

VOICE & DATA

Connecting the Digital World

CyberMedia

DIGITAL TRANSFORMATION HITS BUDGET REALITY

With spending under pressure, CIOs are cutting sprawl and forcing cloud, networks and platforms to prove value.

TELECOM
LEADERSHIP
FORUM

5G+

BEYOND THE 5G ROLLOUT,
THE AGE OF EXECUTION

58





APEEJAY SVRAN GLOBAL SCHOOL

Sector 21 D, Faridabad | Estd. in 2011 Under the aegis of Apeejay Education

Foundation for lifelong learning starts here

ADMISSIONS OPEN
FOR 2026-27
NURSERY TO CLASS IX & XI

Apply now for
attractive scholarships

Discount Available on Admission Fee



KEY HIGHLIGHTS



Value-based holistic education



Focus on experiential and
competency-based learning



Research-based curriculum



Safe & secure campus



State-of-the-art infrastructure
and learning beyond classroom



Excellent CBSE board and
competitive exam results

For admission enquiry, please contact:

Bakshi Marg, Sector 21 D, Faridabad, Haryana 121001

Admission Helpline Number:
8527-543-543

Follow us on:



When it comes to higher recall, **TRUST PRINT.**



That's the power of print. In addition to **70% higher recall**, according to neuroscience research it's proven that print content is **21% easier to understand** and more memorable than digital media. That is why, print content connects with our brain more efficiently and effectively. So, choose to read newspapers.

INS

THE INDIAN NEWSPAPER SOCIETY

EDITORIAL

MANAGING EDITOR: Thomas George
CONSULTING GROUP EDITOR: Ibrahim Ahmad
EDITOR: Shubhendu Parth
CONSULTING EDITOR: Pradeep Chakraborty
CONTRIBUTING EDITOR: Pratima Harigunani
ASSISTANT EDITOR: Ayushi Singh
CONTENT EXECUTIVE (Online): Punam Singh
SUB EDITOR: Manisha Sharma
SR. MANAGER DESIGN & COVER DESIGN: Vijay Chand
VICE PRESIDENT RESEARCH: Anil Chopra
MANAGER CYBERMEDIA LABS: Ashok K Pandey

LARGE BUSINESS CONVENTIONS & PROJECTS
CONFERENCE PRODUCER: Ajay Dhoundiyal

BUSINESS SOLUTIONS & SALES
VICE PRESIDENT - SALES & MARKETING: Aninda Sen
SR MANAGER: Ajay Dhoundiyal (North)
SR MANAGER: Sudhir Arora (North, East)
SR. MANAGER: Anita Swamy (South)

MARKETING & ALLIANCES
SR MANAGER: Ajay Dhoundiyal
ASSISTANT MANAGER: Mohd Atif Uddin

EVENTS, OPERATIONS & COMMERCIALS
SR. MANAGER, OPERATIONS: Ankit Parashar
CREATIVE DESIGN: Sunali
SR. MANAGER - ONLINE AD OPERATIONS: Suneetha B S
SR. MANAGER - COMMERCIAL & MIS: Ravi Kant Kumar
MANAGER - COMMERCIAL & ADMIN: Ashok Kumar

DISTRIBUTION & GROWTH:
GM - DISTRIBUTION & GROWTH: Prateek Malik
SR. MANAGER - INSTITUTIONAL SUBSCRIPTION: Sudhir Arora
SR. MANAGER - INSTITUTIONAL SUBSCRIPTION: C. Ramachandran (South)
SR. MANAGER - AUDIENCE GROWTH: Alok Saxena
EXECUTIVE - AUDIENCE SERVICE: Kusum Sharma
MANAGER - CREATIVE OPERATIONS: Suraj Singh
SOCIAL MEDIA EXECUTIVE: Amit Bhardwaj, Priyanshi Goyal
SEO TEAM: Neha Joshi, Chandan Kumar Pandey
PRESS CO-ORDINATOR: Rakesh Kumar Gupta

OUR OFFICES
GURGAON (CORPORATE OFFICE)
Cyber House
B-35 Sector-32, Gurgaon, Haryana - 122 003
Tel: 0124 - 4237517, Fax: 0124 - 2380694

BENGALURU
205-207, Shree Complex (Opposite RBANMS Ground)
#73, St John's Road, Bengaluru - 560 042
Tel: +91 (80) 4302 8412, Fax: +91 (80) 2530 7971

MUMBAI
INS tower, Office No. 326, Bandra Kurla Complex Road,
G Block BKC, Bandra East, Mumbai - 400051
Mobile: +91 99694 24024

INTERNATIONAL
Huson International Media
President, 1999, South Bascom Avenue, Suite 1000,
Campbell, CA95008, USA
Tel: +1-408-879 6666, Fax: +1-408-879 6669

Voice&Data is printed and published by Pradeep Gupta on behalf of Cyber Media (India) Ltd, D-74, Panchsheel Enclave, New Delhi - 110 017, and printed by him at M/s Archana Printers, D-127, Okhla Industrial Area, Phase-1, New Delhi 110020. Editor: Shubhendu Parth

For subscription queries, please email: subscriptions@cybermedia.co.in or send a WhatsApp message to 9289870545.

All Payments Favoring: CYBER MEDIA (INDIA) LTD
Distributors in India: IBH Books & Magazines Dist. Pvt. Ltd, Mumbai.
All rights reserved. No part of this publication be reproduced by any means without prior written permission from the publisher
Corporate Website: www.cybermedia.co.in
www.ciol.com (India's #1 IT Portal)

February 2026

[CONTENTS]

COVER STORY 20

DIGITAL TRANSFORMATION HITS BUDGET REALITY

With spending under pressure, CIOs are cutting sprawl and forcing cloud, networks and platforms to prove value.



INDUSTRY SPEAK

08 Telcos recast as AI-driven full-stack digital platforms

10 From systems to strategy: The enterprise infrastructure shift

14 Data as a product: Powering AI on the cloud

TRENDS

16 Enterprise AI infrastructure moves from hype to habit

18 Networks that think, data centres that grow

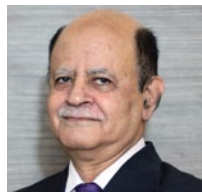
TECHNOLOGY

48 Intelligent fibre for distributed AI ecosystems

51 Secure SD-WAN: Foundation of a true SASE design

54 The flight deck layer for autonomous AI networks

TELECOM TALK



30 App-layer fraud: It is time for a stronger trust architecture

LT GEN DR SP KOCHHAR

PERSPECTIVE



34 Shopfloor change is now driven by data and intelligent networks

PRAVEEN ARORA

FOCUS

38 Five signals for India's digital infrastructure shift

ANALYSIS

42 From fiscal math to tech sovereignty strategy

USE CASE

45 Building real-time risk engines on telco networks

REPORT

58 Beyond the 5G rollout, the age of execution

66 Businesses rethink infrastructure as AI takes control

COMMENTARY

69 DPDPA vs GDPR: India's consent-only rules strain operations

72 Securing the digital stack at the silicon core

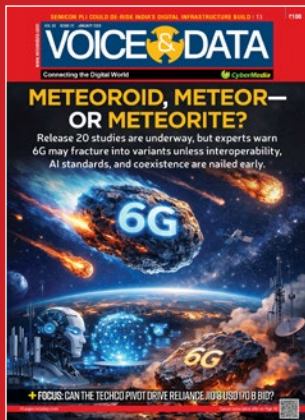
REGULARS

06 Voicemail

07 Opening Note

74 Postscript

[NEXT ISSUE]



JANUARY 2026

Scan QR Code
& Subscribe now...



SEND YOUR FEEDBACK FOR US
TO SERVE YOU BETTER...

For **subscription queries**, please email:
subscriptions@cybermedia.co.in or
send a WhatsApp message to **9289870545**.

You can also write to
Reader Service Executive, **VOICE&DATA**,
Cyber House, B-35 Sector 32,
Gurgaon-122 003, Haryana
Tel: 9953150474, 7993574118



Share your views at vndedit@cybermedia.co.in

NEXT
ISSUE

THE INDUSTRIAL IOT INFRASTRUCTURE STACK



For any query: ajaydh@cybermedia.co.in



SHUBHENDU
PARTH
[OPENING NOTE]

BSNL, Budget 2026–27, and what the numbers quietly signal

For the telecom sector, India's Budget 2026–27 brings the focus back on BSNL, primarily because of the scale of public funding routed through the Department of Telecommunications (DoT). At first glance, the numbers appear reassuring: a net outlay of Rs 73,990 crore, a push on capital expenditure, and continued emphasis on rural broadband and digital infrastructure. But a closer look at the allocations and the broader macro context raises questions about what this funding is designed to address—and what it does not.

A large share of the DoT outlay is effectively pre-committed. Around Rs 20,000 crore is earmarked for BharatNet, while more than Rs 17,000 crore flows through the Universal Service Obligation Fund. These allocations are meant to expand rural connectivity, meet coverage obligations, and compensate service providers for mandated rollouts. In this framework, BSNL is positioned less as a commercial challenger and more as a public infrastructure executor.

That positioning aligns with the Economic Survey 2025–26, which increasingly treats digital networks as future-ready public infrastructure, justified by economy-wide spillovers rather than near-term commercial returns. This explains why coverage and control are prioritised over profitability. But it also underlines a structural risk: infrastructure-led funding does not resolve the long-term economics of the telecom sector.

The numbers reinforce this concern. There are no dedicated allocations for 5G densification, enterprise or private 5G services, cloud-edge integration, or next-generation network platforms. DoT's R&D allocation stands at about Rs 400 crore, modest relative to ambitions around AI, data centres, and digital public infrastructure. Similarly, domestic industry incentives under DoT remain under Rs 2,000 crore, limiting their impact on export-oriented telecom equipment or advanced network IPs.

Revenue projections add another layer of caution. Despite higher public spending, telecom sector revenues are projected at around Rs 1.17 trillion in 2026–27, lower than the revised estimates for the current year. This suggests continued financial stress in the sector. The Economic Survey's discussion on India's high cost of capital further sharpens this point. Telecom, among the most capital-intensive sectors, continues to operate under high financing costs without relief on levies, spectrum pricing, or monetisation pathways.

In this context, optimism around BSNL must be interpreted carefully. The budget appears to be betting on BSNL primarily as an instrument of policy execution—particularly for rural broadband and sovereign infrastructure—rather than as a driver of sector-wide revival or innovation-led growth. That may be defensible from a public policy perspective, but it leaves unresolved questions about competitiveness and private investment incentives.

The message is clear: telecom is an essential infrastructure, assumed to scale alongside data centres, AI platforms, and digital services. But without integration into these growth engines—and without addressing the sector's structural economics—there is a risk that networks remain foundational yet financially constrained. The challenge for policy, therefore, is not merely to fund connectivity, but to align telecom execution with India's broader digital, export, and productivity ambitions.

shubhendup@cybermedia.co.in

Telcos recast as AI-driven full-stack digital platforms

TSPs in India are expanding beyond connectivity, bundling cloud, OTT and analytics to deepen user engagement, strengthen retention and lift revenue metrics.



BY PEEYUSH VAISH

Telecom operators (telcos) in India are moving beyond connectivity and repositioning themselves as AI-ready digital platforms, intensifying competition not only within the sector but also with hyperscalers and IT services firms in managed AI, data and security.

A major telecom company in India has announced what it describes as the world's first Gen-AI collaboration, offering bundled benefits to eligible customers. At the same time, another operator is pursuing a data-driven freemium

strategy built around its own cloud and AI services, curated OTT content—particularly live sports—and 5G expansion to deepen engagement across digital touchpoints.

The telecom market in India, long characterised as an oligopoly, is undergoing strategic realignment. As operators embed themselves more deeply in consumers' digital lives, the emphasis on voice and data tariffs is diminishing. In its place is a broader portfolio of digital products and services designed to extend customer relationships beyond basic connectivity.

The SIM is no longer the endpoint but the gateway to a layered digital stack built on cloud, AI tools and sustained engagement across user journeys.

Investor confidence signals belief that telecom networks can distribute, scale and monetise AI, cloud and data services beyond connectivity.

FROM CONNECTIVITY TO PLATFORM ECOSYSTEMS

A central feature of this shift is the transformation of telecom services into platform-based ecosystems. Operators are deploying freemium models that bundle free cloud storage, OTT subscriptions and other digital services to drive adoption. While such incentives may initially appear to be cash burn, they represent a long-term strategy to secure customer loyalty as the ecosystem matures.

By integrating additional services into core plans, operators reduce churn risk as tariffs rise and encourage customers to adopt technologies such as 5G and cloud-enabled applications. Free or bundled services function as low-risk engagement tools, keeping users within the operator's digital environment.

Freemium strategies, combined with consolidated entertainment offerings, aim to increase subscriber stickiness and maximise lifetime value. The objective is sustained engagement, lower churn and higher average revenue per user (ARPU).

According to the TRAI FY2025 report for the year ended March, ARPU rose 19% year on year from Rs 153.54 in FY24 to Rs 182.95 in FY25, supported in part by bundled and differentiated offerings. By extending beyond network quality and speed, operators are signalling a shift towards platform-led service ecosystems.

Integrating connectivity with a full-stack digital suite—spanning entertainment, cloud and AI—enhances the value proposition and strengthens long-term loyalty. Customers are no longer tied solely to a SIM card but to an interconnected portfolio of services, reinforcing a digital-first ecosystem in India's evolving telecom landscape.

COMPETITIVE ADJACENCY AND DATA MONETISATION

This transition places telecom operators in direct competitive adjacency with traditional IT and digital service firms. As they expand into managed AI, cloud and cyber-security, telcos are entering domains once dominated by technology integrators and hyperscalers.

The market appears to recognise this shift. In at least one case, a telecom operator's market capitalisation has surpassed that of several large-cap IT firms. Investors are pricing in expectations that telecom companies can unlock multi-channel growth by leveraging their customer base, network assets and data capabilities.

This divergence also reflects broader dynamics in India's digital economy. While telecom operators benefit from rising data consumption and platform integration, segments of the IT services industry are contending with global economic pressures and technology-driven restructuring.

At the core of the telecom pivot is data. As customers engage with entertainment, cloud storage, and AI-driven tools, operators accumulate behavioural insights that can be analysed to enable personalised upselling and cross-selling. Premium applications and differentiated tools are positioned to encourage migration to higher-tier plans.

Such integration enables telecom companies to operate as digital ecosystem providers rather than pure-play connectivity vendors. By combining network services with AI, cloud and other digital offerings, they create multiple monetisation levers across the customer lifecycle.

Aggregating usage data across services enables targeted marketing and tailored plan design. Personalised offers based on consumption patterns, layered on top of connectivity, strengthen the commercial model. At the same time, the depth of integration raises barriers to entry for new competitors. As more services are bundled into a single platform, switching providers becomes less straightforward for consumers, giving established players structural advantages.

India's telecom operators are evolving to redefine their role in the digital economy. By shedding their pure-play connectivity skin and transitioning to AI- and cloud-driven platforms, they are seeking to anchor themselves at the centre of the country's digital transformation. 🌟

The author is a Partner & TMT Industry Leader at Deloitte India.

feedbackvnd@cybermedia.co.in



From systems to strategy: The enterprise infrastructure shift

As hybrid work, data growth, and cyber risk converge, enterprises are re-architecting digital infrastructure to gain agility, resilience, and regulatory confidence.



BY PRAKASH KUMAR

In today's digital-first environment, information technology (IT) has shifted from a support role to a core enabler of enterprise transformation. It no longer functions solely to maintain systems but is now central to how businesses in India and the Asia-Pacific region drive operational efficiency, user experience, and long-term competitiveness. Modern IT systems underpin infrastructure for collaboration, ensure continuity in hybrid environments, and provide the foundation for data-led decision-making.

The growth of hybrid work and globally distributed teams has changed how organisations plan and invest

in IT infrastructure. In India, the adoption of hybrid work models has grown significantly post-pandemic, requiring enterprises to support secure, seamless access to systems and data from anywhere. A 2023 Nasscom report noted that nearly 70% of Indian enterprises are investing in technologies that enable hybrid operations.

To meet these evolving requirements, organisations are deploying scalable digital infrastructure, including cloud platforms, virtual collaboration environments, and remote access systems. These capabilities help ensure business continuity and real-time collaboration

Infrastructure decisions are no longer technical choices alone; they now shape how enterprises manage risk, scale innovation, and compete globally.

As data volumes surge, the real differentiator lies not in collection but in how securely and responsibly enterprises manage and integrate information.

while maintaining flexibility for future growth. They also support data integration across locations, helping enterprises maintain consistency and responsiveness across business units.

DATA INFRASTRUCTURE AS A STRATEGIC ASSET

As businesses scale and digital adoption increases, the volume of data being generated across platforms, systems, and devices is expanding rapidly. In India, where the digital economy is expected to reach USD 1 trillion by 2025, data has become central to enterprise value creation. When integrated effectively, enterprise data can improve workflows, support analytics, and inform strategic decisions.

However, infrastructure challenges around data governance, security, and compliance are also growing. For instance, India's Personal Data Protection Bill outlines regulatory expectations for data use, privacy, and transparency. Enterprises must balance the need to extract value from data with the responsibility of managing it securely and ethically.

This has led to increased investment in data platforms, storage systems, and advanced analytics tools that can process information efficiently and securely. By establishing clear data management frameworks, businesses are positioning themselves to comply with evolving regulations while leveraging insights to remain agile in competitive markets.

CYBERSECURITY EMBEDDED IN INFRASTRUCTURE DESIGN

As digital infrastructure grows more complex, cybersecurity has become a critical design principle rather than an afterthought. With increased exposure to Internet-based threats, businesses in India and the broader Asia-Pacific region face a rising number of cyber incidents. According to a 2023 Gartner report, cyberattacks in the region have increased by 30% year-on-year, with India among the more frequently targeted markets.

To reduce this risk, enterprises are embedding security within infrastructure architecture—building it into networks, systems, and endpoints. This includes



IN BRIEF

- IT infrastructure has moved from back-office support to a strategic layer that enables enterprise agility, resilience, and long-term competitiveness.
- Hybrid work has accelerated demand for secure, scalable access to systems, driving investments in cloud, collaboration, and remote access platforms.
- Data infrastructure is now a core enterprise asset, requiring stronger governance, security, and compliance frameworks.
- Cybersecurity is being embedded into infrastructure design, shifting from reactive controls to proactive, architecture-led defence models.
- Cloud-native and modular infrastructure is helping enterprises scale faster, avoid legacy bottlenecks, and respond to shifting market demands.
- India's Global Capability Centres are emerging as global hubs for cloud operations, cybersecurity, and infrastructure automation at scale.

proactive risk assessments, access controls, and layered defence models. Infrastructure teams are also incorporating secure cloud configurations and regularly updating systems to close known vulnerabilities.

Cyber resilience is increasingly determined by design choices made early in infrastructure planning, not just by tools added after deployment.

Additionally, user education is emerging as a key part of the security framework. With many breaches resulting from misconfigurations or human error, enterprises are strengthening internal protocols and awareness initiatives to build a more resilient digital environment.

INFRASTRUCTURE SCALABILITY AND BUSINESS AGILITY

Enterprises are increasingly prioritising scalable infrastructure that can adapt to evolving business needs. Whether expanding to new markets, onboarding digital services, or supporting growing user bases, scalability has become critical to business resilience. Without it, legacy systems often become bottlenecks that slow innovation and responsiveness.

In India, the rapid expansion of digital-native sectors such as fintech and e-commerce has underscored the need for cloud-native infrastructure that can scale quickly without compromising performance or security. A recent IDC study highlighted that 60% of Indian enterprises are using cloud technologies to improve scalability and drive transformation.

Infrastructure modularity—enabled through microservices, containers, and API-led integration—is also gaining traction. These systems allow enterprises to scale parts of their infrastructure independently, enabling faster rollouts and improved resource efficiency.

GLOBAL CAPABILITY CENTRES AND DIGITAL INFRASTRUCTURE

Global Capability Centres (GCCs) in India are increasingly playing a pivotal role in shaping enterprise IT infrastructure strategy. The Asia-Pacific region accounts for over 40% of the world's GCCs, according to Nasscom, with India emerging as a key location for infrastructure-centric operations.

Many multinational organisations use their Indian GCCs to manage large-scale cloud environments, cybersecurity operations, and data platforms. These centres act as central hubs for building standardised infrastructure practices across global regions, supporting resilience and performance in distributed enterprise setups.

