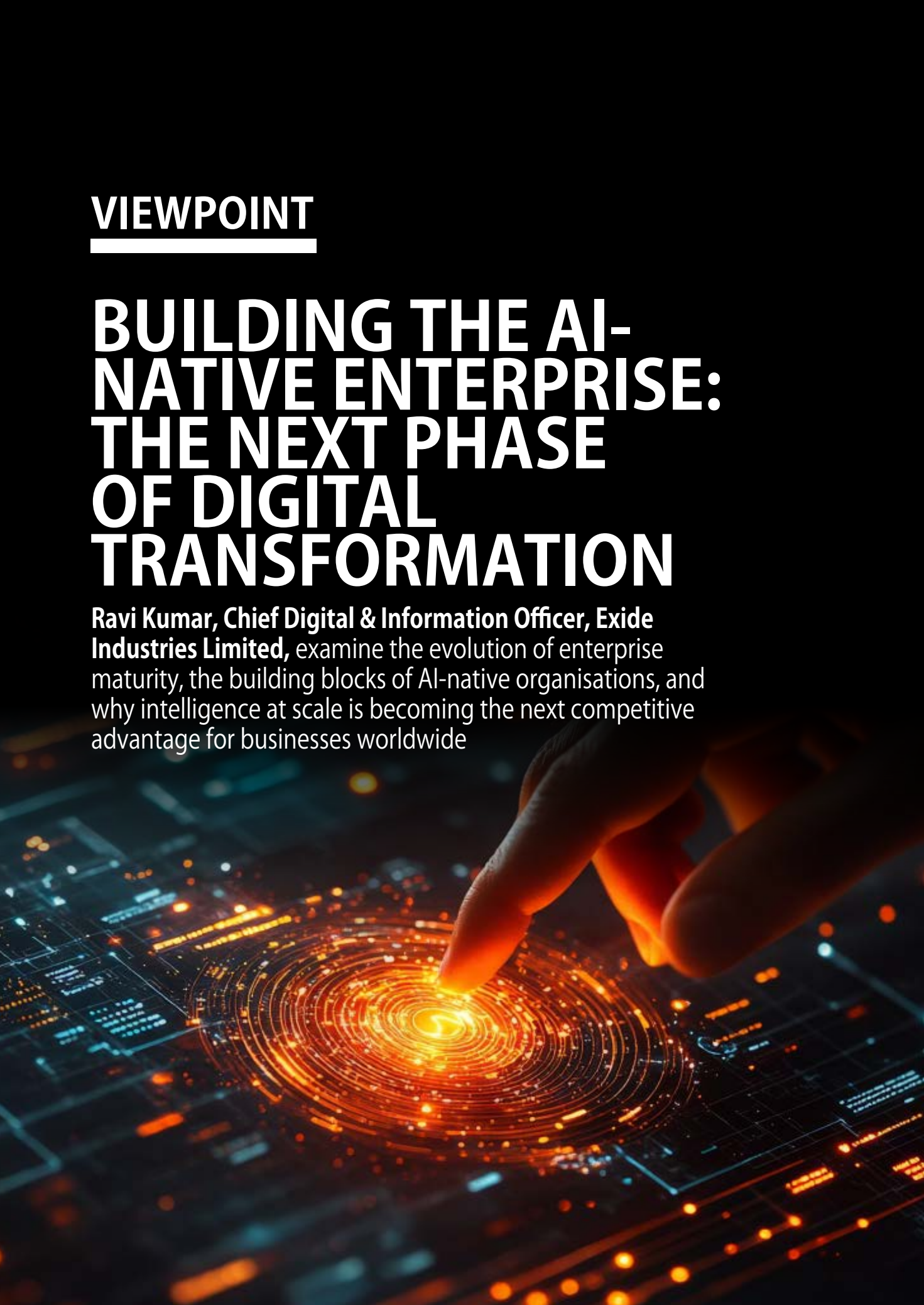
India's digital transformation story is far from complete. The government's continued focus on strengthening DPI is aimed at creating a future where citizens and business can participate seamlessly in the digital economy.

As the world looks for models of technology-led development, India's UPI revolution stands as a powerful reminder that true disruption is not measured by technology alone, but by the number of lives it transforms.■

VIEWPOINT

BUILDING THE AI-NATIVE ENTERPRISE: THE NEXT PHASE OF DIGITAL TRANSFORMATION

Ravi Kumar, Chief Digital & Information Officer, Exide Industries Limited, examine the evolution of enterprise maturity, the building blocks of AI-native organisations, and why intelligence at scale is becoming the next competitive advantage for businesses worldwide



The Next Competitive Advantage: Intelligence at Scale

Every major technology wave changes the economics of business. ERP transformed transactions. The internet transformed connectivity. Cloud-transformed infrastructure. Mobile transformed access. Digital transformation transformed processes. Artificial Intelligence is now transforming something even more fundamental: intelligence itself.

For over a decade, organizations have focused on digitizing workflows, integrating systems, and building data platforms. These investments have delivered unprecedented visibility, efficiency, and scalability. Yet, despite these advances, many critical business decisions continue to rely on fragmented information, individual experience, and manual intervention.

The next phase of digital transformation is fundamentally different. It is not about creating more dashboards, automating more workflows, or collecting more data. It is about building AI-native enterprises, organizations where intelligence is embedded into every workflow, every interaction, and every decision.

