ITPV

Connecting with Solution Provider in
EMERGING MARKET

Vol XIV | Issue 10 | February 2026 | Pages 32

▪ Northern ▪ Eastern ▪ Maharashtra ▪ Gujarat ▪ MP & Chwattisgarh ▪ North East ▪ Southern ▪ UP & Uttarakhand ▪ Bihar & Jharkhand

Union Budget 2026–27
What It Means for India's IT and Digital Economy

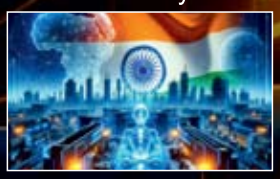
In Conversation

Ransomware-Ready in 2026: Neeyamo & Cyber Vigilens on Closing the Last Mile

Sachin Kawalkar
Neeyamo

Saurabh Barjatiya
Cyber Vigilens

India in 2026: Should Technology Nationalism Shape the Future of Cloud, AI and Security?



Digital Transformation Isn't the Problem—Slow CXO Decision-Making Is Killing ROI

TECHPLUS MEDIA

BenQ

As Native as Your Mac.
As Brilliant as Your Vision.

MA320U Monitor offers flawless MAC integration, perfect color matching & minimalist design- crafted to complement your Apple ecosystem seamlessly

GOOD DESIGN AWARD 2024

Match your Mac Colors

Integrated MacBook Control

Desktop Partition Feature

4K
3840x2160

Mac Color Tuning

97% DISPLAY P3

Nano Matte Panel

Dual
Type C
Upto 90W PD

MA series is also available in 27 inches

3 Onsite Warranty Years

Contact Person – Rahul Das | West Bengal | Rahul.Das@BenQ.com | 9560886360

"Available across all leading retail stores, BenQ Brand Online store & Amazon India"

www.BenQ.in | Sales.enquiryin@BenQ.com | 1800 419 9979 | Like BenQ India on

Scan to Know more

SEAGATE | mozaic 3+ | EXOS™

Maximize scale. Optimize TCO. Sustain the future.

Powered by Seagate's Mozaic 3+ technology, the Exos M 32TB hard drive breaks through data center limitations with an exceptional 3TB per platter density.

Best-fit applications

- Scalable hyperscale applications/cloud data centers.
- Massive scale-out data centers.
- Big-data applications.
- High-capacity, high-density RAID storage.
- Mainstream enterprise external storage arrays.
- Distributed file systems, including Hadoop and Ceph.
- Enterprise backup and restore–D2D, virtual tape.

www.seagate.com

For sales enquiries, contact: **Sanjay Khushlani (Supertron)** - 98110 59025. Email: sanjay.khushlani@supertronindia.com
For marketing support, contact: **Talwinder Singh** - 96438 99527. Email: talwinder.singh@seagate.com

Seagate Authorised Distributor SUPERTRON®

CONTENT

COVER STORY 6

Union Budget 2026–27 What It Means for India's IT and Digital Economy

IN CONVERSATION

Observability, Security Intelligence & AI: Inside Datadog's APAC Partner Motion

10

SACHIN KAWALKAR,
Chief Information Security Officer, Neeyamo

SAURABH BARJATIYA,
CTO, GBB and Co-Founder, Cyber Vigilens

CHANNEL NEWS 15,18-26

INSIGHT 27-29

INK TANK
PRINTERS

brother
at your side

Newly Launched

PRINTS BEYOND IMAGINATION

Wireless Direct

DCP-T230
Print • Scan • Copy
MRP ₹ 13,990/-*
(Incl. of all taxes)

Duplex Wireless Direct ADF

DCP-T730DW
Print • Scan • Copy
MRP ₹ 22,990/-*
(Incl. of all taxes)

Works with
Apple AirPrint

#Not applicable for DCP-T230

Wireless Direct

DCP-T430W
Print • Scan • Copy
MRP ₹ 15,590/-*
(Incl. of all taxes)