In several cases, GCCs are leading infrastructure automation efforts, driving adoption of DevOps and Site Reliability Engineering (SRE) models, and building capabilities in AI-driven operations management. Their growing role in developing and maintaining digital infrastructure is contributing to more consistent service delivery and improved operational metrics across the enterprise.

INFRASTRUCTURE PRIORITIES FOR THE FUTURE

As the business environment continues to evolve, enterprise IT priorities are being recalibrated around three pillars: connectivity, data management, and cybersecurity. These areas will define how infrastructure is designed, deployed, and operated in the coming years.

Reliable connectivity remains fundamental—especially with the spread of hybrid work and multi-cloud strategies. Data infrastructure will continue to require investment in integration, storage, and governance frameworks to keep pace with regulatory requirements and business needs. Meanwhile, cybersecurity will need to evolve alongside threat vectors, requiring adaptive systems and continuous monitoring capabilities.

The challenge for IT leaders lies in building an infrastructure that is not only scalable and secure but also agile enough to support innovation. Investments in cloud platforms, network optimisation, and infrastructure automation are expected to drive enterprise competitiveness and enable sustainable growth.

By aligning infrastructure priorities with strategic goals, enterprises can create resilient environments that support digital transformation, manage risks, and respond effectively to new opportunities. The next wave of IT infrastructure will not only support current operations but will also serve as a foundation for future-ready enterprises. 🌟

*The author is the Head of Corporate IT of
ZEISS India.*

feedbackvnd@cybermedia.co.in



7th Edition
TELECOM LEADERSHIP FORUM
5G+

DIGITAL INFRASTRUCTURE FOR VIKSIT BHARAT

15 January 2026 New Delhi

HEARTFELT THANKS TO EVERYONE WHO MADE THE VOICE&DATA 5G+ CONFERENCE A REMARKABLE SUCCESS

**Full Day Conference | 5 Sessions | 5 Keynotes & Fireside Chat
30+ Speakers | 110+ Attendees | 50K Engagements**



Partners

Gold
NOKIA

Associate
brother
at your side

Academia
APEEJAY EDUCATION
SOARING HIGH IS MY NATURE

Research
CMR
Insights powered by research

Media
DATAQUEST

Supporting Partners



For information on upcoming events, please write to:
Mohd Aif | Assistant Manager - Marketing | Email: atifu@cybermedia.co.in | Mobile: +91 83086 21705

Data as a product: Powering AI on the cloud

Fragmented data architectures limit AI scale and decision velocity, making structured, governed infrastructure essential for sustained enterprise growth.



BY NIRAJ KUMAR

Nearly 402.74 million terabytes of data are generated every day. For businesses, this constant stream is more than just digital exhaust—it is a critical resource. But most of it remains unused: scattered, siloed, and invisible. A 2024 study by IBM IBV shows that 67% of CFOs believe their C-suite has the data necessary to capitalise on new technologies. Still, only 29% of tech leaders strongly agree that their data meets quality, accessibility, and security standards. This gap between available and usable data limits organisations' ability to scale generative AI effectively, exposing a critical divide between potential and actionable insights.

This is where the Data-as-a-Product (DaaP) becomes essential. By treating data as a managed, reliable product, organisations can standardise, validate, and connect datasets, turning raw information into intelligence that guides strategy, anticipates market shifts, and strengthens competitive advantage.

Cloud platforms are the backbone of this transformation, unifying dispersed data, providing the analytical power necessary for timely insights, and enabling faster, smarter decision-making. This structured approach turns abstract data into tangible assets, laying the foundation for organisations to systematically harness information and convert it into measurable business value.

TRANSFORMING DATA INTO STRATEGIC ASSETS

Organisations are increasingly recognising that data is not just a byproduct of operations but an asset that drives decisions, strategy, and competitive advantage. Each dataset is assigned clear ownership, quality standards, and performance metrics, ensuring insights are reliable, timely, and aligned with organisational goals. Cloud platforms amplify these benefits, centralising data, securing access, and integrating seamlessly with analytics tools, transforming fragmented information into actionable intelligence.

Only a fraction of enterprise data meets the quality, accessibility and governance standards required to scale generative AI systems reliably and responsibly

For example, a large grocery retailer modernised its data infrastructure by migrating hundreds of complex and near-real-time data pipelines to a unified cloud environment. This streamlined data ingestion, reduced latency, and improved data quality. While runtime improved by over 40%, costs dropped by more than 30%, and overall efficiency increased across analytics and reporting. With real-time insights, teams can optimise inventory, personalise customer experiences, and make faster, data-driven decisions.

DRIVING OPERATIONAL AGILITY AND INNOVATION

Treating data as a product also enables organisations to respond to change with speed and confidence. Verified, standardised datasets allow teams across departments to collaborate more effectively, reduce duplication, and experiment faster. This agility accelerates product development, shortens decision cycles, and positions companies to act ahead of competitors.

AI and automation further extend these advantages. Continuous data analysis helps enterprises anticipate bottlenecks, identify emerging risks, and optimise resources in near-real time. For instance, AI-enabled predictive maintenance can reduce maintenance costs by up to 30% and unplanned downtime by 45%. As systems learn and adapt, businesses can make faster, smarter decisions, turning data into a measurable source of competitive intelligence and strategic differentiation.

ENHANCING TRUST THROUGH DATA GOVERNANCE

As data becomes a strategic asset, trust and accountability are critical. Organisations must ensure that insights are accurate, transparent, and compliant with regulations such as the GDPR in Europe and India's DPDP Act, thereby building confidence among customers, regulators, and partners. The evolving threat landscape also makes strong governance essential.

Sophisticated attacks now bypass traditional defences. The CrowdStrike 2025 Global Threat Report shows that 79% of detections in 2024 were malware-free, and some breaches can occur in as little as 51 seconds. More than half of vulnerabilities were linked to initial access attacks exploiting weak identity and access controls, underscoring the need for proactive, structured data management.

To mitigate these risks while fostering innovation, organisations can use anonymised synthetic datasets to test AI models safely. Cloud platforms reinforce trust by centralising security policies, automating compliance, and enabling real-time audits. Together, these measures safeguard operations and ensure insights remain reliable, unlocking the full strategic potential of Data-as-a-Product.

CHALLENGES IN REALISING DATA AS A PRODUCT

Despite its benefits, adopting DaaP comes with organisational and cultural challenges. Teams may hesitate to share data or adopt new workflows, slowing collaboration and innovation. Clear ownership, communication, and change management are critical to effectively embedding DaaP principles.

Data literacy is another hurdle, as employees across roles may struggle to interpret insights without intuitive tools, training, and support. Technical complexity can also arise when scaling infrastructure or integrating diverse datasets, requiring careful planning and optimisation. Organisations that address these hurdles cultivate a culture where data drives decisions, ensuring operational efficiency, agility, and trust, while maximising strategic value.

Data-as-a-Product transforms how organisations harness information. Managing datasets with precision allows businesses to uncover trends, customer preferences, and market opportunities in real time. Cloud platforms provide the scale, connectivity, and analytics needed to turn fragmented data into coherent intelligence. This approach enables faster experimentation, informed risk-taking, and proactive strategy adjustments, creating a clear edge in dynamic markets.

Beyond operational gains, DaaP fosters a culture where data can drive decisions and fuel innovation. Organisations that embed this mindset can anticipate shifts, respond decisively, and translate raw information into measurable strategic impact. 🌟

The author is the Chief Technology Officer of Onix.

feedbackvnd@cybermedia.co.in



Enterprise AI infrastructure moves from hype to habit

In 2026, enterprises will succeed not by scaling models, but by embedding governed, domain-aware AI agents into core workflows.



BY NICK EAYRS

Artificial Intelligence (AI) has reached a point where it can meaningfully accelerate enterprise productivity. The central challenge for organisations is no longer gaining access to more powerful models, but refining and deploying AI in ways that reliably automate routine, time-consuming work. Done well, this frees teams to focus on higher-value, creative and strategic tasks.

Closing the gap between AI's potential and its reliability will define 2026. Rather than chasing ever-larger models, enterprises are beginning to demand smarter, contextual systems that align closely with their specific needs.

Six shifts are emerging as critical: building agents that reason over proprietary data, operate collaboratively, are evaluated continuously, work across modalities, integrate seamlessly into workflows, and are supported by a workforce trained to work alongside them.

FROM GENERALISED TO DOMAIN-SPECIFIC AI AGENTS

General-purpose models trained on public internet data often struggle with the complexity of enterprise environments. They lack deep organisational context and are poorly suited to navigating internal processes, exceptions and compliance requirements. At the same time, enterprises face growing expectations around data and AI sovereignty, driven by regulatory, geopolitical and privacy considerations.

Domain-specific agents, grounded in proprietary data with governed lineage, are better equipped to interpret internal rules, edge cases and regulatory constraints. They also support sovereignty requirements by ensuring data privacy, security and jurisdictional compliance. This level of control reduces risk, meets legal and ethical obligations and helps preserve competitive advantage.

Examples from industry show that organisations focusing on data quality, domain depth and governance achieve better outcomes than those prioritising model size alone. The direction of travel is clear: success in the next phase of AI adoption will depend less on scale and more on secure integration, robust governance and contextual understanding.

FROM SINGLE AGENTS TO MULTI-AGENT ORCHESTRATION

Enterprise workflows are rarely linear, and AI systems must reflect that reality. Real-world processes typically involve multiple stages, including data retrieval, validation, approvals and decision-making across different systems and teams. These workflows exceed what a single agent can handle reliably.

Multi-agent orchestration addresses this complexity by assigning specialised agents to discrete tasks such as compliance checks, reasoning or data access, while a supervising agent coordinates their activity. This supervisory layer sequences tasks, delegates responsibilities and synthesises outputs in natural language, enabling AI systems to operate at scale within governed, auditable and adaptable workflows.

FROM ONE-OFF TESTING TO CONTINUOUS EVALUATION

As AI systems move into production, continuous evaluation becomes essential. Models that perform well during development often degrade when exposed to live data or shifting conditions. Without ongoing assessment, reliability can erode quickly.

In response, enterprises are adopting evaluation-centric practices, where AI agents are measured continuously against real tasks, real feedback and changing operational environments. This approach allows organisations to detect drift early, reduce uncertainty and improve performance over time. Continuous evaluation also enables AI systems to learn from outcomes, ensuring they adapt more closely to enterprise requirements.

FROM TEXT-BASED AI TO MULTIMODALITY

AI has historically been text-first, but enterprise communication increasingly spans voice, video, images, sensor data and messaging platforms. Multimodal AI reflects this reality by combining and interpreting diverse inputs, significantly expanding the scope of automation.

In practice, multimodal systems augment human interpretation at scale. In customer service, AI can

analyse written queries, tone of voice and visual evidence simultaneously. In healthcare, models can combine patient records, medical images and sensor data to support diagnosis and treatment decisions. In retail and e-commerce, multimodal agents can process reviews, images and usage videos to better understand customer preferences and identify fraud.

FROM VISIBLE FEATURES TO INVISIBLE INTEGRATION

The most effective AI systems do not demand attention. Instead, they are embedded seamlessly into workflows, improving productivity without adding friction. This “invisible AI” becomes part of the operating environment rather than a tool employees must consciously engage with.

When AI is integrated in this way and evaluated continuously, collaboration between humans and machines becomes more natural. Productivity gains follow not from novelty, but from consistency, reliability and ease of use.

SUSTAINED FOCUS ON SKILLS AND CAPABILITY

As AI agents become embedded in daily operations, organisations must continue investing in people. This means equipping employees not only to build AI systems, but to manage, guide and collaborate with them.

Crucially, benefiting from AI does not require deep technical expertise. A marketer automating reporting tasks, for example, primarily needs skills in prompting, workflow design and oversight. Developing these capabilities across the workforce will be essential to realising AI’s full value.

2026: WHEN AI TRULY UNDERSTANDS THE BUSINESS

Taken together, these six shifts redefine enterprise AI adoption. Domain-specific and sovereign agents make AI business-aware; orchestration, continuous evaluation and multimodality make it dependable at scale; and invisible integration combined with skills development ensures it fits naturally into everyday work.

The organisations that succeed in 2026 will not be those deploying the largest models, but those that build strong data and AI governance, treat domain-aware agents as trusted collaborators, and continuously evolve how people and systems learn from one another. 🧠

The author is the Vice President, Field Engineering for Asia Pacific and Japan at Databricks.

feedbackvnd@cybermedia.co.in



Networks that think, data centres that grow

AI, autonomous networking, and embedded security are turning data centre infrastructure into a self-learning system, driving growth and resilience.



BY RANGANATH SADASIVA

The data centre is set to undergo a structural shift in 2026, evolving from a backend facility into an intelligent, self-optimising platform powered by AI, high-performance networking, and autonomous operations. Rather than serving as passive compute environments, data centres will function as adaptive systems that directly influence enterprise growth and competitive positioning.

What was once treated as backend infrastructure overhead will now operate as a programmable learning environment. Autonomous Ethernet networks will predict and adapt in real time. Edge deployments will mature into powerful “micro-hyperscalers”, with capabilities previously associated with large cloud providers. Security will be embedded directly into the network fabric. The

result is a move away from cost-centre thinking towards infrastructure as a measurable source of advantage.

Here are five developments that will define intelligent data centres in the year ahead.

#1 AI-NATIVE DATA CENTRES REDEFINE OPERATIONS

“AI-native” will replace “cloud-native” as the dominant architectural principle. Functions ranging from workload placement to cable diagnostics will be AI-assisted. The data centre will operate as a closed-loop system, anticipating failures, tuning performance, and optimising energy consumption in coordination with utilities. Manual intervention will decline as predictive systems assume operational control with increasing precision.

Manual configuration will give way to intent-driven orchestration as networks learn, adapt, and correct without human intervention.



IN BRIEF

- AI-native design will replace cloud-native design, with closed-loop systems that predict faults and automatically tune workloads and energy use.
- Edge facilities will evolve into micro-hyperscalers, running high-bandwidth AI workloads closer to users and regulation zones.
- Ethernet-based AI fabrics will displace proprietary interconnects as models scale and open up, and as high-performance networking gains traction.
- Switch ASICs with embedded telemetry will enable self-optimising fabrics that manage congestion, power, and microbursts in real time.
- Security will be built into the fabric, with hardware identities, micro-segmentation, and encrypted east-west traffic as defaults.
- Infrastructure will shift from a cost overhead to a strategic asset, shaping innovation, resilience, and competitive positioning.

#2 EDGE AND AI CONVERGE INTO THE MICRO-HYPERSCALER

The edge data centre will resemble a scaled-down hyperscale campus rather than a telecom room. With 400G and 800G Ethernet, AI inference accelerators, and autonomous management, regional facilities will process workloads traditionally handled in centralised clouds. Cities, retailers, and universities will operate their own

micro-hyperscalers to meet regulatory requirements, address latency constraints, and achieve resilience objectives. The edge will shift from a support function to a revenue enabler, directly contributing to service innovation and user experience.

#3 THE AI FABRIC TAKES CENTRE STAGE

Network fabric design will move to the core of data centre architecture. As trillion-parameter AI models scale, Ethernet is expected to displace proprietary interconnects in large-scale AI environments, driven by demand for open, interoperable high-performance fabrics. The emphasis will move from discrete “AI clusters” to integrated “AI fabrics” that are adaptive and application-aware across the entire network path.

#4 ETHERNET MOVES TOWARDS AUTONOMY

Ethernet will incorporate embedded AI telemetry within switch ASICs to optimise congestion control, manage microbursts, and improve power efficiency. The ambition of intent-based networking will advance as fabrics gain the ability to learn, predict, and self-correct in real time. Command-line configuration will give way to automated orchestration and continuous optimisation.

#5 SECURITY BECOMES NATIVE TO THE FABRIC

Network security will no longer be bolted on; it will be built into the fabric itself. Every packet, port, and process will carry its own trust score, verified by distributed AI engines that detect anomalies at line rate. Hardware-rooted identities, continuous micro-segmentation, and encrypted east-west traffic will make the “zero trust data centre” more than a slogan; it will be the default blueprint. Attackers will have to breach physics, not just firewalls.

Together, these advancements indicate a transition from infrastructure management to infrastructure intelligence. As AI, networking, and security converge within the fabric itself, the data centre will no longer host applications; it will shape how enterprises compete, innovate, and scale in a digital economy defined by speed, data, and automation. 🧩

The author is the CTO of HPE India.

feedbackvnd@cybermedia.co.in



[COVER STORY]
INFRASTRUCTURE

DIGITAL TRANSFORMATION HITS BUDGET REALITY



As spending tightens, CIOs are cutting sprawl and proving value fast—turning cloud, networks, and platforms into disciplined systems built to perform.

BY SHUBHENDU PARTH

In 2026, digital transformation is no longer defined by how much an organisation spends, but by how intelligently businesses use their digital infrastructure. What is increasingly under scrutiny is not digital ambition, but digital justification—how every rupee spent translates into resilience, efficiency, or measurable business outcomes.

After nearly a decade of aggressive modernisation, marked by cloud migration, automation initiatives, platform expansion, and early-stage AI deployments—organisations are entering a phase of recalibration. Budgets are becoming tighter, scrutiny is sharper, and boards are asking harder questions about outcomes.

This shift does not signal a retreat from digital ambition. Instead, it reflects a maturing mindset—

one that treats digital infrastructure as an economic system rather than a technology stack. Cloud platforms, networks, security frameworks, data estates, and operational tools are being evaluated not in isolation, but in terms of how they reduce waste, improve resilience, and deliver measurable returns within six to twelve months.

The implicit question for CIOs is no longer “What should we modernise?” but “What must work without failure?”

Across sectors, CIOs and technology leaders are moving away from transformation as aspiration and towards transformation as execution discipline. The emphasis is now on cutting complexity, extracting value from existing infrastructure, and funding only those initiatives that can demonstrate near-term impact—while

The most critical infrastructure question has shifted from what to modernise to what must never fail under financial and operational pressure.



“Network upgrades today are justified by reliability and operational efficiency, with enterprises prioritising uptime and resilience over pure capacity expansion.”

PANKAJ MALIK

CEO & Director, Invenia-STL Networks



IN BRIEF

- In 2026, digital transformation is being judged by outcomes, with infrastructure spend tied to resilience, efficiency, and near-term business impact.
- Enterprises are shifting from parallel modernisation efforts to sequenced execution, prioritising initiatives that deliver measurable value in 6–12 months.
- Cloud economics are under board scrutiny as cost leakage from over-provisioning and tool sprawl forces stronger governance and accountability.
- Observability, automation, and consolidation are now framed as cost-control levers rather than optional resilience enhancements.
- Lean infrastructure strategies focus on optimisation and utilisation gains instead of capacity expansion or disruptive rip-and-replace programmes.
- AI investments are being sequenced behind data, governance, and operational maturity to avoid cost inflation and execution risk.

continuing to protect non-negotiables such as uptime, compliance, and readiness for AI.

“In a constrained capital environment, the biggest risk is not under-investing in digital transformation, but investing without strategic clarity. Enterprises protect ROI when they prioritise need-first initiatives that remain valuable even if the technology stack changes,” says Pankaj Malik, Chief Executive Officer and Whole Time Director, Invenia-STL Networks.

FROM EXPANSION TO EXECUTION DISCIPLINE

The defining shift in 2026 is managerial rather than technological. For much of the past decade, enterprises pursued transformation through parallel initiatives—cloud migration alongside application modernisation, automation layered on legacy processes, and new security tools added in response to emerging threats.

Under tighter budgets, however, that model is proving unsustainable. The cost is no longer abstract; it shows up as operational drag, governance gaps, and delayed decision-making.

According to Siddharth Tipnish, Partner, Deloitte India, enterprises are fundamentally rethinking how transformation programmes are sequenced and governed. “The focus has shifted from running multiple initiatives in parallel to prioritising those that demonstrate measurable business value within six to twelve months,” Tipnish says.

Cloud strategy sits at the centre of this recalibration. Early assumptions that elasticity would automatically translate into efficiency are being challenged as organisations confront persistent cost leakage from over-provisioned compute, idle storage, and duplicated tooling. Cloud is no longer treated as an open-ended platform for experimentation, but as an operating environment that must justify its unit economics—cost per application, transaction, or workload.



“In a constrained year, ROI breaks when operations scale linearly; winners codify service delivery into software, enabling outcomes to scale without adding headcount.”