The winners of the next decade will not necessarily be organizations with the most data or the most AI models. They will be those that can systematically convert intelligence into action at scale.

As organizations continue their digital evolution, the conversation is shifting from automation to intelligence. The real opportunity now lies in transforming enterprise operating models so that decision-making becomes faster, smarter, and increasingly proactive. This requires moving beyond isolated AI experiments and creating environments where intelligence becomes an integral part of daily business operations.

The Evolution of Enterprise Maturity

Enterprise transformation has evolved through four distinct stages. The first wave focused on digitizing transactions and processes. Organizations implemented ERP systems, CRM platforms, workflow automation tools, and digitized business operations. The primary objective was efficiency, standardization, and operational control. The key question was: "Can we capture transactions digitally?" This stage established the foundation for modern enterprises by creating structured digital records and reducing dependence on manual processes.

As digital footprints expanded, enterprises accumulated vast amounts of operational data. This led to investments in data lakes, analytics platforms, dashboards, and business intelligence solutions. Organizations gained unprecedented visibility into customers, operations, and performance. The key question evolved to: "Can we generate insights from data?" While valuable, many organizations discovered that visibility alone does not guarantee better decisions. Access to information became easier, but transforming that information into meaningful action remained a challenge.

The next evolution introduced AI as a decision-support capability. Machine learning models,


The next phase of digital transformation is not about digitizing workflows. It is about embedding intelligence into workflows

recommendation engines, conversational assistants, and predictive analytics began augmenting human decision-making. The key question became: "Can AI help people make better decisions?" Most enterprises today operate in this stage. Sales teams receive recommendations, service teams receive diagnostic suggestions, recruiters receive candidate matching scores, and executives interact with conversational analytics platforms. Decision-making becomes faster, more informed, and more consistent.

The AI-native enterprise represents a more profound shift. Rather than providing recommendations after the fact, intelligence becomes embedded directly within business workflows. The key question changes to: "Can intelligence become part of the workflow itself?" In an AI-native enterprise, customer interactions are supported by intelligent agents, warranty claims are validated automatically, IT issues are resolved proactively, supply chain decisions are continuously optimized, and employees access enterprise knowledge through natural language conversations. Intelligence becomes pervasive, contextual, and available at the moment decisions are made.

Where Many Organizations Get Stuck

Despite significant AI investments, many enterprises struggle to move beyond experimentation. The reason is rarely technology. Most organizations attempt to layer AI onto fragmented processes rather than redesigning workflows around intelligence. Three common pitfalls emerge.

Treating AI as a Technology Initiative

AI is often delegated to technology teams without clear business ownership. Successful organizations start with business outcomes, not algorithms. The most successful AI programs are those where business leaders and technology leaders work together to define measurable outcomes and transformation goals.

Starting with Models Instead of Decisions

The most important question is not: "Which AI model should we deploy?" The more important question is: "Which business decision are we trying to improve?" Organizations that begin with business decisions rather than technology choices are far more likely to achieve meaningful results and sustainable adoption.

Deploying AI Outside the Workflow

Employees do not want another AI application. They want better decisions inside the applications they already use. The most successful AI implementations are often invisible. They appear precisely where work happens, enabling

users to act on insights without disrupting existing workflows.

Building Blocks of an AI-Native Enterprise

Organizations seeking to become AI-native must focus on five foundational capabilities.

Unified Data Foundation

AI is only as effective as the quality, accessibility, and trustworthiness of enterprise data. Organizations need integrated views across customers, products, operations, finance, and supply chains. A modern data platform is no longer a competitive advantage. It is a prerequisite. Without trusted and accessible data, even the most advanced AI initiatives will struggle to deliver business value.

Intelligence Embedded in Workflows

AI should not operate as a separate destination. It must be embedded within ERP systems, CRM platforms, service applications, and collaboration tools. At Exide Industries, AI-driven recommendations are increasingly being integrated directly into sales, service, warranty, and support workflows, ensuring that intelligence is available at the point of decision-making. This significantly improves adoption and accelerates decision cycles.

Human-AI Collaboration

The future is not human versus machine. It is human plus machine. AI excels at pattern recognition, prediction, and speed. Humans excel at judgment, context, creativity, and ethics. The most effective enterprises design workflows where each contributes what it does best. Organizations that achieve this balance can unlock higher productivity while maintaining accountability and trust.

Agentic Operating Models

The next frontier extends beyond recommendations. AI agents are increasingly capable of performing tasks, orchestrating workflows, and resolving routine issues autonomously. Digital workers are becoming part of the enterprise operating model. Organizations must prepare for managing teams that include both human and AI coworkers. This represents a significant shift in how work will be structured and executed in the future.

Responsible AI Governance

As AI becomes deeply embedded within business

processes, governance becomes critical. Organizations require clear frameworks for accountability, transparency, privacy, security, and bias mitigation. Trust will become one of the most important differentiators in the AI era. Responsible AI governance ensures that innovation can scale without compromising compliance, ethics, or stakeholder confidence.

From Experimentation to Enterprise Scale: Lessons from Exide

The transition from AI-assisted to AI-native is already underway. At Exide Industries, AI is being embedded across customer-facing, operational, and enterprise workflows.