RAJIV SHESH

Chief Revenue Officer, HCLSoftware

ENTERPRISE SPENDING PRIORITIES

As budgets tighten in 2026, CIOs are not resorting to across-the-board cuts. Instead, they are making deliberate trade-offs—trimming areas that inflate cost or complexity, while ringfencing investments that protect business continuity and future readiness.

What CIOs are scaling back?

- **Overlapping tools and platforms:** Multiple point solutions added over time—especially across monitoring, security, and automation—are being consolidated to reduce licensing, integration, and operational overheads.
- **Poorly governed cloud consumption:** Always-on capacity, idle workloads, and loosely owned cloud resources are being aggressively right-sized or shut down as cost visibility improves.
- **Manual-heavy operations:** Processes that rely on repetitive human intervention—incident handling, reporting, routine maintenance—are being automated or eliminated to reduce operating cost.
- **Parallel transformation programmes:** Large initiatives running simultaneously across cloud, data, applications, and security are being sequenced or paused, particularly if they lack near-term impact.

What CIOs continue to protect?

- **Resilience and availability:** Infrastructure that reduces downtime, improves MTTR, or strengthens business continuity remains non-negotiable, especially in regulated or high-availability environments.
- **Security and compliance foundations:** Spend that improves exposure visibility, audit readiness, and risk prioritisation is being preserved, even as tool sprawl is reduced.
- **Data and AI readiness:** While headline AI deployments may be phased, investments in data quality, governance, and automation continue, ensuring future capabilities can be adopted without rework.

In many organisations, failure to do so is now a board-level concern rather than an IT optimisation issue. This has elevated financial governance from a support function to a core pillar of digital infrastructure planning. FinOps, once confined to cloud teams, is now embedded into enterprise decision-making, with consumption visibility and accountability becoming as important as capacity planning itself.

The same discipline is reshaping transformation roadmaps more broadly. Anurag Agrawal, Business Head – Americas, To The New, observes that budget pressure has made prioritisation unavoidable. “If an initiative cannot show operational or financial impact in the near term, it is being re-scoped or deferred,” Agrawal says. Transformation is still progressing—but it is being sequenced rather than scattered.



“Enterprises are narrowing focus, backing initiatives that show business value quickly instead of running multiple transformation tracks in parallel under tighter budgets.”

SIDDHARTH TIPNISH

Partner, Deloitte India

“In a constrained year, transformation has to shift from ambition-led to outcome-led. The winners are not the ones doing more projects, but the ones making every initiative measurable, governable, and easier to run,” says Rajiv Shesh, Chief Revenue Officer, HCLSoftware.

WHERE BUDGETS LEAK FIRST AND FAST

As enterprises scrutinise digital spending, a clearer picture is emerging of where transformation budgets erode fastest.

Contrary to popular belief, the biggest leaks are rarely caused by large, headline investments. Instead, they stem from accumulated inefficiencies—tool sprawl, manual operations, and poorly governed infrastructure environments that quietly inflate operating costs over time. Left unaddressed, these inefficiencies compound, turning operational friction into structural cost.

“Cost leaks in digital infrastructure are rarely dramatic, but relentlessly cumulative. Organisations that unlock savings fastest institutionalise cost optimisation as an architectural discipline—designing infrastructure that is elastic, observable, and continuously aligned to real business demand,” Malik adds.

Platform proliferation is one of the most persistent sources of waste. Over the past few years, many organisations added new tools across monitoring, security, testing, and automation in response to growing

complexity. While each addressed a specific gap, the cumulative effect has been fragmented environments that are expensive to maintain and difficult to optimise.

Michael Raj, Executive Vice President – Cloud, Infrastructure, Security and Testing, Birlasoft, points out that the cost of sprawl extends well beyond licensing. “Every additional platform adds skills dependency, integration overhead, and operational complexity. Consolidation is often the fastest path to savings without compromising resilience,” Raj says.

Operational inefficiency is another hidden drain. In many IT environments, incidents are still handled through manual workflows, fragmented dashboards, and reactive processes. Each unresolved alert or delayed response consumes engineering time, disrupts business operations, and increases downstream costs. Over time, this operational debt limits an organisation’s ability to respond to change, regardless of how modern its infrastructure appears.

This is why observability and automation are increasingly being reframed as cost-control mechanisms rather than resilience upgrades. Simon Rizkalla, Vice President – Customer Advocacy, New Relic, describes this as an invisible tax on IT teams. “Unresolved alerts, delayed incident response, and lack of end-to-end visibility create a firefighting tax. That tax shows up as higher costs and slower business response,” Rizkalla says.



“Consolidation often delivers faster savings than new investments by reducing skills dependency, integration overhead, and operational drag across platforms.”

MICHAEL RAJ

EVP – Cloud, Infrastructure, Security & Testing, Birlasoft



“Poor visibility creates a firefighting tax, where unresolved alerts and slow response quietly inflate costs and delay critical business decisions.”

SIMON RIZKALLA

Vice President – Customer Advocacy, New Relic

“Most budget problems in IT are death by a thousand cuts—unmanaged consumption, overlapping tools, and manual operations. The fastest savings come from visibility, consolidation, and automation, not from freezing change,” Shesh adds.

Cloud environments amplify these challenges when governance is weak. Without clear ownership and financial visibility, elastic infrastructure can encourage over-provisioning and complacency. Enterprises are now responding by right-sizing workloads, shutting down unused resources, and, in some cases, selectively repatriating applications where cost predictability matters more than theoretical flexibility.

DESIGNING LEAN INFRASTRUCTURE AT CORE

Out of this scrutiny has emerged a clearer definition of what “lean infrastructure” means in practice. Rather than rip-and-replace programmes, enterprises are favouring incremental modernisation that improves utilisation, reduces manual effort, and simplifies operations.

Raj explains that the focus has shifted from capacity expansion to efficiency optimisation. Enterprises are rationalising workloads across hybrid environments, modernising core infrastructure to support automation, and using AIOps to reduce human intervention. In several Indian enterprise deployments, Birlasoft has seen improvements in uptime and operational efficiency without expanding capacity.

Observability plays a central role in this shift. By consolidating monitoring tools and automating incident response, organisations are reducing mean time to resolution and improving service reliability. Rizkalla notes that these gains are often visible within months, making them particularly attractive investments in a budget-constrained environment.

Lean infrastructure is also becoming the foundation for AI adoption. Murali Thiagarajan, Global Practice Head – AI-Led Intelligent Systems and Operations, Altimetrik, argues that AI-readiness does not require massive new investments if the underlying infrastructure is modernised intelligently. “AI readiness is about standardised data pipelines, automated operations, and scalable platforms that allow AI to be introduced without runaway costs,” Thiagarajan says.

MAKING SECURITY SPEND MORE ACCOUNTABLE

Security is undergoing a similar re-evaluation. Under budget pressure, it is increasingly being treated not as a parallel investment track, but as a cost-avoidance mechanism embedded into infrastructure decisions.

According to Ben Mudie, Field CTO for APJ, Tenable, exposure management has become central to this shift. “Every unresolved vulnerability represents potential financial impact—from downtime to regulatory penalties. Prioritising exposure reduction helps organisations focus spend where it matters most,” Mudie says.



“Budget pressure has made prioritisation unavoidable, with programmes lacking near-term operational or financial impact being deferred rather than abandoned.”

ANURAG AGRAWAL

Business Head – Americas, To The New



“AI readiness depends more on standardised data pipelines and automated operations than on large, upfront technology investments.”

MURALI THIAGARAJAN

Global Practice Head – AI-led Intelligent Systems & Operations, Altimetrik

Security consolidation is also reducing operational burden. Fewer tools mean better visibility, simpler workflows, and lower ongoing effort—particularly for compliance reporting. Raj reinforces this view, noting that governance-by-design is becoming essential as enterprises scale digital operations. Embedding security and compliance upfront avoids costly rework later, especially in regulated sectors.

NETWORKS AND THE INDIA-SCALE EQUATION

Network infrastructure continues to play a critical role, particularly in India-scale deployments where reliability and reach are non-negotiable. In these environments, network failure is not a technical inconvenience—it is a direct business disruption with measurable financial and reputational impact.

Malik observes that network modernisation is being driven by efficiency rather than expansion. “Enterprises are evaluating network upgrades based on reliability and operational efficiency, not just capacity,” he says.

In sectors such as telecom and manufacturing, the economics of uptime are clear. The cost-of-service disruption often outweighs the cost of infrastructure modernisation. Investments in fibre and IP networks are therefore being justified as mechanisms to reduce downtime, simplify operations, and support distributed digital architectures. Retrofitting resilience later—after outages or failures—has consistently proven more

expensive than designing it upfront.

“Hybrid and edge are no longer technology choices; they are economic and risk choices. The real question is where you can run a workload with predictable cost, reliability, and compliance,” Shesh says.

Tipnish adds that network strategy is also evolving alongside hybrid and multi-cloud adoption. Connectivity today is as much about predictable performance and integration with cloud and security architectures as it is about bandwidth.

BUILDING AI READINESS WITHOUT BLOAT

AI remains a strategic priority, but funding is becoming more disciplined. Rather than launching large-scale AI programmes, enterprises are focusing on readiness—data quality, governance, and operational maturity. There is growing recognition that poorly governed AI initiatives, built on fragmented data and parallel platforms, often increase cost and risk before delivering value.

Thiagarajan notes that many organisations are shifting from descriptive analytics to decision intelligence by modernising data platforms and automating data operations. These steps deliver immediate efficiency gains while laying the groundwork for more advanced capabilities. The emphasis is on sequencing to ensure AI ambition follows infrastructure readiness, not the other way around.



“Reducing exposure risk allows organisations to direct security spend toward vulnerabilities that materially limit financial, operational, and regulatory impact.”

BEN MUDIE

Field CTO – APJ, Tenable

Budget pressure is accelerating a managerial reset, forcing CIOs to treat infrastructure decisions as long-term economic commitments.



Open architectures and standardisation are playing a key role in cost control. Raj points out that simplified data estates reduce duplication and improve scalability, allowing AI workloads to be introduced incrementally and aligned with business priorities rather than technology hype.

PROOF POINTS FROM THE FIELD

Early proof points suggest that success under tight budgets is being achieved through disciplined optimisation rather than large-scale reinvention. One such example is SRF, where a renewed focus on exposure management and security consolidation has helped reduce risk while simplifying operations.

According to Mudie, the manufacturing major prioritised visibility and remediation across its expanding digital footprint instead of adding multiple point tools. “By focusing on exposure reduction and risk prioritisation, organisations like SRF are able to direct investment to areas that materially reduce operational and compliance risk,” he says.

Similar patterns are visible across other businesses. In manufacturing and asset-heavy sectors, selective infrastructure upgrades—combined with automation and tighter governance—have improved availability and reduced unplanned downtime without expanding capacity. Raj notes that these organisations are achieving resilience through consolidation and smarter utilisation rather than incremental spend.

Digital-native and services firms are seeing parallel benefits from operational optimisation. By consolidating observability platforms and automating incident response, several enterprises have reduced mean time to resolution and lowered the cost-of-service disruptions. Rizkalla observes that such improvements are often visible within months, making them particularly attractive in a budget-constrained year.

Taken together, these examples reinforce a consistent lesson: budget-led transformation does not dilute digital ambition. Instead, it sharpens focus—rewarding



THE CIO CHECKLIST

Use this checklist to assess whether your digital transformation programme is disciplined, defensible, and outcome-driven.

1. Budget discipline & governance

- ☐ Can every major infrastructure initiative show measurable impact within 6–12 months?
- ☐ Do we track unit economics (cost per app, transaction, user, workload)?
- ☐ Is FinOps embedded in decision-making—not just reporting cloud bills?

2. Cloud & infrastructure efficiency

- ☐ Have we identified and eliminated over-provisioned compute and idle storage?
- ☐ Are workloads placed deliberately (public cloud, private cloud, on-prem, edge) based on cost predictability and performance, not habit?
- ☐ Are we consolidating platforms rather than adding new ones?

3. Operations & observability

- ☐ Do we have end-to-end visibility across applications, infrastructure, and networks?
- ☐ Is MTTR trending down quarter-on-quarter?
- ☐ Have we automated incident response and routine operational tasks?

4. Security & compliance economics

- ☐ Are we reducing exposure and risk, or merely adding more security tools?
- ☐ Can we prioritise vulnerabilities based on business impact, not volume?
- ☐ Does our security posture lower audit effort, downtime risk, or regulatory exposure?

5. Network & resilience readiness

- ☐ Are network upgrades justified by uptime, reliability, and operational efficiency, not just bandwidth?
- ☐ Can the network support hybrid cloud, distributed apps, and secure access consistently?
- ☐ Is resilience designed in, or added later at higher cost?

6. AI and data readiness (without overspend)

- ☐ Is our data estate standardised, governed, and automation-ready?
- ☐ Are AI initiatives built on existing platforms and workflows, not parallel stacks?
- ☐ Can we scale AI use cases incrementally without re-architecting infrastructure?

7. Final reality check

- ☐ If budgets tighten further, do we know what to pause and what to protect?
- ☐ Are we cutting inefficiency—or cutting capability?



organisations that prioritise efficiency, resilience, and governance over unchecked expansion.

The emerging picture is one of maturity rather than retrenchment. Enterprises are not abandoning digital transformation; they are redefining it. Budgets are tighter, scrutiny is higher, and tolerance for open-ended programmes is limited. In this environment, infrastructure decisions are becoming harder to reverse—and mistakes more visible.

As Tipnish concludes, “The next phase of digital transformation will reward precision—organisations that align infrastructure decisions with business outcomes while maintaining resilience and compliance will be best positioned for the future.” For CIOs, success will increasingly be measured not by what was launched, but by what consistently works under pressure. 🍌

shubhendup@cybermedia.co.in

PCQUEST FEBRUARY 2026 EDITION CYBERSECURITY IN 2026: WHEN IDENTITY BECOMES THE PERIMETER

ALSO READ MORE ON

- Cracking the identity code in cybersecurity
- Are hackers targeting Windows first while Macs fly under the radar in India?
 - Best cybersecurity solutions for 2026: What actually works now
- Who is accountable when AI goes rogue? • The quiet revolution in creativity
 - Five smartphones rewriting mobile photography in 2026
- **REVIEWS:** Infinix GT 30 5G+ | Vivo X300 Pro | Realme Buds Air 8

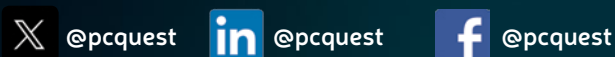


Scan QR Code
& Subscribe now...

PCQUEST IS OFFERING
SPECIAL DISCOUNTS
FOR **NEW SUBSCRIBERS**
AND ITS READERS.
AVAIL THE OFFER NOW

Link: <https://bit.ly/3QvNQh8>

FOLLOW PCQUEST FOR THE REGULAR
UPDATES ON TECH AND TRENDS



Leverage PCQuest platform & network. Write to:
Ajay Dhoundiyal | ajaydh@cybermedia.co.in | +91 99535 40318



For Subscription queries::

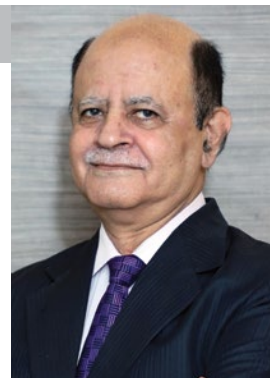
subscriptions@cybermedia.co.in

9289870545

LT GEN DR SP KOCHHAR

APP-LAYER FRAUD: IT IS TIME FOR A STRONGER TRUST ARCHITECTURE

With scams increasingly originating on messaging platforms, India must correct regulatory asymmetry and strengthen verification to protect digital trust.



India's digital transformation has been both rapid and inclusive. App-based communication platforms have become the backbone of everyday interactions, enabling everything from social connections and commerce to financial transactions and service delivery. However, this remarkable growth has also created a serious and persistent challenge: fraud and scams on these platforms have escalated into a systemic threat to public trust and the digital economy.

This is no longer a marginal cybercrime issue. It is a structural vulnerability that requires coordinated attention from policymakers, platforms, industry and citizens alike.

APP-BASED COMMUNICATION ADDS FRAUD SURFACE

During the last five years, the nature of digital fraud in India has changed fundamentally. Fraud has migrated

from traditional voice calls and SMS to app-based communication platforms that offer scale, anonymity and speed. According to the Ministry of Home Affairs, app-based messaging and social communication platforms now account for the largest share of cybercrime complaints in the country.

In the first quarter of 2024 alone, thousands of cyber-fraud complaints were linked to such platforms, making them the single biggest channel for reported cybercrime. Financial losses underline the severity of the issue. As per official estimates, Indians lost over Rs 22,800 crore to digital fraud in 2024, with a significant proportion of cases originating on app-based communication platforms and later moving to UPI and other digital payment systems.

These figures represent only reported cases, and the true scale is likely much higher due to under-reporting driven by stigma and low recovery expectations.



Fraud risk must be addressed where it originates; telecom networks cannot remain the sole line of defence for threats emerging on app platforms.



Fraud has migrated to the least-regulated digital layer, exposing persistent verification gaps across app-based platforms now operating at a nationwide scale.



IN BRIEF

- Frauds and scams have migrated from regulated telecom channels to lightly governed app-based communication platforms.
- Telecom KYC and anti-spam reforms have reduced SIM misuse, but fraud now originates through messaging apps.
- Messaging app platforms classified as intermediaries face weaker verification and accountability obligations.
- Expecting telcos to block fraud initiated on third-party apps and completed via banking rails is unrealistic.
- Measures such as SIM binding can close identity gaps without compromising encryption or privacy.
- A coordinated framework across platforms, telecom and finance is essential to restore digital trust.

The reason for this shift is straightforward. App-based communication services enable mass outreach at negligible cost, rapid creation of disposable identities, and seamless redirection to payment methods. Fraudsters exploit familiarity and trust rather than technical vulnerabilities. In effect, human behaviour becomes the attack vector.

COMMON FRAUD PATTERNS AND THEIR IMPACT

Across law enforcement advisories and industry

analyses, several recurring fraud patterns have crystallised. Part-time job and task-based scams promise easy income through simple online activities, then demand refundable deposits or prepaid tasks.

Investment and trading scams, including long-grooming models often referred to as pig-butcher, use sustained engagement on communication platforms before directing victims to fake trading dashboards and payment channels. Digital arrest scams impersonate law enforcement or regulatory authorities, isolating victims through continuous app-based calls and coercing them into transferring large sums for so-called verification.

Illegal digital lending scams use app-based messaging as their acquisition and harassment channel. In contrast, brand impersonation scams pose as customer support for well-known companies to extract payments or credentials. Romance scams, sextortion and malware distribution through malicious links further widen the threat landscape.

What is striking is not just the diversity of scams, but their scale and repeatability. Individual losses now frequently exceed millions per victim. More importantly, these frauds erode confidence in digital platforms that are otherwise central to India's economic and social life.

REGULATORY ASYMMETRY AND ITS CONSEQUENCES

India has made significant progress in securing traditional telecom channels. Telecom operators operate under strict KYC norms, continuous regulatory oversight and robust anti-spam frameworks. These measures have delivered results, including sharp reductions in spoofed calls and SIM misuse, as documented by government data.

However, app-based communication platforms are governed under a different regulatory construct. Classified as intermediaries, they are not subject to telecom-style KYC, spam regulations or uniform accountability norms. As a result, fraud has predictably migrated to this less-regulated layer.

This asymmetry creates a distorted risk environment. Expecting telecom operators to act as the sole choke point

Telecom operators strengthened KYC and anti-spam controls, yet scams increasingly originate on messaging apps that face far lighter verification standards.

for fraud initiated on third-party platforms, transacted through banking rails, and often orchestrated from outside India is neither realistic nor equitable. Risk must be addressed where it is created.

EXTENDING ACCOUNTABILITY TO THE APP LAYER

Recent policy discussions on measures such as persistent SIM binding for app-based communication services must be viewed in this context. SIM binding is not an alien or intrusive concept. It already underpins critical digital systems such as UPI, where it has strengthened security without undermining usability or privacy.

The objective of SIM binding is not to enable content surveillance or dilute encryption. It is to ensure a basic, verifiable link among the user, the device, and the communication account. This closes a long-standing loophole that has allowed accounts to operate even after the removal or replacement of the associated SIM, enabling anonymous misuse at scale.

SIM binding is a layered and proportionate security measure. It does not require additional data collection, disrupt enterprise workflows, or prevent legitimate use, including for users travelling internationally. Its value lies in restoring accountability in a high-risk digital environment.

BUILDING A SHARED DEFENCE FRAMEWORK

India's response to digital fraud has already evolved beyond isolated enforcement. Institutions such as the Indian Cybercrime Coordination Centre, the national cybercrime reporting portal, and the 1930 helpline have strengthened coordination and reporting. The Department of Telecommunications' Digital Intelligence Platform and the Financial Fraud Risk Indicator represent important steps towards real-time, risk-based intervention across telecom and financial systems.

Telecom operators continue to tighten KYC, share intelligence and integrate with national fraud detection mechanisms. Banks and payment platforms are deploying advanced analytics and transaction-level safeguards. These efforts echo the approach in which citizen participation, AI-driven detection, and institutional

coordination together form the backbone of a resilient fraud prevention ecosystem.

However, the effectiveness of this ecosystem depends on comparable commitment from app-based communication platforms. Stronger verification for high-risk and business accounts, faster takedown of fraudulent networks, clearer disclosure of official communication channels and deeper integration with national fraud intelligence systems are no longer optional. They are essential to preserving trust at scale.

Finally, citizens remain a critical line of defence. Empowerment, not blame, must guide public engagement. Simple principles continue to hold. Genuine employers do not charge for jobs. No law enforcement or regulatory authority conducts arrests or verification over app-based calls. Unsolicited financial offers should always be treated with caution.

When citizens report suspicious activity, they contribute directly to intelligence systems that protect others. In this sense, every user becomes a participant in national cyber resilience.

RESTORING TRUST IN INDIA'S DIGITAL ECOSYSTEM

India does not face a choice between innovation and security, or between privacy and accountability. With risk-aligned regulation, proportionate safeguards and shared responsibility across platforms, telecom networks, financial institutions and users, it is possible to strengthen trust without stifling growth.

App-based communication platforms are now part of the country's critical digital infrastructure. As their role expands, so must their responsibility. The credibility of India's digital economy depends on getting this balance right, and on acting decisively before trust erosion becomes irreversible. 🧩

The author is a decorated military veteran who retired as the Signal Officer-in-Chief, the head of the Indian Army's ICT division. He was also the first CEO of the Telecom Sector Skill Council and is the Director General of the Cellular Operators Association of India (COAI).

feedbackvnd@cybermedia.co.in

DATAQUEST FEBRUARY 2026 EDITION: DATA CENTRES, REIMAGINED

ALSO READ MORE ON

- From claims to proof: measuring sustainability in India's data centres
- Bridging the gap between connectivity and compute at scale - Ashish Arora
- From Copilots to Colleagues: The rise of agentic AI in enterprises
- Is AI Killing Sustainability
- Target's Brad Thompson Explains the Rise of Reliable, Responsible Agentic AI in Retail
- HPE Rewrites the Playbook for AI-Native Infrastructure
- Reclaiming Control in the AI Era: A Conversation - Kalyan Kumar
- Reclaiming Control in the AI Era - Kalyan Kumar



Scan QR Code
& Subscribe now...

DATAQUEST 40+ YEARS CELEBRATIONS:
GET 40% EXCLUSIVE DISCOUNT ON
DATAQUEST PRINT SUBSCRIPTION
AND DATAQUEST DIGITAL
SUBSCRIPTION AT FLAT 420/- ONLY.
AVAIL THE OFFER NOW

<https://shorturl.at/vn6tN>

**FOLLOW DATAQUEST FOR REGULAR
AND LATEST UPDATES ON THE
BUSINESS OF ICT ECOSYSTEM.**



Dataquest



dataquestindia

Leverage Dataquest platform & network

Ajay Dhoundiyal | ajaydh@cybermedia.co.in | +91 99535 40318



#ImpactingICTfor4Decades

For Subscription queries:



subscriptions@cybermedia.co.in



9289870545

[INTERVIEW]

TATA COMMUNICATIONS



PRAVEEN ARORA

Vice President – IoT (Business Unit),
Tata Communications

“Shopfloor change is now driven by data and intelligent networks”

India's factory floors are no longer defined only by machines, throughput, and shift rosters. They are being rewired into data-rich environments where sensors, video feeds, enterprise systems, and worker safety signals converge into a single operational picture.

Praveen Arora, Vice President – IoT (Business Unit), Tata Communications, in this exclusive interaction with **Shubendu Parth**, explains how industrial IoT is moving from reactive alarms to proactive, pattern-led prevention, and why “people first” is the real starting point of Industry 4.0. He also shared insights on how frugal, subscription-based models can help MSMEs adopt digital workflows without hiring a new tech team, the edge-versus-cloud decisions, agentic AI's early role in shopfloor orchestration, and why resilience must cover both the customer layer and the underlying infrastructure. Excerpts:

Tata Communications' Q3FY25 results underscore a pivot towards data-led growth. Where does industrial IoT sit in that shift, and what is changing in manufacturing demand?

From the standpoint of the shift to digital, there are four key focus areas we are working on. These include, IoT fabric, network fabric, interaction fabric, and the cloud fabric. Together, these are helping the pivot towards new digital growth.

If you look at how markets are moving—towards digitalisation and a more data-driven journey across clients, be it manufacturing, be it cities, be it ports, be it across the financial sector—that is how these shifts are happening. Especially in manufacturing, within the IoT fabric, the shift is towards intelligence-based systems. They are no longer reactive; they are becoming proactive.

And this is happening through integration of data—coming from sensors and devices—plus intelligence

built on that data. It is not only devices; it is also existing enterprise systems and manufacturing systems on the shopfloor. That integration is where the value themes are emerging: efficiency, safety, and a smarter way to run operations.

On India's shopfloors, how are we moving from basic monitoring to predictive, AI-led decision systems? What does that transition look like in practice?

If you compare India to mature markets, India is shifting towards becoming a manufacturing hub, where efficiency and throughput matter. On the shopfloor, changes are now driven by data and intelligent networks.

Think of manufacturing in two parts: core operations and peripheral or auxiliary systems that support manufacturing. The shift is happening across both. What we are seeing is the integration of machine-to-machine and human interactions in both core and support systems.

When we talk about efficiency, we always start with people—“people first” is our approach, even for automation. The brain behind automation is still human. Now, as interactions become more intelligent, you see more automation on the core line and also in peripheral systems.

Within the IoT fabric, we have a factory span—factory operations integrated into a single element. It can include vibration data, machine performance, current throughput, and plant output to various systems. These interactions generate large volumes of data, and the data shows deviation from the planned output. For example, vibration data can indicate a proactive failure, so maintenance happens before breakdown, not after a blaring alarm. That is the shift from reactive to proactive.

The other dimension is the workforce. Manufacturing involves hazardous environments and heavy equipment.

Connected worker offerings monitor pulse rate, heart rate, fall detection, entry into hazardous areas, and activity patterns. The first five minutes are a golden window for incident prevention. In continuous manufacturing, even a 20–30-minute disruption can have a major effect—sometimes it takes one to two days to return to efficiency levels. So predictive interactions matter.

And then you have digital twins and digital threads linking all this together. In a steel plant, for instance, there might be 15,000 sensors. Beyond sensors, there are MES, SCADA, and enterprise systems. You can imagine the data volumes now available. That data is being used to improve efficiency, identify bottlenecks, and prevent slowdowns.

Even in discrete manufacturing, if the throughput of station A versus station B shifts over time, efficiency drops. Proactive action reinforces process parameters, enabling the line to balance dynamically. Those are the systems helping companies improve efficiency—10–12% in continuous manufacturing can be significant, and even 2–3% in discrete manufacturing is a meaningful gain. These technologies were once on the hype curve. Now they are maturing and being put to work.

You have emphasised a “people first” approach. What mindset shift is still required in Indian manufacturing to scale Industry 4.0 and 5.0?

We see two or three areas where a mindset shift is needed. First, these changes are for the entire workforce. It is not only about productivity and efficiency, but also about safety, because manufacturing processes revolve around humans. “People first” needs to be part of the operating philosophy.

If you look at earlier eras—Industry 1.0 and 2.0—interaction was mechanical input with machines. Later, interaction evolved, but it remained reactive: alarms go off, then action happens. Now with AI embedded, the interactions are more mature and seasoned. You know something is likely to happen, and you take corrective action so failure does not occur or quality is not impacted.

A simple example is computer vision and video analytics for quality inspection. The human eye can focus for a limited time. Research says attention drops after about 20 minutes, and faults may be missed. Video analytics helps inspect cracks, paint issues, fitting issues, dimensional tolerance issues, and missing components across industries. On a line, products may flow at five to

10 per minute. This is digitally analysed, on the edge or in the cloud. That is the shift: technology exists to assist and raise quality, not to replace intent.

The next mindset shift is around Industry 4.0 or 5.0 adoption—more human-interaction-based. And the traditional thought that “this is an expense” needs to change. Recovery can happen within a year or two. The decision is about uplifting manufacturing output and efficiency—not just for one company; for India as a whole.

Your steel-sector deployments have reportedly prevented several near-fatal incidents. Can you walk us through how such a predictive safety system works and the kinds of interventions that happen on the ground?

The system rests on four core components. First are the devices—wearables such as helmet tags or wristbands. Second is zone intelligence, where areas are classified as hazardous, work-at-height, restricted or permitted. Third is the AI layer, where incidents and risk patterns are analysed using historical and real-time data from sensors, machines and enterprise systems. The fourth component is feedback—alerts routed to supervisors, workers or emergency response teams for proactive intervention.

These elements come together across sensors, networks, analytics and operational processes. For instance, if a worker enters a hazardous zone, the wearable checks access permissions. If the entry is unauthorised, an alert is triggered before an incident occurs. In another case, if a fall is detected and the heart rate spikes, both signals are correlated and emergency response can be activated within the first five minutes—the critical window for preventing fatalities.

In work-at-height scenarios, video analytics verifies whether safety harnesses are worn. If not, warnings are issued before unsafe climbing begins. In high-heat zones, exposure time and distance are monitored to prevent dehydration or collapse.

All zones—hazardous, restricted and operational—are mapped using machine vision, analytics and worker data. The system continuously observes patterns and provides early warnings when conditions indicate elevated risk. In some cases, it even flags anomalies such as theft as a secondary outcome. The objective is simple: intervene early and prevent harm before it occurs.

Digital adoption should not require a new tech team; frugal, subscription-based IoT models let MSMEs focus on output while platforms run remotely.

Edge versus cloud is a practical design question. In a manufacturing set-up, what decisions happen at the edge, and what stays in the cloud?

Let us take video analytics as a simple example. A camera might run five to 10 use cases—some related to productivity, some to safety compliance, whether process steps are followed, whether a required person is present, and whether material movement creates conflict on the floor.

These use cases can run on the edge—close to the facility's camera. But training models to achieve accuracy beyond 90–95% requires learning, which is done in the cloud. Hence, you use the cloud for training.

When an incident happens, capture happens at the edge. Then you choose what to send—say, plus or minus a few minutes of frames—to the cloud. That balances the load, optimises data flows, and improves response time on the line. Cloud also supports long-term storage and integration with enterprise systems. So, it is not edge versus cloud—it is a design in which the load is balanced and responses are fast.

Tata Communications is often associated with large enterprises. What does the MSME play look like, and how do you make adoption financially viable?

For MSMEs, it can include the full IoT fabric. It covers device and sensor data, network connectivity, AI/ML engines and value creation through use cases. For smaller units, it becomes outcome-focused: how digital enablement improves throughput and efficiency as planned.

It includes sensors on the line, visual analytics, an IoT platform to ingest and analyse data, and AI/ML engines for insights. Then you have a services layer. Many MSMEs fear digital requires additional manpower. But we can run it end-to-end remotely, so they focus on their product and core operations, and digital helps meet targets.

On pricing—just to enable adoption—we launched a frugal approach where an MSME can onboard up to 500 devices at around Rs 10,000 per month, with data management space included. Beyond that, when they

add more complex devices or integrate other systems, it can move to pay-per-use or subscription. The idea is to make the entry cost practically negligible so the use of technology is democratised.

We already have a few deployments and more are being discussed. We want adoption to become “click of a button”. Earlier a request would come, then enablement would happen. Now we are enabling through a simple UI tool to make it user-friendly.

And there is another point—people and planet. Efficient utilisation of resources matters. In India, manufacturing's digital adoption is still behind. We are trying to make adoption prudent and self-reliant. We also work on non-standard sensor requirements, frugally, through our hardware IoT platform and plug-and-play approaches.

For CXOs planning Industry 4.0 and 5.0, what is your modular blueprint—what to digitise first, what comes next, and what can wait?

I will break it down into three phases. Phase one is visibility—basic enablement of the digital layer. Put in a few basic sensors, get an IoT platform, ingest the data and read it. Do it frugally. Digitalise inputs coming in, and keep “people first” in view—basic safety and basic machine signals.

Phase two is intelligence—introduce edge-based intelligence, AI/ML programming, real-time analytics. The plant can take action based on intelligence. Phase three is optimisation. Now the system is integrated end-to-end—not just sensors, but human interaction, MES systems, enterprise systems, reporting systems, raw material logistics. Operations become seamlessly integrated.

Large industries are already in visibility. They need to step up to intelligence and optimisation. For MSMEs, start with visibility, with intelligence onboard where possible. It is an ongoing journey. Once the core gains are understood, the shift becomes immediate—digitalise, make it intelligent, and optimise. 🍀

shubhendup@cybermedia.co.in

Five signals for India's digital infrastructure shift

Nirmala Sitharaman outlines India's AI- and data-centre-led roadmap, signalling structural shifts in networks, compute and digital sovereignty.



BY SHUBHENDU PARTH

Delivering her 85-minute-long Budget 2026–27 speech on Sunday, Finance Minister Nirmala Sitharaman did not mention “telecom” for once, even though she placed digital infrastructure at the centre of India's investment-led growth strategy.

At first glance, the budget appears restrained on headline-grabbing technology announcements. There is no single flagship telecom scheme, no dramatic artificial intelligence (AI) outlay, and no reform package for networks. However, a closer look reveals five important signals about how India plans to develop its digital, telecom, and computing backbone over the next decade.

Like the rest of the budget—focused on three *kartavyas* or key duties—the announcements for the technology and digital infrastructure sector are less about specifics and more about setting direction, priorities, and structure.

For telecom operators and network vendors, the implications are substantial, even in areas where the budget does not specifically address industry concerns.

AI: FROM PILOTS TO POPULATION-SCALE PLATFORMS

If the world is gravitating towards AI, can India be behind? In fact, it is the one technology thread that quietly runs

The FM reframes digital infrastructure as an economic multiplier, embedding AI, cloud and compute into logistics, governance and trade systems nationwide.

through the budget—not as a headline-grabbing sector, and certainly not as a big-ticket allocation, but as an enabling layer that can drive everything from governance to service delivery.

Reflecting the Economic Survey 2025–26, the budget adopts a “bottom-up, application-focused” approach, focusing on solving real-world problems in sectors such as health, agriculture, and education, rather than attempting to build massive, capital-intensive frontier models.

The launch of Bharat-VISTAAR, a multilingual AI system meant for integrating AgriStack and ICAR data, is a case in point. This demonstrates the government’s intent to implement AI directly in public service delivery, especially in rural and agricultural sectors where reach and reliability are as important as sophistication.

This is also evident from the proposed Education-to-Employment and Enterprise Standing Committee, which will assess how emerging technologies, including AI, will reshape jobs, skills, and curricula. The mandate links AI adoption to workforce transformation and employability, both of which rely on connectivity, cloud access, and robust digital infrastructure.

From a telecom sector perspective, this suggests increasing demand for low-latency networks, rural broadband, and edge-capable infrastructure, even if these needs are not explicitly stated in the budget.

DATA CENTRES: THE NEW STRATEGIC NATIONAL ASSETS

One of the most consequential technology signals in the budget relates to data centres, with the Finance Minister referring to them seven times during her speech. However, the emphasis is reflected more in the tax proposals aimed at attracting investment than in direct technology announcements.

The government’s proposal to offer a tax holiday until 2047 for foreign companies providing global cloud services using data centres located in India marks a strategic repositioning of data centres as sovereign digital infrastructure.



IN BRIEF

- AI moves from pilot projects to population-scale deployment, linking governance, agriculture and skilling to scalable digital networks.
- Data centres receive long-term tax clarity, repositioning India as a competitive base for global cloud and AI workloads.
- Semiconductor Mission 2.0 shifts from fabs to full ecosystem depth, spanning IP, materials, equipment and rare-earth corridors.
- Infrastructure capex increasingly embeds digital systems, making fibre, edge and secure networks foundational to logistics and cities.
- Telecom remains an assumed enabler, with no levy reform or 5G-specific incentives for private operators.
- BSNL receives a higher allocation, while private telcos face demand growth without parallel balance-sheet relief.

This approach is reinforced by a 15% safe-harbour provision for resident entities providing data centre services to related foreign companies offering cloud services outside India. Together, these measures aim to make India a competitive base for global cloud and AI workloads.

Data centres are positioned as sovereign digital assets, but the fiscal and regulatory framework for fibre, transport and last-mile networks remains undefined.

For telecom operators, the opportunity may be indirect, but it is significant, as large-scale data centres and AI compute facilities depend heavily on dense fibre networks, resilient backhaul, high-capacity transport layers, and edge connectivity.

Interestingly, while the budget proposes incentives for investment in data centres, it stops short of formally positioning telecom operators as strategic partners in this ecosystem. Their role is assumed rather than defined, leaving open questions about how network investments will be incentivised alongside compute infrastructure.

SEMICONDUCTOR: FROM POLICY SHIFTS TO ECOSYSTEM DEPTH

After years of focusing on fabs and manufacturing incentives, Budget 2026–27 suggests that India's semiconductor policy is entering a more mature phase.

With the announcement of India Semiconductor Mission 2.0, the government has signalled a shift from a narrow manufacturing lens to a broader ecosystem approach. The focus now extends beyond fabrication to include equipment and materials manufacturing, full-stack Indian intellectual property, and industry-led research and skilling centres.

This ecosystem-oriented thinking is reinforced by the expanded outlay for electronics components manufacturing and the proposal to establish rare-earth corridors across mineral-rich states.

For telecom networks and data centres, the implications are long-term and structural, as network equipment, optical systems, and compute infrastructure are becoming increasingly chip-intensive.

Supply-chain resilience and cost competitiveness will therefore depend not just on final assembly, but on access to domestic design capabilities, materials, and specialised components. As indicated in the Finance Minister's speech, this reflects an understanding that digital infrastructure sovereignty cannot be separated from semiconductor depth.

INFRASTRUCTURE: SPENDING TURNS DIGITAL-FIRST MODEL

On paper, the budget's push for infrastructure looks familiar—higher capital expenditure and continued investment in transport, logistics, and urban development. However, a significant shift is underway.

The budget proposes raising public capital expenditure to Rs 12.2 lakh crore for 2026–27, maintaining momentum across transport, logistics, urban development, and connectivity. What is changing, however, is the character of infrastructure itself. Initiatives such as City Economic Regions, AI-enabled customs scanning, integrated digital clearance systems, and software-driven logistics platforms point towards data-centric, network-dependent infrastructure.

Traditionally physical projects such as freight corridors, waterways, and urban transport are increasingly being designed with stronger digital coordination, platform-led oversight, and intelligent control systems. This highlights a structural shift in demand.

Future infrastructure investment will therefore require deep fibre penetration, edge computing, secure networks, and high-capacity telecom backbones, even if these needs are not always explicitly stated in the budget.

THE CONVERGENCE: SERVICES, TELECOM, TECH EXPORTS

The budget consolidates IT services, IT-enabled services, knowledge process outsourcing, and software R&D into a single category with a higher safe-harbour threshold, formally recognising the convergence of software, services, and deep technology.

Similarly, incentives for bonded warehousing, toll manufacturing, and global cloud services reflect a clear effort to align electronics manufacturing, digital services, and data-centre-led exports.

This convergence presents telecom operators and network vendors with a strategic opportunity. As enterprises and governments shift towards platform-

Semiconductor policy signals ecosystem maturity, expanding beyond fabs to materials, IP depth and specialised supply chains critical for telecom and AI hardware.

based delivery models, connectivity alone will not be sufficient.

Success will depend on evolving towards infrastructure-as-a-service and platform-adjacent roles, supported by policy frameworks that recognise this transition.

WHAT BUDGET 2026-27 MEANS FOR TELECOM OPERATORS

Although the budget places AI, data centres, and semiconductors at the centre of India's digital strategy, telecom is positioned more as an enabler than as a vertical receiving targeted policy attention.