Sales and Channel Effectiveness

AI-powered product recommendation engines, outlet prioritization models, and Next Best Action capabilities help field sales teams focus on the right opportunities and improve decision quality at scale.

Customer Service and Warranty Management

AI-powered service voice agents support customer interactions, while AI-driven warranty forensics automate claim validation and anomaly detection, improving both speed and accuracy.

Enterprise Productivity

Internal AI assistants enable natural-language access to business insights. AI-powered recruiter solutions accelerate candidate screening, while intelligent IT support agents help resolve routine employee issues more efficiently.

AI-driven recommendations are increasingly being integrated directly into sales, service, warranty, and support workflows, ensuring that intelligence is available at the point of decision-making

The objective is not simply automation. The objective is embedding intelligence directly into the flow of work. These initiatives demonstrate how AI can move beyond experimentation and become a core capability that supports enterprise-wide transformation.

The Leadership Imperative

Building an AI-native enterprise is not a CIO agenda. It is a CEO agenda. AI-native organizations require leaders to rethink operating models, decision rights, workforce capabilities, and performance management systems. The winners of the AI era will not be determined by who deploys the most AI models. They will be determined by who redesigns work most effectively.

Leadership teams must move beyond viewing AI as a productivity tool and begin viewing it as a new operating paradigm. Success will depend on aligning business strategy, technology investments, workforce readiness, and governance frameworks into a unified transformation agenda.

Looking Ahead

The last decade belonged to digital enterprises. The next decade will belong to AI-native enterprises. As AI technologies become increasingly accessible, competitive advantage will no longer come from technology adoption alone. It will come from an organization's ability to embed intelligence into every workflow, every interaction, and every decision.

In the digital era, enterprises competed on process efficiency. In the AI era, they will compete on intelligence at scale. Organizations that successfully combine data, technology, people, and governance will be best positioned to lead in an increasingly intelligent and interconnected future.

VIEWPOINT

THE FUTURE OF MANUFACTURING IN AN AI-DRIVEN WORLD

Sudhir Kanvinde, CIO, The Supreme Industries Ltd., highlights the growing impact of AI across predictive maintenance, quality control, product innovation, supply chain resilience, and sustainability, while emphasizing the critical role of human-AI collaboration in driving the next wave of industrial growth

The factories poised to lead the next decade are not necessarily the biggest, they will be the most intelligent. Artificial intelligence is transforming manufacturing from a regime of rigid automation into a world of connected intelligence, where every machine, workflow, and decision can become smarter. This paradigm shift is redefining how products are designed, produced, maintained, and delivered across the global industry.

Predictive Maintenance: Eliminating Downtime Before It Happens

One of the most immediate and impactful applications of AI is predictive maintenance. AI systems analyze sensor data and equipment patterns to predict maintenance requirements before failures occur, minimizing downtime and extending machinery life. This capability is crucial because unplanned downtime can cost manufacturers millions annually.

By detecting anomalies early, AI enables maintenance teams to address issues proactively rather than reactively, dramatically improving operational efficiency. As manufacturing environments become increasingly connected, predictive maintenance is emerging as a foundational capability for operational excellence.

Quality Control: AI-Enhanced Defect Detection

AI-enhanced quality control is revolutionizing how manufacturers ensure product excellence. Using sophisticated image recognition and machine learning techniques, AI systems simplify defect detection, minimize waste, and ensure superior product quality. AI-driven automation is projected to detect defects at 90% accuracy, significantly outperforming traditional human inspection methods. By as early as 2028, 40% of manufacturers will leverage Generative AI to automate product quality management, considerably improving development time and cost.'The result is not only higher product quality but also improved consistency, reduced rework, and enhanced customer satisfaction.

Productivity Gains and Efficiency

The productivity implications are staggering. AI-driven automation is projected to boost manufacturing productivity by up to 40% by 2035. This transformation stems from multiple factors, including reduced operational expenses, improved efficiency, and enhanced product quality.

Data is steering the future of the manufacturing sector, with developments in robotics, AI, and the Internet of Things guiding organizations toward more cohesive, intelligent, and automated manufacturing solutions. These technologies are enabling manufacturers to optimize resources, improve throughput, and respond more effectively to changing market demands.

Generative AI: Redesigning Product Development

Generative AI holds significant promise for addressing urgent challenges in product design, service excellence, and supply chain oversight. GenAI can significantly streamline data management by efficiently collecting, organizing, and summarizing vast amounts of structured and unstructured data from


GenAI can significantly streamline data management by efficiently collecting, organizing, and summarizing vast amounts of structured and unstructured data from diverse sources

diverse sources, including design, manufacturing, supply chain, distribution, customer feedback, and service support.

Through synthetic data augmentation, GenAI facilitates comprehensive and accurate simulations, aligning product development with stringent requirements and customer preferences while saving time and resources.

As a result, manufacturers can accelerate innovation cycles, improve product quality, and reduce the time required to move from concept to market.

The Asia-Pacific Manufacturing Hub

The Asia-Pacific region, serving as the world's largest manufacturing and consumer hub, is expected to continue growing despite challenges such as a sluggish global economy, higher interest rates, material cost inflation, and protectionist trade policies.

Governments across the region—including India, China, South Korea, Taiwan, Singapore, Malaysia, and Thailand—are actively supporting manufacturing advancement through policy initiatives and infrastructure development.