The government has proposed increasing the outlay for the telecom sector to Rs 73,990 crore, nearly 40% higher than last year's revised estimates. Most of this increase, however, is allocated to BSNL for spectrum costs, network rollout, BharatNet implementation, and internal capital requirements.

According to PTI, Telecom Minister Jyotiraditya Scindia described this allocation as an effort to strengthen BSNL's operational and financial position, particularly in rural broadband and domestic network deployment. This emphasis on the public-sector operator is notable as the broader industry continues to face structural challenges.

The government projects telecom sector revenues of Rs 1.17 trillion in 2026–27, lower than the revised estimates for 2025–26. This reflects continued financial pressure on operators, including the impact of converting Vodafone Idea's spectrum dues into equity, which limits adjusted gross revenue-linked inflows for the next decade.

Licence fees and spectrum usage charges, set at 8% of AGR for telecom operators, remain the government's primary revenue streams from the sector.

For private operators, the budget offers growth opportunities through rising demand but provides no balance-sheet relief. There are no explicit concessions

on levies, no clarity on spectrum pricing reform, and no targeted incentives for 5G expansion or fibre rollout.

Instead, private-sector telecom operators are expected to benefit indirectly from demand generated by data centres, AI platforms, and digital infrastructure, while direct public investment is focused on BSNL.

EXECUTION GAPS TO DECIDE TELECOM'S ROLE IN GROWTH

The budget does not announce major telecom-specific growth measures, but it prepares the ground for future expansion. It signals a focus on AI-native platforms, data-centre-driven growth, a deeper semiconductor ecosystem, and digitally integrated infrastructure.

For telecom operators and network vendors, the budget also highlights what remains unresolved. While AI platforms, cloud infrastructure, and electronics manufacturing receive clear policy direction, telecom networks are treated as an assumed layer rather than explicitly addressed. There is limited clarity on network modernisation, fibre expansion, or how telcos are expected to participate in AI, cloud, and edge-compute ecosystems.

This lack of detail does not diminish the budget's digital ambition. Instead, it shifts the burden of execution to policy follow-through. For India's AI-driven and data-centre-focused vision to scale, telecom networks cannot remain implicit. They must become an explicit pillar of the country's digital infrastructure strategy.

For telecom operators, the most important signals are likely to emerge after the budget. These include the structure and timing of spectrum auctions in 2026, deployment priorities under the Digital Bharat Nidhi, execution models for BharatNet, and any recalibration of AGR-linked levies.

Equally important will be whether telecom networks are formally integrated into India's AI, cloud, and data-centre roadmap. Without this alignment, telcos risk remaining essential yet economically constrained enablers of India's next technology cycle. 🌟

shubhendup@cybermedia.co.in

From fiscal math to tech sovereignty strategy

Capital discipline, targeted incentives and ecosystem bets reposition technology as a sovereign asset shaping India's long-term economic power.



BY JAIDEEP GHOSH

The Union Budget 2026-27 is a well thought-through extension of prior fiscal blueprints. Building on the 2025 reforms, this budget reinforces policy continuity, signalling predictability to investors amid global volatility. Rather than hype and new announcements, it embeds technology as an enabler across economic pillars, fostering competitiveness in AI-driven tech, semiconductors, and telecom.

The philosophy here is a shift from service to sovereignty. India is moving beyond just writing code for the world to owning the compute, the silicon, and the energy that powers it. The Finance Minister, Nirmala Sitharaman, has effectively declared that for India, technology is no longer just a service sector to be exported, but a sovereign asset to be secured.

The tax holiday until 2047 signals India's ambition to host global AI workloads, shifting from a consumption market to a compute jurisdiction.

Semiconductor policy now targets upstream materials and IP depth, acknowledging ecosystem control matters more than isolated fabrication wins.

The fiscal backdrop sets the stage. By sticking to the fiscal glide path and bringing the Fiscal Deficit down to 4.3% of GDP, the government has delivered a “Good Deficit.” The borrowing is not fuelling consumption; it is fuelling a record Rs 12.2 lakh crore in Capital Expenditure. For capital-intensive sectors like telecom and tech infrastructure, this fiscal discipline is the best news; it signals macroeconomic stability, potentially lowering the cost of capital for the massive 5G and 6G network rollouts still ahead.

But the real signal lies in the specific, targeted interventions that aim to build what may be described as India’s “Sovereign Tech Stack”—from the minerals to the cloud.

CLOUD INCENTIVES AND DATA GRAVITY PLAY

The most significant geopolitical signal in the budget is buried in the tax proposals: a Tax Holiday until 2047 for foreign companies providing global cloud services using Indian data centres. This is a masterstroke.

By aligning the tax incentive with the centenary of India’s independence, the government is playing the long game on Data Gravity: data is heavy, and expensive to move. By making it fiscally irresistible for global hyperscalers like Amazon, Google, and Microsoft to host their global data in India, the policy framework seeks to ensure that the AI models of the future are trained here, reside here, and are subject to Indian jurisdiction.

Coupled with the 15% Safe Harbour provision for resident entities providing data centre services, the message is clear: India intends to move beyond being merely a market for digital consumption and position itself as a major participant in the digital economy.

AI WOVEN INTO REFORM ARCHITECTURE

In AI and broader tech, the budget positions artificial intelligence not as a standalone sector but as a pervasive force multiplier. This aligns with the government’s three kartavya framework, where AI enhances productivity, economic growth, governance, and inclusion. For instance, the emphasis on cutting-edge technologies in the Reform Express initiative—over 350 reforms since



IN BRIEF

- Fiscal deficit at 4.3% and Rs 12.2 lakh crore capex signal macro stability, lowering risk for telecom, semiconductor and AI infrastructure investors.
- A tax holiday until 2047 aims to anchor global cloud workloads in Indian data centres, strengthening jurisdictional control over AI compute and data.
- Semiconductor Mission 2.0 shifts from fabs to ecosystem depth—materials, equipment and domestic IP—to reduce structural import dependence.
- Rare Earth Corridors embed technology policy within national security, linking mineral processing to quantum, AI and strategic hardware supply chains.
- AI is framed as a cross-sector productivity lever, tied to reforms, skilling and services exports rather than treated as a standalone industry.
- Telecom funding and rural broadband expansion reinforce networks as the enabling layer for agri-stack, digital governance and enterprise AI adoption.

Rare Earth Corridors connect mineral strategy to advanced hardware ambitions, reframing supply chains as instruments of sovereignty.

2025 streamlines compliance and data flows, enabling AI integration in manufacturing and services.

The high-powered committee on Education to Employment and Enterprise targets 10% global services share by 2047, explicitly assessing AI's job implications. This proactive stance could mitigate displacement risks while amplifying India's IT-BPM strengths, potentially adding 2-3% to GDP growth through optimised processes.

Overall, these reforms could elevate India's AI readiness index by 15-20 points, positioning it as a global innovation hub. There is, however, a talent gap. The budget's skilling push, including Samarth 2.0 for textiles and AVGC labs training two million professionals supports AI workforce development.

This is in continuation of the previous years' Budget that proposed key skilling initiatives: five National Centers of Excellence, expanding capacity at IITs and medical colleges, launching enhanced research fellowships at IISc and IITs, creating 50,000 new Atal Tinkering Lab Incubation Centres in schools, funding private-sector R&D and providing broadband connectivity to all government schools and public health centres.

THE HARDWARE PIVOT: SECURING THE UPSTREAM

The launch of the India Semiconductor Mission (ISM) 2.0 shifts focus from fabrication plants to the ecosystem—equipment, materials, and full-stack Indian IP. The increased outlay of Rs 40,000 crore for electronics components manufacturing acknowledges a hard truth: one cannot be a tech superpower if one has to import every capacitor and resistor.

Crucially, the budget links technology to national security by announcing Rare Earth Corridors in Odisha, Kerala, Andhra Pradesh, and Tamil Nadu. In a world where critical minerals are the new oil, securing domestic processing capabilities for the raw materials of Quantum and AI hardware is a definitive sovereignty play.

THE INVISIBLE INFRA: TELECOM AS THE BACKBONE

Although the budget does not announce a headline-

grabbing telecom reforms package, the sector underpins multiple policy initiatives. While there was no headline Telecom Package, the sector is the silent beneficiary of every major announcement. Adequate funding of Rs 73,990 crore, has been allocated to the sector, a substantial part through BSNL, for Bharat net and rural broadband infrastructure buildout.

Take Bharat-VISTAAR, the new AI-driven agri-stack. is a demand generator for rural data connectivity. To deliver real-time, AI-customised advisory to millions of farmers requires a robust, low-latency telecom backbone that goes beyond urban centres.

EASE OF BUSINESS: THE GCC BOOST

Finally, the budget offers a massive olive branch to the IT Services and Global Capability Centres (GCCs) that drive India's services exports. By raising the Safe Harbour threshold for IT services to Rs 2,000 crore and introducing a One-Click automated approval process, the government has effectively eliminated a decade of transfer pricing litigation.

This creates the certainty needed for GCCs to further move up the value chain—from process support to high-value R&D and product innovation, supporting the ambitious target of India capturing 10% of global services exports by 2047.

CAPEX DISCIPLINE AND SOVEREIGN TECH VISION

The budget for 2026-27 is a 'Maturity Budget'. It avoids the hype of launching new, unfunded missions and focuses instead on the unglamorous but essential work of constraint management—fixing energy, securing supply chains, and training workforce. For the telecom and tech sectors, the signal is unambiguous. The government views them as the "horizontal spine" of Viksit Bharat.

With sustained execution, this could propel India's digital economy to USD 1 trillion by 2030, underscoring the value of policy stability in an uncertain world. 🌟

The author is a Management Consultant and a former Partner at KPMG in India. (Views are personal.).

feedbackvnd@cybermedia.co.in



Building real-time risk engines on telco networks

BFSI firms are redesigning risk systems using AI, blockchain, and low-latency networks to enable real-time fraud prevention and compliance.



BY ROHIT GORE

The construct of risk and resilience in the financial services landscape is evolving rapidly. Today, the BFSI industry has entered a phase in which risk management cannot be solely based on static controls or traditional data models. The global risk landscape has swiftly expanded from cyberattacks and geopolitical volatility to the more subtle ethical challenges of artificial intelligence, exponentially increasing the impact of data privacy breaches.

In response, a quiet revolution is taking place: a movement towards what is being called Risk Management 4.0, marking a shift from static, isolated controls and audit-based oversight to dynamic, real-time ecosystems. In the emerging realm, predictive analytics

and blockchain technologies operate synergistically to enable autonomous, accountable, and adaptive risk management frameworks that are resilient to modern threats and complexities.

Organisations are exploring strategic, technology-enabled risk frameworks that bring tangible impact in their risk anticipation and mitigation lifecycles. Fundamentally, this transformation rests on a synergy between Agentic AI and blockchain technologies, which is helping redefine risk management for financial institutions. The historical reliance on isolated legacy systems, characterised by static, batch processing, has given way to a cloud-native data environment. Integrated with AI, this environment has established an ecosystem

Telecom providers are embedding AI, edge, and secure links into networks, reshaping how BFSI firms process and respond to risk signals.

in which data, algorithmic decisions, and risk controls no longer operate sequentially but interact continuously in real time.

TELECOM INFRASTRUCTURE: A KEY ENABLER

This change in the BFSI industry is being enabled by telecom and digital infrastructure providers in many ways. For instance, telecom providers are partnering with financial services to support them in use cases such as fraud prevention and transaction processing. They are embedding AI-powered monitoring, secure private connectivity, and edge computing into their networks, allowing financial institutions to process risk signals effectively.

In globalising economies such as India, banks handling high-volume digital payment flows have partnered with telecom and digital infrastructure providers to deploy low-latency private networks and edge-adjacent data centres. These architectures support real-time fraud detection and transaction-risk scoring at the point of origination, blocking malicious links in near real time across the telecom network.

Another frontier is being shaped by agentic systems coupled with blockchain's immutable and distributed ledger architecture. This combination is augmenting risk resilience for organisations, improving accountability and traceability in the compliance journey. It is enabling organisations to tap into autonomous systems. For instance, organisations can record real-time credit decisions using a permissioned blockchain or a specialised high-speed public blockchain with an efficient consensus mechanism, while minimising latency.

As financial services adopt real-time, agentic risk systems, the impact on network traffic and data processing infrastructure also grows significantly. Operations such as continuous streaming analytics and agent-to-agent communication are increasing the traffic volume within data centres and across hybrid cloud environments. This situation demands higher network bandwidth and edge computing nodes that can process risk signals closer to customers, devices, or origination points.



IN BRIEF

- BFSI firms are shifting to Risk Management 4.0, powered by AI and blockchain for adaptive, autonomous, and accountable operations.
- Telecom infrastructure is enabling real-time risk detection via private networks, edge computing, and low-latency data flows.
- Agentic AI and permissioned blockchain are helping automate credit decisions, compliance workflows, and audit trails in real time.
- BFSI players are adopting cloud-native, microservices-based platforms to integrate risk analytics closer to the data source.
- AI-driven autonomy poses new risks, such as cascading failures and model drift, requiring human oversight and explainable systems.
- Regulators and financial firms must align on governance, validation formats, and API-based integration for future-ready compliance.

Real-time risk scoring at the point of transaction is now possible through edge-adjacent data centres and private telecom networks.

Global telecom providers such as Verizon have publicly positioned private 5G and mobile edge computing as enterprise-grade foundations for low-latency, real-time decision systems. These trends highlight the growing need for such infrastructure upgrades to support fraud detection and market surveillance in the financial services industry.

BUILDING RESILIENCE THROUGH AGENTIC SYSTEMS

Several BFSI organisations have taken a step towards revamping their platforms by using microservice-based, cloud-native models. For instance, a recent finding suggests that nearly 63% of global BFSI firms have already adopted cloud microservices for real-time transaction processing, fraud detection, and customer analytics. This transformation not only delivers efficiency but also enables companies to easily integrate distributed ledger components and Agentic AI engines into their operational workflows.

However, the model does have myriad challenges. Agentic AI-driven autonomy can create new vulnerabilities, such as chained failures, in which an error in the initial AI agent cascades through the system. Organisations are also likely to face long-term systemic risks, especially if multiple institutions adopt similar AI models. Additionally, blockchain may pose challenges such as scalability, regulatory oversight, and integration with the existing BFSI estate in the future.

Risk Management 4.0 also raises other concerns, including talent readiness, regulatory adoption, cybersecurity threats posed by autonomous systems, and integration with legacy systems. The solution calls for a Human-in-the-Loop approach while simultaneously investing in a workforce that combines deep business understanding with AI fluency.

There is also a need for organisations to work in tandem with regulators and allied industry stakeholders to establish uniform governance models. Some immediate interventions may include introducing common, evidence-based validation formats to reduce the need for regulatory sandboxes and adopting API-first, adapter-

based integration patterns to safely and incrementally link advanced AI agents to legacy data infrastructure.

Regulators and industry stakeholders also need to account for the black-box challenges in which AI models make decisions or predictions based on complex internal processes that are not easily interpretable, even by their developers.

The next decade will also be defined by the convergence of Agentic AI and blockchain with the physical world, leading to three key indicators of the future. Firstly, AI-Driven Simulation is likely to establish truly anticipatory risk management by stress-testing ecosystems. Likewise, Autonomous Smart Contracts will empower AI agents to execute self-adjusting, compliance-aware rules on a blockchain in real time.

In this context, Human-in-the-Loop and AI agent integration play a critical role in mitigating redundancies. It is also expected that Explainable (X) Governance will merge XAI and blockchain auditability to ensure that every autonomous decision is transparent and globally compliant.

Risk Management 4.0 is no longer optional. It is the new operational baseline for digital-age resilience, enabling the industry to address unique challenges, including high transaction volumes, financial inclusion objectives, and multiple regulatory layers. For the BFSI sector, the ability to process risk signals in real time, automate compliance decisions, and maintain trust across distributed ecosystems will define its competitiveness.

There are already examples of homegrown AI agents being developed for the sector to automate compliance, risk, and audit functions—and this trend is likely to grow. By responsibly integrating Agentic AI's speed with Blockchain's integrity, organisations can transform their risk function from a necessary cost into a strategic engine for competitive advantage. 🧠

*The author is the Chief Digital Officer
of Anaptyss.*

feedbackvnd@cybermedia.co.in



Intelligent fibre for distributed AI ecosystems

As AI workloads stretch across hyperscale, edge, and GPU clusters, ultra-low-loss fibre and automation now define network performance and resilience.



BY ANKIT GOEL

The digital ecosystem is undergoing a structural shift. Applications and data are no longer confined to a single data centre or location. Instead, workloads are increasingly distributed across hyperscale cloud platforms, colocation facilities, enterprise captive data centres and edge environments.

This proliferation has created a highly interconnected environment in which users, applications, and systems must interact seamlessly across multiple locations, networks, and access media.

Architectures are evolving accordingly. The design philosophy has moved from scale-in to scale-out, and

Microsecond delays in GPU synchronisation can throttle AI output, turning fibre route design into a strategic lever for performance.

As workloads distribute across clouds and edge, fibre shifts from a passive conduit to the performance layer that defines AI velocity.

now to scale-across. For hyperscalers, this means distributing datasets across multiple data centres rather than consolidating them in a single facility.

The consequence is a surge in real-time data transfer between GPU clusters spread across geographies. Delivering fast responses in such an environment demands fibre quality that can sustain AI-grade performance without compromise.

FROM SCALE-OUT TO SCALE-ACROSS

In this distributed landscape, connectivity is no longer a passive utility. It has become a central enabler of performance, scale and digital experience. Enterprises expect to test AI- and cloud-based applications rapidly, deploy them at speed, fail fast when necessary and retire them just as quickly.

According to Gartner's 2024 research, more than 60% of enterprises experience performance degradation due to network latency and reliability issues. The implication is clear: connectivity must not only scale, but also flex in real time to interconnect multiple cloud providers, cloud infrastructure platforms and edge environments.

Beyond flexibility, enterprises require bandwidth that can expand on demand. AI-driven workloads, data-intensive applications, and real-time processing models place variable, often unpredictable pressure on networks.

Static provisioning models struggle to accommodate these spikes. What is required instead is an interconnected, scalable connectivity fabric that enables customers to consume capacity dynamically in line with business priorities rather than being constrained by fixed infrastructure limits.

Such ecosystems must rest on reliable, high-performance infrastructure supported by intelligent management platforms. As AI workloads expand, the underlying network must scale seamlessly without compromising latency, throughput or reliability. The

performance envelope of AI infrastructure is unforgiving. It requires precision engineering at both the physical and application layers.

FIBRE AS THE AI PERFORMANCE LAYER

AI workloads typically operate in two distinct phases: training and inference. Training involves processing large datasets to build models, which requires substantial computational capacity and sustained bandwidth. Inferencing, by contrast, focuses on real-time prediction and response, often requiring the lowest possible latency to enable instantaneous communication between AI servers hosting distributed datasets. Both phases impose different but equally stringent requirements on network infrastructure.

Ultra-low-loss fibre, typically in the range of 0.2-0.25 dB, provides additional headroom to support higher bandwidth over the same link. When combined with the shortest, most direct routes, it delivers lower latency, enabling faster synchronisation between GPU clusters and quicker presentation of processed data to the user. In GPU-to-GPU synchronisation, even microsecond delays can throttle performance and diminish the gains of advanced compute environments.

This is where fibre infrastructure becomes indispensable. Large language model training and real-time inference consume significantly higher bandwidth than traditional enterprise applications. They demand ultra-low latency, consistent performance and uninterrupted availability—requirements that fibre alone can deliver at scale.

As compute migrates toward high-density GPU clusters and distributed architectures, fibre forms the physical backbone that allows geographically dispersed data centres and edge locations to function as a unified compute ecosystem.

Conventional terrestrial fibre typically exhibits losses in the range of 0.4 to 0.6 dB per kilometre, limiting the ability to transmit large capacities over long distances without amplification. As AI scales, demand for lower-

Hollow-core fibre trials signal a structural rethink of latency engineering, promising faster inter-data-centre synchronisation at scale.

loss, lower-latency fibre will intensify. Hyperscalers are already experimenting with hollow-core fibre technologies that promise not only higher capacity but also latency reductions of up to 33%.

These innovations are not incremental enhancements; they represent foundational shifts in how performance is engineered across digital infrastructure.

AUTOMATION AND INTELLIGENT OPERATIONS

Fibre is critical, but it does not complete the equation on its own. As networks expand in scale, complexity and geographic reach, traditional manual operating models struggle to keep pace. Managing performance, reliability and quality of service in dense fibre environments requires a fundamentally different operational approach.

Intelligent automation has therefore emerged as a parallel enabler of scalable, high-performance connectivity. Advanced fibre monitoring technologies, such as Remote Fibre Monitoring Systems (RFMS), enable operators to observe and assess the entire fibre infrastructure in near-real time. Operating continuously and autonomously, these systems detect anomalies, degradations or faults before they escalate into service-impacting incidents.

The result is improved reliability, reduced mean time to repair and greater operational resilience.

When integrated with OSS and BSS platforms, intelligent monitoring extends beyond fault detection. It enables automated alarm generation, accurate fault localisation, workflow initiation and faster resolution cycles. In effect, the infrastructure begins to operate at the speed of demand. Automation transforms fibre from a passive asset buried beneath the ground into an actively managed, data-rich platform that responds dynamically to network conditions.

TRANSPARENCY IN A CONNECTED ECOSYSTEM

As enterprises increasingly consume connectivity across multiple clouds and geographies, transparency, visibility and control become equally critical. Dynamic

consumption models require precise insight into how services perform and how capacity is utilised.

Customer-facing digital platforms address this need by offering granular visibility into fibre and network performance—path by path and fibre pair by fibre pair—across different segments and layers of infrastructure. Such transparency enables enterprises to align network usage directly with business outcomes. It supports better planning, faster decision-making and greater confidence in service reliability.

Fibre design itself is evolving in response to these demands. Innovations such as ultra-low-loss fibre and hollow-core fibre are emerging to support long-distance, high-capacity inter-data-centre connectivity with improved latency characteristics and more efficient transmission over extended distances. These advances strengthen fibre's position as a strategic asset in AI-powered economies, reducing cost per transmitted unit while enhancing performance thresholds.

The future of connectivity lies in a fully interconnected ecosystem powered by intelligent fibre infrastructure. Fibre is no longer merely a conduit for data; it is becoming a dynamic platform enriched by automation, analytics and data-driven operational intelligence.

"Intelligence in Fibre" encapsulates this shift. It reflects the effective integration of advanced technologies, automated operations and intelligent management to deliver measurable business outcomes—higher reliability, faster deployment cycles, scalable performance and improved customer experience.

As India enters the era defined by distributed AI, hyperscale data centres, and next-generation digital services, competitive advantage will depend not only on fibre deployment but also on how intelligently it is designed, operated, and consumed. 🌐

The author is the Founder and Chairman of the Space World Group.

feedbackvnd@cybermedia.co.in



Secure SD-WAN: Foundation of a true SASE design

Hybrid work and multi-cloud sprawl are forcing enterprises to unify networking and security into a single architecture that delivers control, performance and resilience.



BY VIVEK SRIVASTAVA

As organisations invest in secure access service edge (SASE) solutions, they are evaluating both security and networking functions. The right SD-WAN solution is critical to enabling a truly effective SASE architecture. A unified SASE framework built on secure SD-WAN provides consistent security, optimised connectivity, and unified

management for users and applications across hybrid and cloud environments.

Two major factors are driving organisations to adopt SASE. The first is the rise of the hybrid workforce, now a standard operating model across many industries. The second is the shift to digital-

As SD-WAN evolves from a connectivity tool to a security platform, the depth of its integration determines whether SASE delivers real architectural value.

Identity, context and device posture now anchor access decisions, redefining perimeter security in distributed enterprise environments.

first strategies. Most organisations have adopted, or plan to adopt, digital-first approaches, with workloads increasingly distributed across public and multi-cloud environments. SASE is designed to support the dynamic and secure access needs of today's organisation. It plays a critical role in ensuring that security can be delivered anywhere — at the WAN edge, cloud edge, data centre edge and even endpoint devices used by a hybrid workforce.

Gartner predicts that by the end of 2026, nearly 60% of new SD-WAN purchases globally, including India, will be part of a single-vendor SASE offering — a significant increase from 15% in 2022. It also projects that 47% of enterprises will have deployed SASE by 2027, with many CISOs moving away from fragmented legacy architectures towards unified platforms to manage AI-related data risks. According to Coherent Market Insights, the India SASE market is expected to reach USD 2,136.6 million by 2032, growing at a compound annual growth rate (CAGR) of 22.1%.

Organisations typically begin their SASE journey in one of two ways: by connecting SD-WAN to secure service edge (SSE), or by integrating SSE with SD-WAN. In both approaches, success depends on unifying networking and security capabilities, maintaining consistent policy enforcement for on-premises and remote users, and leveraging agentic AI to strengthen defences and simplify operations.

What, then, are the SD-WAN capabilities that make it the cornerstone of an effective SASE deployment?

CONVERGED SD-WAN SECURITY AT THE EDGE

For years, SD-WAN has transformed enterprise networking by enabling organisations to transition away from costly MPLS circuits while maintaining reliable broadband performance. It introduced intelligent traffic steering and centralised management to enhance user experience and simplify operations. Its most important evolution today is the integration of advanced security into a single platform, powered by a single operating system and unified management.

This integration delivers significant advantages when expanding to SASE. It enables secure local internet breakout without backhauling traffic to the data centre, SSE, or chaining services to additional security devices. By reducing latency and minimising the number of hops to the final destination, organisations can provide direct connectivity to applications and enhance user experience. Secure site-to-site communication can also be maintained without routing traffic through an SSE point of presence (POP), optimising overall performance.

ZERO TRUST ENFORCEMENT ACROSS TRAFFIC FLOWS

As organisations adopt universal zero-trust network access (ZTNA) to ensure granular, secure access regardless of user or application location, embedding a ZTNA application gateway within the SD-WAN solution is critical. This integration allows organisations to enforce ZTNA tags and policies directly within the network fabric.

Beyond user-to-application access, advanced security capabilities within secure SD-WAN also reduce the attack surface by protecting east-west traffic. This is particularly important in distributed environments where traffic flows between branches, data centres, and cloud workloads, and where data must be inspected and secured without introducing performance bottlenecks.

Integrated security and ZTNA enforcement ensure that users and applications connect safely, but performance and reliability are equally important. Once traffic is secured, SD-WAN's intelligence in steering applications across multiple networks becomes the next key factor in delivering a seamless experience. This is especially relevant as organisations balance on-premises infrastructure, cloud deployments and SaaS workloads.

INTELLIGENT STEERING ACROSS CLOUD WORKLOADS

As applications are distributed across data centres, clouds, and SaaS environments, SD-WAN must intelligently steer traffic for each request. With application-aware routing across thousands of applications and integrated security capabilities, secure SD-WAN can direct SaaS

True SASE maturity depends less on bundling tools and more on native integration across SD-WAN, SWG, CASB, ZTNA and FWaaS.

traffic without requiring an SSE POP at the outset. This reduces network hops and lowers latency.

Resilient application steering also includes optimising traffic flows from SSE POPs to applications. For remote users accessing private applications, this ensures both performance and availability. Intelligent, adaptive path selection helps maintain a consistent user experience even under fluctuating network conditions.

AI-DRIVEN OPERATIONS FOR RESILIENT NETWORKS

In distributed environments, accelerating troubleshooting, configuration and policy enforcement is essential. Enhanced visibility from branch to application through digital experience monitoring (DEM) strengthens operational control. Predictive anomaly detection powered by AI-driven operations, including agentic AI, helps maximise uptime and sustain performance.

AI-enhanced SD-WAN reduces operational friction by automating repetitive tasks, identifying potential issues before they escalate, and improving overall service reliability within a unified SASE framework.

UNIFIED MANAGEMENT FOR POLICY CONSISTENCY

As organisations scale towards SASE, SD-WAN's ability to integrate with SSE and simplify management becomes a defining capability. Unified management ensures consistent policy enforcement across a hybrid workforce and distributed infrastructure. It also accelerates the deployment of connectivity and cloud security services by providing a single control plane for configuration and oversight.

Purpose-built application-specific integrated circuits (ASICs) further strengthen this foundation. By accelerating networking and security functions in hardware, ASICs offload compute-intensive tasks and maintain high performance even as inspection and encryption demands increase.

DEPLOYING SASE ON SECURE SD-WAN CORE

Before deploying SASE, organisations must clearly

identify the core problems the architecture is intended to address. Common drivers include securing hybrid workforces with consistent access policies, improving application performance for remote and branch users, reducing complexity caused by managing multiple point solutions, and meeting compliance requirements across geographies and industries.

Clarifying these objectives guides architectural decisions and deployment sequencing, whether the organisation is re-architecting its WAN, consolidating cloud security tools, or pursuing both in parallel. At its core, SASE unifies SD-WAN, secure web gateway (SWG), cloud access security broker (CASB), zero-trust network access (ZTNA) and Firewall-as-a-Service (FWaaS). True unification means integrating these capabilities natively rather than merely bundling them under a single brand.

In a perimeter-less environment, identity becomes the primary security anchor. SASE architectures must support dynamic access controls that evaluate not only user identity but also contextual factors such as device posture, location, time of access and behavioural risk indicators. At the same time, not every organisation is prepared to transition immediately to a fully cloud-native model. An effective SASE strategy should therefore support both cloud-delivered and hybrid architectures, enabling alignment with existing infrastructure, geographic constraints and compliance requirements.

A unified SASE architecture does more than consolidate tools; it also simplifies their management. Building tomorrow's SASE framework on a secure SD-WAN foundation delivers measurable benefits. Centralised management and self-healing capabilities reduce downtime. Intelligent traffic steering and purpose-built ASIC acceleration enhance application performance. Simplified operations lower the total cost of ownership. Together, these capabilities position secure SD-WAN as the essential foundation for a scalable and resilient SASE deployment. 🌟

The author is the Country Manager, India & SAARC at Fortinet.

feedbackvnd@cybermedia.co.in



The flight deck layer for autonomous AI networks

As AI networks act autonomously, embedded observability is evolving into a governing layer that orchestrates telemetry, policy and real-time corrective action.



BY SIMON RIZKALLA

For technology leaders who have spent decades in the trenches of distributed systems, observability was akin to forensic archaeology. Engineering teams spent nights digging through disparate logs and fragmented traces, trying to reconstruct a crime scene after a critical service had failed.

We are now in the era of autonomous, AI-driven networks, where these reactive approaches pose an existential risk. C-Level technology leaders recognise that the world is moving away from a deterministic, “if-then” logic to a probabilistic reality, one shaped by agentic AI and self-healing infrastructures.

In this new age, observability must transcend its role as a diagnostic window to a true control plane, the nervous system dictating how intelligent networks operate, scale, and protect themselves.

FROM REACTIVE MONITORING TO ACTIVE CONTROL

The black-box nature of an AI-driven network’s decision-making poses a major challenge for organisations. Traditional monitoring tools, built for static environments, are blind to the nuances of prompt engineering, vector database latency, and LLM and AI agent hallucinations. When an AI agent reroutes network traffic or allocates

AI agents rerouting traffic and reallocating compute demand more than logs; they require contextual telemetry embedded directly in the execution path.

new compute resources based on a shifting model, it is not following a scripted model; it is responding to data patterns.

If observability is outside this decision-making loop, organisations have limited insight into how their networks are performing. A true control-plane approach integrates intelligent observability into the execution path by providing unified context. It correlates telemetry from GPU clusters through the application's semantic layer, enabling teams to set guardrails rather than react to alerts.

By creating a feedback loop in which the system detects a logical deviation and automatically steers the network back toward the desired state, observability becomes proactive.

BREAKING THE COST OF TOOL FRAGMENTATION

The 2025 Observability Forecast by New Relic found that the most significant barrier to reliability is tool sprawl. Even today, many infrastructure, development, and security teams rely on dashboards in separate, siloed tools. In an AI-powered environment, fragmentation is a tax on innovation.

AI models thrive on high-quality, high-cardinality data. When it is trapped in silos, it throttles network intelligence. This is why the industry is moving towards a unified system. By consolidating metrics, events, logs, and traces into a single entity, organisations can achieve full-stack visibility.

This consolidation is not just about reducing licence costs but also about ensuring AI networks have a comprehensive map to manage. When intelligent observability acts as a control plane, it provides the "ground truth" that can prevent AI-driven automation from spiralling into a cycle of cascading failures.

BRIDGING THE AI OPERATIONS SKILLS GAP

For years, troubleshooting bottlenecks was hindered by a gap in expertise or the need for a specialist to know the exact query syntax to find the needle in the haystack. This is shifting towards a "natural language" operations model, with autonomous systems becoming the norm.

The most advanced observability control planes are leveraging AI to bridge the expertise gap. Imagine a system where an engineer can ask, "Why is latency increasing for our users in India?" and the system, acting as an intelligent agent, scans the entire stack, identifies the bottleneck in a specific microservice and suggests remediation.

This is what an intelligent observability platform that understands the underlying context looks like. By integrating these capabilities into common developer environments and communication tools, everyone has visibility, democratising the ability to manage complex AI-powered networks.

ENGINEERING PREDICTABILITY INTO AI SYSTEMS

In 2026, the value of observability will be measured by its ability to offer predictability. Today, high-impact outages cost a median of USD 2 million per hour. At a time when autonomous networks are becoming the norm, C-level leaders need their operations to move at speed. The delay between "something is wrong" and "we know why" is where the most damage is done.

By treating observability as a control plane, organisations adopt a preventive posture, monitoring drift in model performance or saturation in a network buffer before failure occurs. Observability is moving from "monitoring the network" to "governing the intelligence" that runs the network.

For those who have lived through the evolution from monolithic servers to microservices, and now to agentic AI, the mandate is clear: stop treating observability as an insurance policy and view it as an instrument for predictability. Networks of the future will be governed by intelligent platforms that see everything, understand context and help teams act with precision. That is the power of an observability control plane. 🧠

The author is the Vice President – Customer Advocacy for the APJ region at New Relic.

feedbackvnd@cybermedia.co.in



TO STAY AHEAD OF THE CURVE IN TELECOM READ VOICE&DATA

**Celebrating
Dataquest
40 years:
Avail Special
discount
on V&D.**



**Digital
subscription
also available on
Magzter, Zinio,
Readwhere,
& Readly**



Book Digital Subscription Now!

Yes! I want to subscribe to Voice&Data



Scan QR Code
& Subscribe now...

Subscribe to Digital Edition @ ₹735/-

Period	Issues	Print Subscription Rate		Digital Subscription Rate
		New	Renewal	
☐ 1 year	12	₹1,140/-	₹1,050/-	₹735/-
☐ 2 years	24	₹2,190/-	₹2,020/-	₹1,470/-
☐ 3 years	36	₹3,285/-	₹3,020/-	₹2,205/-

or **Subscribe online:** subscriptions.cybermedia.co.in/voicendata

Please tick your subscription choice above, fill the form below in CAPITAL LETTERS and mail it to us at subscriptions@cybermedia.co.in

☐ I want to avail premium service of receiving your copy by courier. Tick which ever is applicable.

☐ ₹ 600/- 1 year ☐ ₹ 1200/- 2 years ☐ ₹1800/- 3 years

Name [•]: Mr/ Ms _____ Date of Birth:

Organisation: _____ Designation: _____

Delivery Address: _____

City: _____ State: _____ Postal Code:

Mob [•]: Tel: Email [•]: _____

GST No. [•]: PAN No. [•]:

☐ I am paying ₹ by DD/Cheque No.: Dated:

Payable at (specify bank and city) _____

OR

☐ Please Remit for ₹ Through RTGS/NEFT to our A/C details given below:

Bank Name: ICICI Bank Limited, A/c no. 017705000132, Branch & IFS Code: Gurgaon, ICIC0000177

[•] Essential fields

Signature _____ Date: Subscription No. (for renewal) _____

Order form can be mailed with payment (cheque/DD) to:

Cyber Media (India) Ltd, Cyber House, B-35, Sector-32, Gurgaon-122003

Contact: Alok Saxena, Tel: 0124-4237517 (Extn-347), 91+9953150474, Email: aloksa@cybermedia.co.in

For Subscription queries:

9289870545

Terms & Conditions: _____

• This offer is valid for a limited period. • Rates and offer valid only in India. • NEFT/UTR No., Email & Mobile number mandatory. • Please allow 4-6 weeks for delivery of your first copy of the magazine by post. • Send crossed Cheques in favour of Cyber Media (India) Ltd. • Please write your name and address on the reverse side of the cheque or DD. All outstation cheques should be payable at par. • Cyber Media (India) Ltd. will not be responsible for postal delays, transit losses or mutilation of subscription form. • Cyber Media (India) Ltd. reserves the right to terminate or extend this offer or any part thereof. The decision to accept or reject any or all forms received is at the absolute discretion of the publishing company without assigning any reason. • Please include pin code for prompt delivery of your copy. • In case payment is through credit card, date of birth must be mentioned. • All disputes shall be subjected to Delhi jurisdiction only.

Beyond the 5G rollout, the age of execution

Industry leaders at the V&D 5G+ Conference debate how India can turn network scale into resilient, intelligent systems that deliver economic value.



BY VOICE&DATA BUREAU

On the winter morning in New Delhi, when policymakers, telecom operators, technology vendors, defence specialists and manufacturing leaders assembled at the Voice&Data 5G+ Conference 2026, the atmosphere was different from the exuberant years that followed India's 5G roll out story. There were no celebratory charts on coverage expansion or headline-grabbing subscriber numbers.

Instead, there was a sharper, more difficult conversation underway.

India has built scale. The country has rolled out 5G at unprecedented speed, digitised payments, built digital public infrastructure and connected vast swathes of its population. But what, precisely, has this infrastructure

matured into? And more importantly, what must it become if India is to translate connectivity into sustained economic capability by 2047?

Across panels and firesides, the theme of Digital Infrastructure for Viksit Bharat took on a clear meaning: expansion has peaked; execution must begin.

INFRASTRUCTURE SETS NEW BASELINE

Welcoming the dignitaries and participants, Pradeep Gupta, Chairman, CyberMedia Group, positioned infrastructure as central to empowering industries, modernising public services and expanding India's global digital footprint. He described the conference as a collaborative platform for policymakers, operators, vendors and industry bodies.

India's 5G expansion has peaked; the next phase demands intelligent, energy-efficient networks that deliver consistent performance at national scale.

Atul Gupta, Partner and Head – Digital Trust and Cyber at KPMG India, framed telecom networks as “digital gateways” and “digital highways” that have enabled inclusion at scale. He said the sector is shifting from a telco to a techco model, where operators move beyond connectivity to deliver integrated digital services.

Gupta identified infrastructure transformation, AI adoption and trust as the three forces shaping this shift. AI, he said, has progressed from generative models to agentic systems capable of autonomous decision-making. However, he warned that AI is a “double-edged sword” that can also empower threat actors. Responsible AI f

eworks and governance mechanisms must therefore become embedded across digital systems. “The real currency in a digital economy will be trust,” Gupta said.

Lt Gen Dr SP Kochhar, Director General, COAI, said India has emerged as a major telecom market supported by private investment and public policy. However, he argued that telecom should be treated as a foundational horizontal service underpinning every sector. He called for long-term spectrum planning and cautioned against treating spectrum allocation primarily as a fiscal instrument. Kochhar also highlighted operational challenges, including connectivity in public spaces and cybercrime reporting, that require coordinated reform.

Ambika Khurana, Chief Regulatory and Corporate Affairs Officer at Vodafone Idea, stressed the need for a network-first approach to economic growth. She pointed to bottlenecks in right of way approvals, public infrastructure access and reliable power supply. Telecom, she said, should be granted utility status, with a consultative regulatory framework. Satellite communications can complement terrestrial networks if policy alignment is clarified.

Pankaj Mahindru, Chairman of ICEA, linked digital infrastructure to India's aspiration of becoming a USD 40 trillion economy. He said India must shift from being a technology consumer to a technology creator, strengthening semiconductor manufacturing, display production and product design alongside mobile device assembly.

Ravi Gandhi, President and Chief Regulatory Officer at Reliance Jio, said coverage expansion has been significant, but device affordability, digital literacy and fixed-line penetration remain gaps. He compared cybersecurity awareness to traffic discipline on newly built highways, arguing that consumer education is essential to secure digital growth.

Sandeep Saxena, Head – Technology and Solutions, Mobile Networks at Nokia India, said networks must evolve to support AI-driven devices, edge computing and real-time applications. High-reliability connectivity is essential for critical communications, immersive services and industrial automation. Networks, he said, must become intelligent and energy-efficient to support the fusion of physical and digital systems.