As a result, IDC predicts that by 2027, more than 30% of Asia-based Top 2000 manufacturers will invest in new advanced planning and scheduling deployments, leading to order fulfillment rates above 95%.'This growth highlights the strategic importance of the region in shaping the future of intelligent manufacturing.

Human-AI Collaboration: Enhancement, Not Replacement

A critical misconception about AI in manufacturing is that it will replace human workers. In reality, AI is designed to enhance the role of human workers, not replace them.

By automating repetitive tasks and providing crucial data insights, AI enables workers to focus on their strengths: creativity, problem-solving, and strategic decision-making. This partnership between humans and machines is key to driving a new wave of productivity, innovation, and growth. The AI era is not replacing manufacturing fundamentals—it is amplifying them.

Sustainability and Energy Optimization

AI contributes significantly

to sustainable manufacturing practices. AI can optimize energy consumption and resource utilization within factories, leading to a more sustainable manufacturing process.

By analyzing production patterns and environmental conditions, AI systems identify inefficiencies and recommend adjustments that reduce waste and carbon emissions. This aligns with growing global pressure for manufacturers to adopt environmentally responsible practices.

Sustainability is increasingly becoming both a business priority and a competitive differentiator, making AI a powerful enabler of greener manufacturing operations.

Safety Enhancements

Enhanced safety is another critical benefit of AI adoption. By automating dangerous tasks and predicting equipment failures, AI creates a safer work environment for human employees. Robots equipped with AI can handle hazardous materials, operate in extreme conditions, and perform tasks that would put human workers at risk. This dramatically reduces workplace injuries and fatalities while improving overall operational reliability.

As workplace safety standards continue to evolve, AI will play an increasingly important role in protecting employees and ensuring regulatory compliance.

Supply Chain Resilience

The future of AI in manufacturing points toward hyper-automation, self-optimizing factories, and human-AI collaboration at every stage of the production process.

Future factories will leverage AI to connect different parts of the supply chain, creating an intelligent ecosystem where production, logistics, and quality control communicate

seamlessly. Manufacturers will expand their spare parts ecosystem partners across the supply chain to confidently deliver resolution and customer outcomes, addressing the challenge of unable-to-meet global repair SLAs.

This interconnected approach will strengthen resilience, improve visibility, and enable faster responses to disruptions.

Product Innovation Through Data

AI enables product innovation by analyzing customer data and market trends to inform product development and create innovative products that cater to evolving consumer needs.

Generative design tools allow engineers to transform napkin sketches into CAD models automatically, accelerating the design-to-production timeline. This capability empowers organizations to experiment with new ideas, reduce development costs, and bring innovative products to market more quickly. As customer expectations continue to evolve, data-driven innovation will become a key driver of long-term growth.

Robots equipped with AI can handle hazardous materials, operate in extreme conditions, and perform tasks that would put human workers at risk

The Winning Formula

The future of manufacturing will not be won by companies that simply buy more machines. It will be won by companies that combine engineering excellence, operational discipline, and digital intelligence.

The factories of tomorrow will not just produce better—they will learn, predict, and adapt continuously. Manufacturing is moving beyond automation into a world where the future belongs to manufacturers that can sense faster, decide faster, and adapt faster. Organizations that successfully integrate technology, people, and processes will establish a lasting competitive advantage in the AI-driven economy.

Conclusion

The future of manufacturing with AI promises a shift that is both revolutionary and necessary. With smarter factories, predictive analytics, and a move toward sustainable practices, AI is not just changing how things are made but redefining what manufacturing can achieve.

As manufacturers continue to embrace digital transformation, AI will be at the core of achieving greater agility, sustainability, and competitiveness in the global market. The real meaning of the AI era is that factories will learn, predict, and adapt continuously—transforming manufacturing into an intelligent, responsive, and resilient ecosystem.■

VIEWPOINT

THE FUTURE OF DIGITAL TRANSFORMATION IN PHARMA: FROM PROCESS AUTOMATION TO INTELLIGENT OPERATIONS

Pramod Gokhale, Co-Founder and CEO, Multione Technologies, Former Sr. President & Global CIO, Mankind Pharma Limited, explores how the pharmaceutical industry is evolving from traditional process-driven operations to intelligent, interconnected enterprises powered by AI, ML, Industry 4.0, and data-driven decision-making

Traditional vs Modern Pharma Industry

When you look back, the traditional Pharma industry was following a very straightforward and focused sales and revenue generation defined roadmap. It use to have a pre-defined manufacturing strategy like only "Make to stock" or "Make to Order". Also, it use to have predefined root to market strategy because of non-availability of various other omni-channels for sales. The entire eco-system was being driven by sales prioritisation till manufacturing and distribution.

The traditional model was largely linear in nature, with each function operating within its own boundaries and limited real-time interaction with other functions. Decision-making was often based on historical data, experience, and periodic reviews rather than continuous intelligence.

Today the change is majorly happening because of exposure and availability of various modern technology trends and solutions, which are triggering and delivering various KPI outcomes across all functions in the organisation with a great agility in delivering results. More importantly it is bringing the complete harmony and automated integrations across all functions and various functions are being compelled to adopt those modern technology trends and solutions.

This impact is on all functions right from R&D till Distribution, to Finance/ Controlling, to HR & Admin. Modern enterprises are increasingly focusing on connected business processes where information flows seamlessly across departments, enabling faster response times, improved visibility, and more effective decision-making.

What Is Called a Modern Industry?

Modern Industry is trending to use modern technology which is more driven by AI/ML and Agentic AI Solutions. Various functions are adopting to replace mundane activities by automated tools. However, these tools are still being judged, being verified for consistent outcomes and then being deployed.

Modern industry is moving from volume based business strategy to value based business strategies. Modern industry is breaking all linear silos and being driven by inter-connected ecosystem right form demand sensing to the end-consumer supply chain, which is data driven and enabling industry to take simpler, faster, and better decision making.

The focus is no longer only on efficiency but also on intelligence. Organizations are increasingly looking at predictive and prescriptive capabilities that can help them anticipate challenges, optimize resources, and improve customer outcomes. This transition is paving the way for truly intelligent operations across the pharmaceutical value chain.

Digital Transformation Across Core Functions

R&D Transformation

R&D functions are moving from person-dependent processes to Network AI/ ML-driven decision making, which is also improving overall process TATs and more accurate data-driven outcomes with optimum cost.

By leveraging advanced analytics and intelligent

Quality Control and Quality Assurance are using AI-based tools for Real-time deviation detection and CAPA generation

models, research teams are able to process larger datasets, identify patterns faster, and accelerate innovation cycles. This helps organizations reduce development timelines while improving confidence in outcomes.

Supply Chain Modernization

Complete supply chain is checking out various outcomes with AI/ML and also bolting this tools on traditional legacy/ ERP or any supply chain applications. Demand sensing and generation is looking out the data till the last ecosystem record like consumer details.

Supply chains are becoming increasingly connected and responsive. The ability to sense demand fluctuations, monitor inventory levels, and predict supply disruptions allows organizations to improve service levels while optimizing costs.

Smart Manufacturing and Industry 4.0

Manufacturing and Quality are adopting Industry 4.0 initiatives and trying to generate RCCP and PPDS with AI based algorithms and especially running these tools to monitor/ control/mitigate constraints in Man-Material-Machines which are pillars of manufacturing. IOT based data is being used for OEE monitoring and AI/ML is being used for predictive maintenance of machines to avoid breakdowns.

This enables manufacturing units to move from reactive operations to proactive and predictive models. Real-time visibility into production environments helps improve operational efficiency, reduce downtime, and enhance overall equipment effectiveness.

Intelligent Packaging and Monitoring

Packing lines are completely monitored with vision based track&trace lines having iOT enablements. These are also monitored with NLP based observatory control towers.

Such capabilities improve traceability, compliance, and operational transparency while reducing manual interventions and improving quality outcomes.

Quality Control and Assurance

Quality Control and Quality Assurance are using AI based tools for Real-time deviation detection and CAPA generation. AI tools are also being used for Quality instruments scheduling and eBMR validations.

The ability to identify deviations early and generate corrective actions in real time helps maintain product quality standards while improving compliance and operational efficiency.

Regulatory Excellence

Regulatory is using Generative AI engines to create dossiers for products for filing in various countries with respect to country specific regulatory requirements.

As regulatory environments continue to

evolve globally, AI-assisted document generation can significantly improve accuracy, consistency, and speed while reducing manual effort in regulatory submissions.

Balancing Benefits with Vulnerabilities

Pharma industry, adopting these new technologies should also have balancing act between agile/fast TATs vs consistent outcomes with data protection initiatives and technical and operational challenges.

The tools being deployed should be checked for its continuous and consistent outcomes and also for some default data leakage loopholes. Even if data is protected within company peripheral area but still data is going out onto some SaaS based solutions. So frequent virgins audits of these SaaS based solution is very crucial to ensure data protection.

Data protection and cyber resilience must be considered as foundational requirements rather than afterthoughts. Organizations must establish strong governance mechanisms to continuously monitor risks and validate controls.

OT Security was air-gapped from corporate IT infrastructure scope and becomes very vulnerable as threat-worker can come into mainstream network from OT loopholes. As IT and OT environments become increasingly interconnected, securing these environments becomes critical. Threat actors often target less protected systems as entry points into larger enterprise networks. This industry should comply all regulatory requirements by confirming all processes and systems for documented, repeatable and explainable evidences. If some black-box algorithms does not provide validated outcomes and could not explain the result, then regulatory compliances can not be met and may become challeng.

Therefore, explainability, traceability, and validation remain critical pillars of any technology deployment within highly regulated pharmaceutical environments.

Key Considerations for Successful Adoption

Industry should identify the use-cases within own scope of working and should not go for adoption of modern trends, until those are not, well evaluated technically, functionally, commercially, and more importantly from cyber security perspective.

From a data and infrastructure perspective, organizations should build automated ALCOA+ data integrity into software designs from day one. At the same time, they should avoid simply lifting and shifting legacy software into the cloud without refactoring its security architecture and control mechanisms.

From an OT cybersecurity perspective, organizations should deploy proper segmentation between plant floor equipment and corporate IT environments. Manufacturing equipment should never be directly connected to corporate networks merely to enable faster analytics, as this significantly increases cyber risk exposure.

True digital maturity in pharma is defined NOT by speed of innovation, but by deploying the rightly evaluated tool at the right use-case with the right CSA proven

For system validation, organizations should use Computer Software Assurance (CSA) methodologies to focus testing efforts on high-risk safety and quality features. Validation should not be treated as a static documentation exercise performed only before a product launch, but rather as a continuous process embedded throughout the system lifecycle.