FROM ACCESS TO MEASURABLE OUTCOMES

Sharing the Industry outlook, Prabhu Ram, Vice President – Industry Research Group, CMR, said India must now move beyond expanding connectivity and focus on building digital capability to achieve its Viksit Bharat 2047 vision.

He described the past decade as one centred on expanding access through affordable smartphones, nationwide 4G networks and digital public platforms. The next phase, he said, will focus on delivering measurable outcomes through predictable and resilient infrastructure. “The last decade was about building access. The next two decades are about delivering outcomes,” Ram said.



Prabhu Ram

Telecom must shift from connectivity growth to accountable digital services that drive measurable enterprise and public sector outcomes.

Calling this shift as an architectural transition, where networks evolve from enabling participation to ensuring consistency and trust, he stressed that AI-native networks will be central to this change. "They are sensing conditions, predicting congestion and acting autonomously within defined limits," Ram said, adding that India's policy direction, digital platforms and AI-ready workforce create favourable conditions.

Ram identified manufacturing, healthcare, agriculture, logistics and energy as sectors where capability-driven infrastructure will shape growth. From autonomous production lines to real-time diagnostics and smart ports, reliable networks will underpin productivity gains. "The question is not whether this transformation will happen, but how effectively it is implemented," he said.

AI NATIVE NETWORKS TAKE CENTRE STAGE

In a session moderated by Sunil David, digital technology consultant and former regional director for IoT at AT&T in India and Asia, panellists examined how 5G must evolve into AI-enabled, intent-driven network operations. "The real question is what outcomes 5G is delivering, sustainably and at scale," David said, arguing that AI must move from being an overlay to forming the core of closed-loop network systems.

Arvind Bali, Vice Chairman and Board Advisor at Globe Teleservices, said networks must evolve from reactive systems to programmable and predictive platforms. AI, he said, can prevent incidents in areas such as security

and fraud rather than merely analyse them after the event.

Sudakshana Laha, Head of Services for MSIT and ADM Cloud Software and Services at Ericsson, said monetisation depends on embedding AI across network, IT and business layers. "Ultimately, revenue is realised only to the extent that OSS and BSS systems allow it," Laha said, outlining a phased approach from automation to intent-based autonomy.

Amit Sethi, Head of 5G Solutions at TCS, said enterprise 5G projects often stall between proof-of-concept and scaled deployment due to spectrum constraints and unclear return on investment. Amit Sinha Roy, Senior Advisor for Digital Ecosystems, Alliances and Innovation, called for stronger ecosystem partnerships and outcome-based service models. The session concluded with the panellists noting that AI-native, resilient and programmable networks will underpin enterprise transformation and public digital services as India advances towards 2047.

TELCOS RECAST ROLE IN ENTERPRISE ERA

Switching gears, the second panel discussion focused on how telcos must reposition themselves as technology partners delivering measurable enterprise outcomes rather than relying on connectivity-led growth.

Moderating the discussion, Jaideep Ghosh, former Partner at KPMG, highlighted that with connectivity nearing saturation, the traditional growth model based on expanding coverage and adding subscribers has reached its limits. "Connectivity has become just the starting point and not the only solution that consumers, both retail and enterprise, are looking for," he said, framing the shift from telcos to techcos as essential for sustained revenue growth.

Rakhee A Chachra, Global Research Leader (TME), Institute of Business Value, IBM, said enterprise expectations have evolved faster than telecom business models. Citing IBM research, she said many communication service providers still expect 70–80% of enterprise growth from connectivity, while enterprises increasingly demand accountability for business outcomes. "They want someone to take accountability



(From L to R) Sunil David, Arvind Bali, Sudakshana Laha, Amit Sethi, and Amit Sinha Roy.

AI-native, self-healing networks are emerging as the foundation for sustainable telecom economics and resilient digital public systems.



(From L to R) Salil Khanna, Sukhjit Singh, Rakhee A Chachra, and Jaideep Ghosh.

and ownership for outcomes,” Chachra said, adding that real-time dashboards, APIs and integrated service models are now baseline expectations.

Salil Khanna, National Head – Customer Operations, Enterprise Business, Reliance Jio, said networks alone do not deliver business impact. Operators must align 5G, cloud and AI capabilities with enterprise workflows across supply chains and operations. “I am not here to sell you connectivity or a pipe. I am here to deliver value into the business processes that you are running,” Khanna said.

Sukhjit Singh, CTO and Director – Technical, AT&T Asia Pacific, said scale-led growth is tapering globally, with enterprises demanding measurable returns rather than incremental speed gains. The panellists stressed that ecosystem partnerships, outcome-based models and sustainable infrastructure strategies are likely to define the next growth phase for telecom operators.

MANUFACTURING DEMANDS DETERMINISM

Sharing insight during a fireside chat on how manufacturing environments are reshaping network expectations, Gaurav Mathur, Vice President – Information Technology at Samvardhana Motherson International, pointed out that enterprise leaders are now redefining expectations from telecom networks, demanding measurable business outcomes rather than basic connectivity.

Highlighting that it not long back, connectivity was only about user experience, he said that the model was



Gaurav Mathur (left) and Ashok Pandey.

now changing with manufacturing environment getting digitally integrated. “Now, the real consumer of IT is my shop floor, not my office. Everything is connected, everything is real time,” he said.

He explained that outages in digitally integrated factories translate directly into revenue loss. Manufacturing Execution Systems, robotics and cloud platforms require predictable latency and uninterrupted performance. Fragmented infrastructure across providers often leaves enterprises without accountability during failures.

Mathur argued that enterprises need intent-based, outcome-driven networks with clear accountability across multiple providers. “Fragmented infrastructure, spanning private wireless, data centres and last-mile links, often leaves enterprises without ownership during outages,” he stated.

While private 5G holds potential, adoption remains limited due to ecosystem gaps. “Machine manufacturers are still not recognising 5G as a medium to support operations,” he said, calling for closer collaboration between telecom operators, vendors and enterprises to align networks with industrial process requirements.

The session that was moderated by Ashok Pandey, Executive Editor of PCQuest and DQ Channels

SECURING MISSION CRITICAL SYSTEMS

The conference also saw defence specialists, telecom

Manufacturing floors and mission-critical services are redefining reliability, where outages translate directly into financial and operational risk.

executives and technologists deliberate on how India must resolve policy, spectrum and governance questions to build a resilient mission-critical communications framework capable of supporting public protection, disaster relief and secure government operations.

Moderated by Col (Rtd) Dr Sidharth Shukla, the panel examined fragmentation across existing agency networks. Shukla said multiple systems built on different architectures create “blind spots”, particularly during the first minutes of an emergency when coordination is vital. He argued that interoperability and zero-trust principles must be embedded at the design stage, suggesting that a dedicated public protection and disaster relief (PPDR) network combining exclusive spectrum with satellite and fibre overlays could address structural gaps.

Dharmendra Khajuria said global models such as those adopted in the US and UK emerged after major crises, but cautioned against direct replication in India. He noted that operators already support intra-circle roaming during disasters, though this may not meet full mission-critical requirements. The key question, he said, is whether India should build a separate PPDR network or prioritise traffic within existing commercial infrastructure.

Col (Rtd) Shantanu Das supported allocating separate spectrum aligned with device ecosystems, while acknowledging that network slicing and reserved

capacity within 4G and 5G systems could meet many needs if governed effectively.

Sunil David emphasised identity management and policy-driven pre-emption to ensure priority access without destabilising public networks. Prashant Chugh highlighted post-quantum risks to public-key cryptography, saying India is developing indigenous capabilities under the National Quantum Mission.

The panellists agreed that centralised standards, zero-trust security and quantum-safe migration plans will determine India’s readiness for secure critical communications.

DEEP-TECH MOVES FROM LAB TO MARKET

Another key aspect of the conference was its focus on R&D investments to drive technology independence and economic growth.

“India is shifting from promoting innovation to building a scalable deep-tech backbone that can convert scientific strength into economic outcomes,” Dr Jyoti Sharma, Head of the RDI Cell at the Department of Science and Technology (DST), Government of India, said.

Sharma said the past decade focused on strengthening innovation through mission-driven programmes such as the National Supercomputing Mission, National Quantum Mission, India Semiconductor Mission and National



(From L to R) Prashant Chugh, Col (Rtd) Santanu Das, Dharmendra Khajuria, Sunil David, and Col (Rtd) Dr Sidharth Shukla.



Dr Jyoti Sharma (left) and Pradeep Gupta.

Cyber resilience is now a strategic priority, as state-linked intrusions target telecom infrastructure for long-term intelligence access.

Green Hydrogen Mission. These initiatives, she said, demonstrate capacity building across interdisciplinary domains rather than isolated research efforts.

India's innovation metrics have improved, with higher Global Innovation Index rankings, rising patent filings and strong PhD output in science and engineering. Startup activity has expanded significantly. However, she pointed out that there were structural gaps that limited commercialisation of deep-tech. "India invests about 0.6–0.7% of GDP in research and development, with private sector contribution at 36.4%, below global benchmarks. Research output remains concentrated in a small number of institutions, while funding gaps, regulatory friction and long gestation cycles slow scale-up."

To address this, the government established the Anusandhan National Research Foundation in 2024 to align research with industry demand. A Rs 1 lakh crore Research, Development and Innovation Fund has been launched to support industry-led deep-tech projects from Technology Readiness Level 4 onwards, offering long-tenure, low-interest financing.

Sharma said closer collaboration between scientists and industry will be essential to translate research into deployable technologies supporting India's 2047 vision.

AI RESHAPES TELECOM ECONOMICS

Telecom economics is being reshaped by artificial intelligence, evolving traffic patterns and the growing need for low-latency services, Randeep Singh Sekhon, CTO of Bharti Airtel, said in a fireside chat with Jaijit Bhattacharya, Founder and President, Centre for Digital Economy Policy Research.

Sekhon said AI has not yet increased overall traffic volumes significantly, but it has altered traffic flows. User queries are shifting from traditional search engines to AI platforms, while future real-time AI applications will demand different network architectures. The inflection point, he said, will come when AI workloads move to the edge. "When AI sits at the edge, latency becomes critical," Sekhon said, noting that applications such as smart



Randeep Singh Sekhon (left) and Jaijit Bhattacharya.

wearables and real-time decision systems will require distributed computing and intelligent routing.

India's data consumption continues to rise, driven by high-resolution video and interactive services. While downlink traffic remains dominant, uplink capacity is becoming more relevant for cloud and AI interactions. "Our two pillars are very clear – customer experience and cost to serve," Sekhon said.

Energy is now the largest operating expense for networks. Airtel is using AI to optimise capacity, powering down surplus resources during low-traffic hours while maintaining coverage. AI systems are also deployed to detect fraudulent links and prevent call forwarding scams.

On satellite connectivity, Sekhon said terrestrial fibre and mobile networks will remain primary, with satellite services addressing remote and emergency use cases.

STATE LINKED THREATS TARGET TELCOS

Telecom operators worldwide are facing sustained, state-linked cyber intrusions aimed at strategic intelligence rather than financial theft, David Sehyeon Baek, Founder and CEO of PygmalionGlobal, said, citing cases in Asia, the United States and Europe.

Baek said recent incidents in Singapore and South Korea demonstrate how attackers are targeting core routing and interconnection systems to gain persistent

R&D investment and deep-tech commercialisation will determine whether India moves from digital adoption to genuine technology ownership.



Presentation through VC by David Sehyeon Baek..

access. In Singapore, a China-linked group targeted Singtel's infrastructure, while in South Korea, an intrusion at SK Telecom triggered a national-level probe. In both cases, there was no evidence of ransomware or data resale. "State-sponsored actors want to observe traffic patterns, map relationships and understand how networks are managed," Baek said.

In the United States, investigations involving major carriers found that some intrusions remained undetected for several years. Attackers blended into routine network activity, avoiding disruption while studying workflows and metadata flows. The prolonged invisibility of such breaches, Baek said, represents a strategic risk.

Telecom networks are attractive targets because they provide nation-scale visibility into government, defence, financial and civilian communications. Lessons from the Ukraine conflict further underscored the importance of resilient and redundant communications during crises.

For countries such as India, Baek said telecom security must be treated as a national security priority, requiring advanced detection capabilities, coordinated governance and infrastructure resilience beyond standard compliance frameworks.

ALIGNING VISION AND ROADMAP FOR 6G

A key aspect of the conference was the discussion on India's 6G blueprint and what the country must do to



(From L to R) Rajesh K Pathak, Nirmesh Yadav, Monika Gupta, Ashwini Kumar, and Jaspreet Singh.

translate its vision to reality. The session moderated by Jaspreet Singh, Partner at Grant Thornton Bharat, highlighted that India must align research, standards, spectrum and ecosystem readiness over the next five years to translate its Bharat 6G Vision into commercial deployment by 2030.

Rajesh Kumar Pathak, Director General, Bharat 6G Alliance, said India's roadmap, unveiled in 2023, provides a foundation but requires coordinated execution. "It is not one thing, it is everything," Pathak said, stressing that government-backed R&D, early telecom operator participation and industry-academia collaboration must progress in parallel.

Nirmesh Yadav, GM and Head – Emerging Technology and Industry Alliance, Bharti Airtel, said 6G should be driven by demand rather than technology cycles. "It has to be driven by use cases and industry demand," Yadav said, cautioning that monetisation challenges seen in 5G must not be repeated.

Monika Gupta, Vice President at Capgemini, said India should selectively prioritise capabilities aligned with domestic needs while observing global experimentation. Ashwini Kumar, Head of Standards and Spectrum Engagements at Nokia Solutions & Networks, highlighted lessons from 5G, noting that application ecosystem development must accompany technology rollouts.

India's 6G ambition will hinge on coordinated research, spectrum planning and ecosystem execution—not vision statements alone.

On standards and global positioning, Pathak said India is working with international bodies to ensure domestic research feeds into global frameworks. Emerging focus areas include the FR3 spectrum band, integrated sensing and communication and energy efficiency.

Singh summed up that India's scale and digital public infrastructure could support 6G leadership, provided investments remain affordable, modular and outcome-oriented.

DESIGN LED MANUFACTURING IMPERATIVE

The conference concluded with a fireside chat on Make in India and why the country must move beyond assembly to build design-led, technology-driven manufacturing if it aims to achieve digital self-reliance.

Sharing insights from his electronic sector manufacturing experience, Avneet Singh Marwah, CEO of Super Plastronics, said that India's electronics manufacturing landscape has shifted significantly since 2020, supported by policy measures such as production-linked incentives. "Mobile devices now account for a large share of output, and exports are rising. However, value addition remains limited," he said.

Tracing the decline of domestic manufacturing in the early 2000s, Marwah said imports became cheaper than local production, pushing many firms towards trading models. The pandemic exposed the risks of import dependence and triggered a renewed focus on indigenous capability. "That is when everyone realised how dependent we were," he said.



Pradeep Gupta (left) and Avneet Singh Marwah.



Marwah stressed that sustained investment in research and development is essential. "Any brand not looking seriously at R&D is playing a very short-term game," he said, noting rapid technological change across devices and networks.

While localisation has progressed in components such as mechanical parts and modules, displays and semiconductors still account for most product value. He said semiconductor initiatives, even if starting with packaging, are strategically important. Marwah added that scale, infrastructure readiness, policy stability and reduced procedural friction will determine whether India can compete globally and move from manufacturing to technology ownership.

As the sessions drew to a close, the deliberations converged on a defining inflection point for India's telecom and digital ecosystem. While infrastructure has been built at scale and platforms have been adopted nationwide, the Digital India story is entering a second phase.

The next challenge is ensuring that networks are intelligent, secure, energy-efficient and accountable enough to deliver measurable economic and social outcomes. If India can align policy, technology, manufacturing and governance around that objective, the ambition of Viksit Bharat 2047 may rest not just on how widely the Internet reaches, but on how effectively it performs. 🌟

feedbackvnd@cybermedia.co.in

Businesses rethink infrastructure as AI takes control

As autonomous systems move into core business operations, the industry is reworking AI infrastructure to close gaps in governance, visibility, and control.



BY SHUBHENDU PARTH

For years, digital infrastructure functioned quietly in the background as a collection of data centres, APIs, cloud services, and pipelines engineered to keep systems running. It processed workloads, scaled compute, and ensured business continuity.

However, this is changing in 2026. Today, infrastructure is no longer passive. Instead, it is being reshaped to participate—to govern, interpret, and, in some cases, decide. The trend is also reflected in three recently published studies—Cisco’s 2026 Data and Privacy Benchmark, New Relic’s AI Impact Report, and HCLSoftware’s Tech Trends 2026.

The reports suggest that the change is not about accelerating cloud migration or modernising data pipelines incrementally. Rather, it is about building trusted, observable, explainable, and adaptive infrastructure because it operates beneath systems that think and act.

This transformation, the reports establish, is being driven by a single force: artificial intelligence (AI). And not just AI as a tool, but AI as an actor—systems that can analyse, reason, and execute autonomously. Enterprises are no longer just deploying AI in applications; they must rethink how infrastructure enables and governs intelligence at scale.

AI-powered observability platforms now interpret signals, reduce operational noise and accelerate root cause analysis across complex environments.

The shifts are also exposing a widening gap between the pace of AI capability advancement and the pace of underlying infrastructure adaptation to support them.

AI HAS ENTERED THE STACK. IS IT READY?

While AI is rapidly being integrated across all digital assets, experts note that the gap between rapidly advancing AI systems and slower-moving infrastructure foundations is becoming difficult to ignore. According to the Cisco report, while 90% of organisations have expanded their privacy programmes to meet the growing need of AI adoption, 93% expect to increase investment in privacy and data governance in the next two years. Yet only 12% report having mature AI governance structures in place.

This mismatch is not about risk aversion. It reflects a deeper architectural strain. Most enterprise infrastructure was built to support human-led decisions, and not autonomous systems. That limitation is now being exposed as organisations deploy agentic AI: intelligent software agents that can operate independently of human prompts.

The HCLSoftware study reports that more than 80% of enterprises are either piloting or scaling such agent-based systems. As these agents move into core workflows, they are placing pressure on every layer beneath them—data, observability, integration, and policy. Enterprises are also discovering that the speed of AI execution is meaningless without the infrastructure to govern and support it.

DATA SYSTEMS MUST ENABLE REAL-TIME CONTEXT

Even though data remains the critical input to any intelligent system, data infrastructure in most organisations struggles to meet the demands of autonomous AI. According to Cisco, 65% of enterprises report challenges in accessing high-quality, well-tagged data. Additionally, 70% are concerned about the potential risks of using proprietary or customer data for AI training. The issue is not only about scale. It is about context, control, and clarity.

HCLSoftware notes that the next generation of AI systems requires data infrastructure capable of supporting real-time orchestration, not just storage and retrieval. The focus is moving from collecting information



IN BRIEF

- AI is moving into core workflows, exposing gaps between autonomous systems and legacy infrastructure foundations.
- Most enterprises lack mature governance models despite rising AI investments and expanding privacy programmes.
- Real-time, contextual data architectures are replacing static lakes to support agent-based AI systems.
- Observability platforms now interpret signals and correlate root causes, accelerating deployment velocity.
- Governance must be embedded at the architectural level through traceable data flows and auditable decision paths.
- Sovereign intelligence demands infrastructure that adapts to regional laws without sacrificing scale or transparency.

to connecting it. This implies a transition from centralised data lakes to distributed architectures — data meshes and fabrics that can feed AI models with governed, localised, and timely data.

In this new model, infrastructure is not just a warehouse for information; rather, it is a live context engine.

Static data lakes are giving way to distributed data meshes and fabrics that deliver governed, real-time contextual intelligence for AI systems.

OBSERVABILITY IS THE NEW INFRASTRUCTURE FOR TRUST

Monitoring systems have always played a supporting role in enterprise IT. But with AI in the loop, observability is being redefined as an active, decision-supporting layer.

New Relic's AI Impact Report provides clear evidence of this shift. In 2025, accounts using its AI-powered observability features achieved a 25% reduction in mean time to close incidents. In peak periods, the performance gap widened further. These platforms did not simply monitor for alerts—they correlated signals, identified probable root causes, and surfaced actionable incidents faster than human teams could process manually.

This is no longer traditional monitoring. Observability platforms are becoming intelligent systems in their own right—interpreting signals, reducing operational noise, and enabling faster action. In doing so, they return engineering time to innovation. Teams using New Relic AI achieved deployment velocity up to five times higher than their non-AI peers. This level of signal clarity and operational feedback is no longer a luxury. It is now a prerequisite for deploying AI systems responsibly.