When it comes to Artificial Intelligence, organizations should implement Explainable AI (XAI) with a mandatory Human-in-the-Loop approval process. Autonomous AI engines should not be allowed to modify GxP parameters without a clear, interpretable, and auditable trail of decisions and actions.

Conclusion: Innovation with Control

The Verdict: Adopt the Tools, but Strictly Control the Architecture

Pharma companies can adopt modern technology trends which are needed for delivering value outcomes with improved TATs. However, they must completely avoid autonomous operational loops, unsegmented vendor connections, and uninterpretable AI models.

True digital maturity in pharma is defined NOT by speed of innovation, but by deploying the rightly evaluated tool at the right use-case with the right CSA proven and completely covered under the perimeter of GxP data integrity.

As the industry continues its journey toward intelligent operations, success will depend on striking the right balance between innovation, compliance, cybersecurity, and governance. Organizations that can combine these elements effectively will be best positioned to unlock sustainable value from digital transformation while maintaining trust, quality, and regulatory compliance.

VIEWPOINT

AI FOR BHARAT: MAKING ARTIFICIAL INTELLIGENCE ACCESSIBLE BEYOND URBAN CENTERS

Atul Pandey, Director – IT & Digital Strategy, Bharat Network Group, highlights how Artificial Intelligence can become a catalyst for inclusive growth by empowering farmers, healthcare workers, students, entrepreneurs, and citizens across Bharat

Artificial Intelligence has become the defining technology of our era. Across boardrooms, enterprises, and smart cities, AI is transforming how organizations operate, innovate, and serve customers. Yet, the true potential of AI for India lies beyond metropolitan hubs and corporate campuses. It lies in its ability to empower farmers in remote villages, assist healthcare workers in underserved regions, support students learning in their native languages, and help small businesses compete in an increasingly digital economy.

India is home to over 1.4 billion people, with a significant population residing in rural and semi-urban areas. While digital adoption has accelerated dramatically over the last decade, a gap still exists between urban technology access and rural digital empowerment. Artificial Intelligence has the potential to bridge this gap and become a catalyst for inclusive growth.

The future of AI in India should not be limited to creating smarter enterprises; it should focus on creating a smarter nation.

Today, India stands at a unique crossroads. On one side, we are witnessing rapid advancements in AI, cloud computing, and digital ecosystems. On the other, millions of citizens continue to face challenges related to access, awareness, and affordability. Bridging this divide is not merely a technological objective—it is a national responsibility.

AI-Powered Agriculture: Empowering the Backbone of India

Agriculture remains one of India's largest economic sectors and supports millions of livelihoods. However, farmers continue to face challenges related to unpredictable weather, pest infestations, water scarcity, and fluctuating market prices.

Artificial Intelligence can transform agricultural practices by providing real-time insights and predictive recommendations. AI-driven systems can analyse weather patterns, assess soil conditions, predict crop diseases, and recommend optimal irrigation schedules. Through mobile applications, farmers can receive actionable guidance that helps improve productivity while reducing costs.

By combining AI with satellite imagery, IoT sensors, drones, and mobile connectivity, India can create a more resilient and sustainable agricultural ecosystem.

Practical Solutions for Agriculture

Some initiatives that can accelerate AI adoption in agriculture include:

- AI-based crop disease detection using smartphone cameras.
- Smart irrigation systems powered by weather and soil analytics.
- AI-enabled crop insurance claim assessment.
- Predictive market pricing platforms for farmers.
- Village-level digital agriculture advisory centres.
- Drone-assisted crop monitoring and yield forecasting.
- AI-powered water resource management systems.

By integrating AI with government schemes and local agricultural networks, farmers can make data-driven decisions without requiring advanced technical knowledge.


"The true success of Artificial Intelligence will not be measured by how many enterprises adopt it, but by how many lives it improves across Bharat."
ATUL PANDEY
DIRECTOR – IT & DIGITAL STRATEGY

"When AI helps a farmer protect a crop, it is not merely a technological achievement—it is an economic and social transformation."

Regional Language AI Assistants: Technology That Speaks Bharat

One of the biggest challenges in technology adoption across Bharat is language accessibility. While many digital solutions are designed primarily for English-speaking users, millions of Indians communicate in regional languages.

For AI to become truly inclusive, it must understand and communicate in the languages people use every day. Multilingual AI assistants can help citizens access government services, financial support, education, and essential information in their preferred language.

The future of AI in India is not just intelligent—it is multilingual.

Practical Solutions for Language Inclusion

Potential implementation ideas include:

- AI-powered citizen service assistants for government schemes.
- Voice-based banking and financial literacy platforms.
- AI helplines for farmers and small business owners.
- Local-language digital commerce assistants for rural entrepreneurs.
- Voice-enabled government service portals.
- AI-driven translation engines for education and governance.
- Conversational AI for public service delivery.

The next billion users of digital technology in India are more likely to interact through voice than keyboards. Therefore, voice-first AI ecosystems will play a critical role in bridging the digital divide.

Transforming Rural Healthcare Through AI Diagnostics

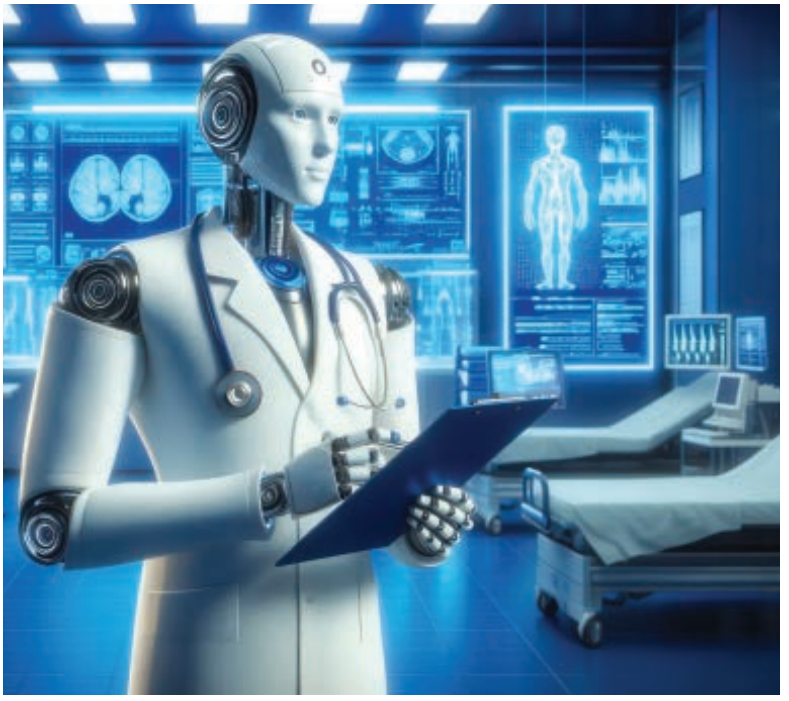
Access to quality healthcare remains a challenge in many rural regions. Shortages of specialists, limited medical infrastructure, and geographical barriers often prevent timely diagnosis and treatment.

Artificial Intelligence can help bridge this healthcare gap by enabling faster and more accurate diagnostics. AI-powered tools can assist healthcare workers in identifying diseases, analysing symptoms, and providing predictive health assessments. Combined with telemedicine, AI can bring healthcare expertise closer to underserved communities.

Practical Solutions for Healthcare

High-impact opportunities include:

- AI-assisted diagnosis for tuberculosis, diabetes, and cardiovascular diseases.
- Mobile health screening units equipped with AI tools.



- AI-powered maternal and child health monitoring systems.
- Telemedicine platforms integrated with diagnostic AI.
- Predictive healthcare analytics for disease outbreak monitoring.
- AI-enabled electronic health records for rural clinics.
- Remote specialist consultations powered by AI triage systems.

Primary Health Centres (PHCs) can become digital healthcare hubs by combining AI, telemedicine, and cloud-based patient records.

"Distance should never determine the quality of healthcare a citizen receives. AI gives us the opportunity to make expertise accessible, regardless of geography."

AI-Enabled Education: Unlocking Potential for Every Student

Education has long been recognized as the foundation of social and economic progress. Yet educational disparities continue to exist between urban and rural regions.

Artificial Intelligence can help create personalized learning experiences that adapt to individual student needs.

AI-powered educational platforms can identify learning gaps, recommend customized study plans, and provide instant feedback to students.

Teachers can also benefit from AI tools that assist with lesson planning, assessments, and performance tracking, enabling them to focus more on mentoring and student development.

Practical Solutions for Education

Key initiatives could include:

- Personalized AI tutors in regional languages.
- Smart classrooms with adaptive learning systems.
- AI-generated learning content for government schools.
- Teacher-assist platforms for lesson planning and assessments.

- Career guidance assistants for students in rural areas.
- AI-powered vocational training platforms.
- Digital skill development programs aligned with future job requirements.

AI can help ensure that every student has access to quality learning opportunities, regardless of location.

AI for Rural Entrepreneurship and Small Businesses

Small businesses, artisans, and entrepreneurs form the backbone of local economies. However, many struggle with limited market access, operational inefficiencies, and lack of digital expertise.

Artificial Intelligence can help level the playing field by enabling businesses to automate processes, improve customer engagement, forecast demand, and expand their market reach.

Practical Solutions for Small Businesses

AI can support entrepreneurs by:

- Automating customer support through AI chatbots.
- Predicting inventory requirements.
- Enabling digital marketing in regional languages.
- Supporting financial planning and cash flow management.
- Connecting local products to broader digital marketplaces.
- Providing AI-powered business advisory services.
- Facilitating customer insights and demand forecasting.

These capabilities can create new economic opportunities and accelerate rural economic development.

India's AI journey should not be defined by the intelligence of machines alone, but by the opportunities we create for every citizen through technology.

Building an Inclusive AI Future

The success of AI in India should not be measured solely by enterprise adoption or technological sophistication. It should be measured by its ability to improve lives, create opportunities, and empower communities.

Achieving this vision will require collaboration between government bodies, technology companies, educational institutions, startups, and local communities. Investments in digital infrastructure, affordable connectivity, digital literacy, and responsible AI governance must remain national priorities.

The goal is clear: AI should not be a privilege reserved for a few. It should be a tool that empowers every citizen.