GOVERNANCE MUST BE EMBEDDED

Across all three reports, one message stands out clearly: governance must become an architectural function. It cannot remain a policy overlay applied after systems are in place.

While Cisco's research underscores this challenge, HCLSoftware's study argues that governance is evolving from a compliance requirement into a design principle. While most organisations acknowledge the need for AI governance, very few have embedded it meaningfully within their infrastructure. Also, responsible autonomy must be enabled by traceable data flows, auditable decision paths, and explainable system outputs.

New Relic's AI observability model reflects this principle in action. The platform logs, correlates, and explains changes and their impact, creating a runtime audit trail. In doing so, it brings governance into the feedback loop—not just at the edge but at the core of operations.

In an AI-led environment, monitoring alone is no longer enough. Enterprises must understand, trace, and defend the decisions being made—not just by humans, but by the systems themselves.

INFRASTRUCTURE MUST SUPPORT LOCAL AUTONOMY

As AI systems operate across borders, another layer of complexity emerges: jurisdiction. Hence, data localisation, compliance with regional rules, and sovereignty concerns are reshaping businesses' infrastructure strategies.

The Cisco study finds that 85% of global organisations report increased costs and complexity due to data localisation requirements. Yet trust in localisation is declining, with belief in the superiority of locally stored data falling from 90% in 2025 to 86% in 2026.

To address this, HCLSoftware introduces the concept of "sovereign intelligence," in which AI systems must operate intelligently across regions while respecting local rules. This is expected to drive a new class of infrastructure design that blends global scale with regional compliance—a 'glocal' approach in which the architecture is aware of legal, ethical, and operational boundaries.

No wonder, then, that enterprises must now build infrastructure that can act differently based on where it is operating, without compromising performance or transparency. The three reports also confirm that digital infrastructure is undergoing an irreversible shift, and the systems supporting enterprise AI can no longer be treated as neutral enablers. They must become intelligent, explainable, and responsive in their own right.

Infrastructure today must do more than host services. It must monitor behaviour, orchestrate data, enforce governance, and adapt to change. It must be able to earn trust—not just for what it processes, but for how it supports decisions made by systems that think.

In fact, it is not a trend; it is a foundational change in how enterprises build, govern, and grow. 🌱

shubhendup@cybermedia.co.in

DPDPA vs GDPR: India's consent-only rules strain operations

India's consent-centric DPDPA diverges sharply from GDPR, creating operational friction for businesses as routine data processing struggles to find a lawful basis.



BY AKSHAY S NANDA

When European regulators designed the General Data Protection Regulation (GDPR), they recognised a practical truth: consent alone cannot sustain a modern privacy framework.

People enter contracts, make purchases, open bank accounts, accept employment and engage in transactions where data processing is intrinsic to the activity itself, regardless of whether they explicitly agree to each processing activity. GDPR therefore established six lawful bases for processing personal data, recognising that while consent is appropriate for some contexts, it is wholly impractical for others.

An organisation under GDPR can process data because the individual consented, but it can equally process data because processing is necessary to perform a contract, to comply with a legal obligation, to protect vital interests, to carry out a task in the public interest, or to pursue the legitimate interests of the organisation.

This diversity of lawful bases reflects operational reality. Modern commerce and governance cannot function if every data processing activity requires explicit individual permission.

WHY GDPR MOVED BEYOND CONSENT ALONE

India's Digital Personal Data Protection Act, 2023

DPDPA's consent-heavy architecture collides with modern digital ecosystems, where multiple distributed entities process personal data without direct user interfaces.

Routine commercial functions—from order fulfilment to digital payments—risk becoming legally cumbersome under a framework lacking contract-based processing grounds.

(DPDPA) takes a narrower approach. It recognises only two pathways for lawful processing: consent or processing for “certain legitimate uses.” It does not include contract performance or legitimate interests as independent grounds. The listed legitimate uses are limited, specific, and rarely apply to ordinary commercial activity.

As a result, most organisations in India must rely on consent—even for routine processing that would fall under contract performance or legitimate interests under GDPR. This structural difference creates operational chaos. Although the framework appears simpler, compliance under the DPDPA becomes significantly more difficult than GDPR compliance in practice.

DPDPA’S NARROW LAWFUL BASIS PROBLEM

Consider a basic commercial scenario, where a customer purchases a product online. The e-commerce platform must process the customer’s name, address, payment information, and contact details to fulfil the order.

Under GDPR, since the customer has entered into a purchase agreement, this processing of data is lawful because it is necessary to perform a contract. Hence, no separate consent is required because the processing is inherent to the contractual relationship.

However, under DPDPA, contract performance is not a recognised ground. The e-commerce platform must obtain explicit consent to process data required to deliver its own service. Not to mention that seeking consent comes with its own challenges and complexities.

The operational challenge further intensifies when the organisation processing data has no direct relationship with the individual whose personal data is being processed. This situation is extraordinarily common in modern commerce. Yet the DPDPA framework assumes a bilateral relationship between Data Fiduciary and Data Principal that often does not exist.

CONSENT BREAKDOWN IN MULTI-PARTY ECOSYSTEMS

Consider an Online Travel Agent (OTA) operating in India.



IN BRIEF

- DPDPA recognises only consent and limited legitimate uses, unlike GDPR’s six lawful bases for data processing.
- Absence of contract performance and legitimate interests creates operational strain for routine commercial processing.
- Multi-party ecosystems such as travel and fintech face structural compliance gaps under consent-only processing.
- Fraud monitoring and security operations lack clear lawful footing without the provision of legitimate interests.
- Layered consent models may not satisfy independent obligations of downstream Data Fiduciaries.
- Consent fatigue risks weakening privacy protection while increasing regulatory exposure for organisations.

When a customer books a flight and hotel through the OTA, it must share personal data with the airline to issue tickets and with the hotel to confirm the reservation. However, each entity—the OTA, airline, and hotel—is a separate Data Fiduciary under the DPDPA because each independently determines the purpose and means of processing the personal data it receives.

Layered consent in platform economies may shift regulatory exposure downstream, leaving airlines, banks and vendors accountable for consent they did not design.

Under GDPR, this ecosystem operates on contract performance. The OTA shares data because it is necessary to fulfil the customer's booking. Airlines and hotels process the data for the same reason. No separate consent is required at each stage.

Under DPDPA, this logic collapses. The airline and hotel do not have any direct contract with the customer since the reservations have been made through the OTA. However, the DPDPA requires that every request for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal.

In practical terms, this means the airline and the hotel must give notice and obtain consent directly from the passenger before processing their data. The big question here is how should they proceed with this? Since the airline and hotel have no direct interface with the customer during booking, should they send a separate email requesting consent before the OTA can complete the booking? Should the hotel interrupt the booking flow with its own consent request?

Such friction would destroy customer experience and make integrated travel bookings practically impossible.

Alternatively, the OTA may seek layered consent covering downstream entities. But the Act suggests each Data Fiduciary must independently comply. But a fundamental question remains: does consent given to one Data Fiduciary satisfy the notice and consent requirements for a different Data Fiduciary? Also, if the OTA's consent is later deemed invalid—if it did not fulfil all requirements of consent under the DPDPA, downstream entities inherit risk without control over the original consent design.

SECURITY, CONSENT FATIGUE, AND REGULATORY RISK

The absence of a legitimate interest basis also creates additional chaos where organisations need to process data for security and fraud prevention. Consider a bank monitoring customer transaction to detect fraud. The bank processes transaction data, analyses patterns, flags suspicious activity, and may freeze accounts or block fraudulent transactions.

Under GDPR, this processing is justified under legitimate interests. The bank has a legitimate interest in preventing fraud and safeguarding customer funds, balanced against customer privacy—a balance that typically favours processing because fraud prevention benefits both parties. Hence, no consent is required.

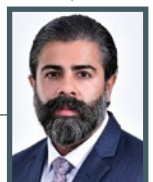
Under DPDPA, no such ground exists. The bank cannot process transaction data for fraud detection unless customers consent or some legitimate use applies. Seeking explicit consent for fraud monitoring is impractical; customers may ignore or refuse it, weakening protection. This also creates a structural dilemma: obtain granular consent that undermines security, or process without a clearly articulated lawful basis and face regulatory risk.

The cumulative effect is that DPDPA compliance is significantly more difficult than GDPR compliance. This two-pathway structure forces nearly everything into consent, creating systemic problems. Similarly, consent fatigue undermines the framework; when nearly all processing must be consent-based, individuals face frequent notices and prompts. Over time, consent becomes mechanical—users click “agree” without reading, or disengage entirely. At the same time, the lack of consent for certain processing activities will create operational barriers that can impede legitimate and necessary business functions.

The solution would be for India to amend the DPDPA to include contract performance and legitimate interests as lawful bases for processing personal data. Such additions would align India with global practices and provide organisations with the flexibility to operate lawfully.

Until such amendments occur, organisations in the country will continue to face a compliance landscape that is more restrictive than the GDPR in theory and far more chaotic in practice. 🧩

*The author is a Partner at Saraf and Partners.
feedbackvnd@cybermedia.co.in*



Securing the digital stack at the silicon core

As AI and hyperscale infrastructure expand, trust must be engineered into semiconductors—the foundational layer powering networks and cloud.



BY NAVIN BISHNOI

Semiconductors are the foundational technology of modern life. They are embedded in virtually everything we interact with today—from smart phones and appliances in our homes to outdoor digital signage and more. Semiconductors are also used to move, store, process and secure the world's data, powering the infrastructure of massive computing systems running within hyperscaler, cloud and enterprise data centres.

These advanced systems utilise high-performance semiconductors across all elements of the architecture—for compute, connectivity, switching, data security, data storage and more—and are the driving force of innovation in the artificial intelligence (AI) field.

As semiconductor devices grow more intelligent and interconnected, and as the new demands of AI technology require a continual evolution of more powerful and efficient silicon solutions, the expectations placed on

the hardware have also transformed to include trust and ethics in chip design.

This is emerging as the next frontier in responsible innovation, alongside stronger cybersecurity practices, where the choices made by engineers at the silicon level will determine the reliability and integrity of the digital ecosystems of tomorrow.

INTEGRATING ZERO-TRUST AT THE SILICON LAYER

The need for security at the hardware layer is essential if one wants to design and implement a trustable, ethical framework at the chip level, as hardware-focused security attacks continue to increase and are getting more sophisticated.

A recent CISO study reported an 88% increase in hardware security vulnerabilities, largely due to the increase in IoT devices and the release of new enterprise

hardware. This makes it imperative for data security to start at the very beginning of the semiconductor design process.

Embedding protection at the hardware level—with techniques like secure boot, hardware-backed encryption and robust isolation—creates a resilient foundation before any software is loaded. Integrating zero-trust principles at the silicon layer can further strengthen this approach by reducing the points of vulnerability. It assumes that no component, user or workload is inherently trustworthy, ensuring semiconductors enforce continuous verification across AI, IoT and cloud deployments.

These mechanisms ensure that systems cannot be tampered with and that sensitive data remains protected at all times.

ENGINEERING ETHICS INTO SEMICONDUCTOR DESIGN

Ethics is often discussed in the context of algorithms or policies; however, it must begin much earlier—within the hardware that powers all AI workloads. Semiconductor engineers should embed capabilities that support traceability, fairness and accountability to ensure that AI systems behave responsibly.

For example, semiconductors can be designed to provide audit trails, enabling stakeholders to investigate and verify how models were trained, what data was used and how outputs were generated. For this, engineers also need to collaborate with other stakeholders like ethicists and policymakers.

Rigorous design reviews will help identify risks such as potential bias, misuse scenarios or unintentional opacity. Ensuring transparency at the hardware level will provide the 'explainability' that critical sectors like healthcare, finance and public services urgently require. Addressing these concerns early will ensure that modern systems do not cause harm as they scale.

POWERING EFFICIENCY AND THERMAL RESILIENCE

AI brings with it significant energy and thermal challenges. Training and deploying advanced AI models not only demands substantially more computational power than traditional data centre systems, but also more advanced connectivity and storage solutions, leading to significant energy and thermal challenges. As a result, maximising power efficiency becomes both an environmental and economic responsibility.

The semiconductor industry can play a major role in global sustainability efforts by prioritising power-efficient architectures at the design stage. Advances in chip packaging, thermal management and power regulation can also significantly lower energy requirements and improve operational efficiency. Better thermal design extends hardware life, reduces cooling costs and lowers the total cost of ownership for hyperscalers, cloud service providers, enterprises and research institutions.

ALIGNING DESIGN WITH GOVERNANCE FRAMEWORK

Technical safeguards need to be supported by strong governance frameworks that emphasise privacy, accountability and transparency. As technologies evolve, the semiconductor ecosystem—semiconductor designers, policymakers, independent industry bodies and academia—must collaborate to address emerging threats, policies, potential biases and ethical issues so that they can be addressed within the product lifecycle.

This will ensure that responsible practices are embedded at every stage, starting at architecture design through deployment.

Opening up access to advanced semiconductor technologies will also allow a more diverse set of innovators to participate in building secure and ethical solutions. Open hardware platforms, modular design tools and shared research resources can level the playing field for startups, academic institutions and public-sector innovators.

When more voices contribute to shaping technology, the outcomes become more inclusive and context-aware. Semiconductors power systems that connect all of us and help us make critical decisions in our daily and professional lives. They are also fundamental technologies driving new waves of innovation in AI, cloud and enterprise computing, scientific research and myriad other fields.

The future of 'responsible technology' will be shaped by what we choose to build into our silicon today—namely, ethics, security and sustainability. And when 'integrity' is part of a chip's core architecture, every layer built upon it becomes more resilient, transparent and trustworthy. 🌱

The author is the AVP Data Centre Engineering and India Country Manager of Marvell.

feedbackvnd@cybermedia.co.in



China builds Meteor 1 parallel optical AI chip

A new photonic processor signals a shift in high-performance computing for AI and data centres amid rising power demands.

Researchers at the Shanghai Institute of Optics and Fine Mechanics and Nanyang Technological University have developed Meteor-1, a first-of-its-kind integrated chip for parallel optical computing, achieving a theoretical peak of 2,560 tera-operations per second at 50 GHz, according to a report by DeepTech.

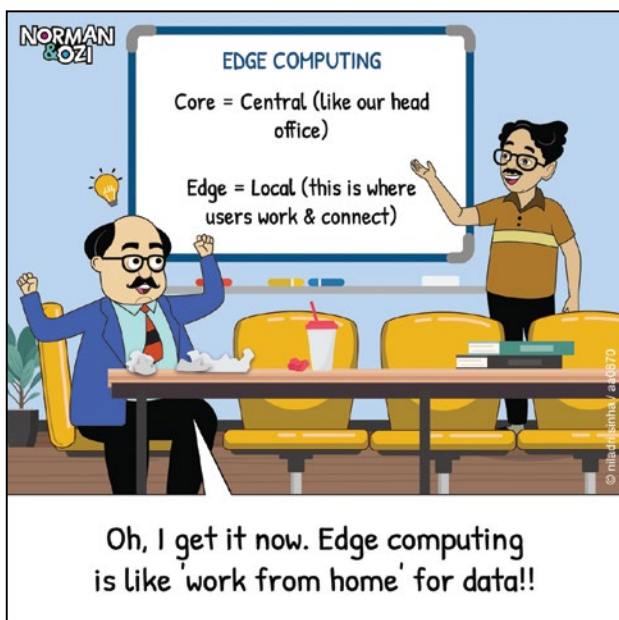
The team, led by Xie Peng and Han Xilin of SIOM and Hu Guangwei of NTU, said the chip enables more than 100 concurrent computing tasks on a single photonic platform. The reported peak performance approaches that of advanced graphics processors such as Nvidia's GeForce RTX 5090 at 3,352 TOPS and RTX 4090 at 1,321 TOPS.

Meteor-1 integrates a self-developed architecture comprising a light-source chip, an optical-interaction chip, an optical-computing chip, and a modulation-matrix driver board. The light source chip uses a micro-cavity optical frequency comb with an output spectrum exceeding 80nm, supporting more than 200 wavelengths. According to the researchers, this multi-wavelength source replaces hundreds of discrete lasers, reducing system size and power consumption while improving integration density.

The optical computing core provides transmission bandwidth above 40nm to support low-latency parallel processing. A custom driver board with more than 256 channels enables precise optical signal modulation and task allocation across frequency channels.

The researchers said their approach focuses on expanding computational parallelism rather than scaling matrix size or frequency, which have constrained earlier optical prototypes. "This achievement enables a 100-fold increase in optical computility through ultra-high parallelism without scaling up the chip size," the authors wrote.

According to Xie, the architecture could position optical computing as a cost-performance alternative to electronic chips for AI workloads and data centres facing rising power and thermal constraints.



YOUR CUSTOMERS ARE EVOLVING. LET YOUR BRAND LEAD WHERE IT MATTERS MOST. CYBERMEDIA'S INTEGRATED GO-TO-MARKET ENGINE PROVIDES INFLUENCE, VISIBILITY, AND HIGH-INTENT LEADS ACROSS INDIA'S MOST TRUSTED TECH MEDIA PLATFORMS.

LEAD THE CONVERSATION USING CYBERMEDIA'S 360° GTM STRATEGY. UNMATCHED REACH ACROSS OUR FLAGSHIP BRANDS



DATAQUEST
Enterprise &
Tech Leadership



PCQUEST
CIOs, Tech
Influencers & SMBs



VOICE&DATA
Telco & Digital
Infra Leaders



DQCHANNELS
ICT Partners &
Channel Decision Makers

OUR BESPOKE B2B MARKETING PROGRAMMES BUILD, ENGAGE AND SCALE COMMUNITIES

Account-Based CXO Connects & C-Level Roundtables | Content-Led Thought Leadership Campaigns | Audience Segmentation Across IT & Business Decision Makers | Print, Digital, Event, Podcast & Research Integration | Measurable ROI & Lead-Nurturing Programmes

High-Impact Verticals We Specialise In: Cloud & Multi-Cloud Solutions | Cybersecurity & Risk Management | Data, AI & Advanced Analytics | Enterprise IT Infrastructure & SaaS | Telecom, 5G & Network | SMBs & Mid-Market Technology Buyers | Transformation | Sustainability & Green IT | Channel Ecosystem: VARs, MSPs, Distributors, SIs | SMBs & Mid-Market Technology Buyers

DELIVER INFLUENCE AND OUTCOMES WITH CYBERMEDIA

42+ Years of Tech Publishing Legacy | Deep CXO Access & Vertical Intelligence | Custom Campaigns with Content + Conversion Focus | Trusted by Top Global & Indian IT Brands

LET'S BUILD SMART, VERTICAL-LED CAMPAIGNS THAT TURN YOUR BRAND MESSAGE INTO MEASURABLE BUSINESS IMPACT.

www.dqindia.com | www.pcquest.com | www.voice&data.com | www.dqchannels.com



APEEJAY SCHOOL OF MANAGEMENT

Dwarka, New Delhi | Estd. in 1993



ADMISSIONS OPEN 2026-28

Transform Your Career with World-Class PGDM Program at Apeejay

Ranked among the top business schools
in India by **Times B-School Ranking 2025**

Post Graduate Diploma In Management

(MBA equivalent by AIU)

Specialisations Offered:

Business Analytics | Accounting & Finance |
Human Resource | Marketing |
Operations & Decision Science

WHY CHOOSE APEEJAY SCHOOL OF MANAGEMENT?



Industry-Driven
Curriculum



State-of-the-Art
Campus



Distinguished
Alumni Network



International collaborations and
opportunities for global exposure



Guest lectures, internships, and placement
drives by leading companies

ACCREDITATIONS



Times B School

2025 RANKINGS



GET CHOSEN BY TOP RECRUITERS

amazon

HDFC BANK

Deloitte

ICICI Bank

ACUITY
KNOWLEDGE PARTNERS

MARUTI

tcs TATA
CONSULTANCY
SERVICES

Gartner

HCL

ION

accenture

cvent

Ameriprise
Financial

& many more...

We offer only placement assistance. Placements may vary with industry requirements, market sentiment and student merit.

Scan for website



Inviting applications for PGDM Batch 2026-28

Institutional Area, Sector - 8, Dwarka, New Delhi – 110077

E-mail: admissions.asm@apeejay.edu | Website: apeejay.edu/asm

FOR ADMISSION QUERIES DIAL:
+91 9560 222 999