Conclusion

India stands at a defining moment in its digital journey. Artificial Intelligence offers an opportunity not only to drive economic growth but also to build a more inclusive and equitable society.

As technology leaders, our responsibility extends beyond deploying innovative solutions within organizations. We must ensure that innovation reaches every village, every classroom, every healthcare centre, every entrepreneur, and every citizen striving to build a better future.

The real promise of AI for Bharat lies not in algorithms alone, but in its power to transform lives. When Artificial Intelligence becomes accessible to every Indian, regardless of geography, language, or economic background, we will move closer to realizing the vision of a truly Digital India.

The future of AI is not just about technology. It is about empowering people, strengthening communities, and creating opportunities for generations to come. And that future must belong to all of Bharat.

SPOTLIGHT

THE EVOLUTION OF SECURITY AND RISK MANAGEMENT

Sanjay Ambadkar, CISO, Bajaj Auto Ltd, shares his perspectives on how the cybersecurity landscape has evolved from traditional perimeter-based security to a Zero Trust mindset in an era defined by cloud, AI, connected vehicles, and borderless digital ecosystems

In manufacturing, things started with physical, and hence, the security too. You locked the gates. You badged the workers. You trusted the people inside the fence and worried about everyone outside it. When we started connecting our systems first internally, then cautiously to the outside world, we simply extended that same mental model. Draw a perimeter. Guard the gateways. Keep the threat outside. It felt logical. It felt safe.

We conveniently sometimes assume that we understand the depth of the internet, where our data lives, about who could reach our systems, and from where. In the era of CYOD and cloud and now AI, satellite internet, and connected vehicles the threats have no boundaries. We must accept now that the perimeter was finished as a concept. Trust cannot be assumed. It cannot be granted once and forgotten. It must be earned at every interaction, verified, re-verified, and never taken for granted simply because someone has the right badge or the right password. Now, we call this Zero Trust. But for me, it wasn't a framework that arrived with a name. It was a lesson that I learnt, and here's what surprised me most as the years went on: this shift from perimeter thinking to continuous verification. It wasn't just a technology shift. It was a business shift.

AI at machine speed: Balancing innovation with governance

I am sure AI excites all! I have watched it detect a threat in milliseconds that would have taken SOC's best analyst days to find. I have seen it surface patterns buried inside noise that no human being, working a full career, could have uncovered on their own. That is genuinely remarkable, and I will not pretend otherwise.

But I have also seen what happens when excitement outruns discipline. AI operates at machine speed. If you remove human judgment from the loop, if you let it act without governance, without guardrails, without someone asking hard questions, a single misclassification doesn't just cause a problem. It cascades. It becomes a catastrophe before the incident response team even knows something went wrong.

> **Where every person, at every level, from the shop floor to the boardroom, understood that they are part of the security chain**

My message is simple here and to every leader and security head deploying AI today is: govern it before you scale it because ungoverned AI is not innovation. It's risk wearing the costume of progress.

Turning data into business value through governance and accountability

In manufacturing, we generate data constantly. Machine telemetry, supply chain flows, production metrics, workforce records, customer contracts. structured & unstructured data, cross-border data that often have conflicting requirements and almost no clear legal precedence.

I am sure that the Legal Counsel, CIO, CISO, and DOP are all slowly realising that the boundaries between

their disciplines are dissolving. Dare to ask: Do you know what data you hold? not just "we have a lot of it." not just "it's stored here." Can you trace where & how it flows? Can you tell with confidence what business decision each dataset enables?

Data without governance is not an asset. It is expensive, regulated, and legally fraught, and security and privacy must walk together. In my experience, the organisations that treat them as separate conversations are the ones that learn this the hard way.

Building resilience through leadership, culture, and shared responsibility

After the breach, after the incident, after the recovery. I have noticed very smart people, surrounded by very expensive technology, ask the same question every time:

How did this happen? Do we still lack the right tool deployment?

In most of the scenarios, the answer is “No on technology. But a gap in awareness. A failure of communication. Someone who noticed something odd and didn't feel safe enough to raise it. A culture where security was IT's problem, and everybody else's exemption. When security stops being a department and starts becoming a shared responsibility, you don't just survive threats. You become genuinely harder to breach.

Preparing future leaders for a world of continuous disruption

The technology will keep changing. The threats will keep evolving. The threats will keep coming faster than the previous ones, and more complex than we can fully anticipate. But the organisations that endure are not the ones with the best tools alone. They are the ones where the culture changed, too. Where every person, at every level, from the shop floor to the boardroom, understood that they are part of the security chain. That is the wall that holds the threats!

BHARAT NETWORK GROUP™

Our Publications

The Founder, The Educator and The Banker—three insightful magazines—delivering expert perspectives on business and finance, education, banking and IT, to empower industry leaders and professionals

To Read our Digital Editions,

Log on to: www.bharatnetworkgroup.com

For Print Editions, Contact:

info@thefoundermedia.com

editor@thefoundermedia.com

UPCOMING EVENTS

CISO HORIZON 2026

OCTOBER | GUWAHATI

A 3-Day Residential Summit for 70+ India's Leading CISOs

FinVision AI Summit 2026 Guwahati

NOVEMBER

An Exclusive 3-Day Residential Summit for 70+ BFSI Leaders

An Initiative of BNG BHARAT™ NETWORK GROUP

Concept by Tech Disruptor media.com