Duplex Wireless Direct Network ADF

DCP-T830DW
Print • Scan • Copy
MRP ₹ 25,590/-*
(Incl. of all taxes)

Duplex Wireless Direct

DCP-T530DW
Print • Scan • Copy
MRP ₹ 17,990/-*
(Incl. of all taxes)

Duplex Wireless Direct Network ADF

MFC-T930DW
Print • Scan • Copy • Fax
MRP ₹ 35,590/-*
(Incl. of all taxes)

Print up to
7,500# Black | 5,000# Colour
Spill-Free & Precise Refilling Technology

Print up to
15,000# Black | 5,000# Colour
Spill-Free & Precise Refilling Technology

***Conditions Apply | *T&C Apply

***Free Installation**
on Wi-Fi and Network Models
with standard warranty of 1 year***

FOR SALES ENQUIRIES : Mumbai : Rajesh Phatangare - 9619655576 **I Pune, Chattisgarh, Goa, Rest of Maharashtra :** Shishir Singh - 9860728548 **I Gujrat, MP :** Pulin Shah - 9924253604 **I Bihar, Jharkhand, Orissa :** Deepak Singh - 9771403031 **I Telangana, Andhra Pradesh, Karnataka :** Saggive Kumar - 9962000969 **I Chennai & Kerala :** Govindrajan S - 9176681639 **I Delhi, Rajasthan, Haryana :** Ashish Kalra - 9899306959 **I Uttar Pradesh, Punjab, Jammu & Kashmir, Uttrakhand :** Ajay Saxena - 9919666636 **I Kolkata & Northeast :** Preetam Panday - 9830472986

MRP mentioned above is for 1 unit and subject to change without prior notice | Yield in accordance with ISO/IEC 24712 (Ink Tank) | IPM speed is in accordance with ISO/IEC 24734

India EPR Compliance I Entity Name: Brother International (India) Private Limited Plastic Waste EPR No.: BO-13-000-08-AADCB0263E-22 I Battery Waste EPR No.: 6821475 I Thickness for PE bag: 50 microns or above

Now get 24x7 support on **WhatsApp** **7045 450 450**

www.brother.in

UNION BUDGET 2026–27
What It Means for India's IT and Digital Economy

India's Union Budget 2026–27 has laid out a decisive roadmap for long-term economic expansion, with technology, infrastructure, and digital capability emerging as central pillars. For the Indian IT industry, the Budget signals policy continuity, regulatory clarity, and a strong push toward positioning India as a global digital and AI-led economy. A key highlight for the technology sector is the government's intent to strengthen India's role as a data centre and digital services hub, supported by long-term tax exemptions on data centre services catering to foreign customers, higher safe-harbour thresholds, and consolidation of IT and R&D services under a unified tax framework. These moves are expected to reduce compliance friction and improve investment predictability for IT services companies across the value chain.

Infrastructure, manufacturing, and tech-led growth

Industry leaders see the Budget's emphasis on infrastructure and advanced manufacturing as foundational to India's tech ambitions. Amit Sharma, MD & CEO, Tata Consulting Engineers, said the Budget reinforces India's execution-focused growth strategy: "The Union Budget 2026–27 sets a clear direction for India's long-term growth, with a strong focus on capital investment, manufacturing competitiveness and technology-led development. Continued high spending on infrastructure strengthens confidence in execution and supports progress across transportation, urban development and logistics. The emphasis on high-speed rail, alongside roads, metros, ports and urban infrastructure, signals a move towards next-generation connectivity.

AMIT SHARMA,
MD & CEO, Tata Consulting Engineers

Policy continuity on clean energy and grid strengthening supports energy security and transition, while the focus on advanced facilities such as semiconductors, electronics, data centres and pharmaceuticals builds domestic capability. Measures supporting hydrocarbons and chemicals, and metals and mining including rare-earth corridors, strengthen critical supply chains. Overall, the Budget underlines the importance of delivery quality alongside investment scale." He added that Tata Consulting Engineers remains committed to converting policy intent into future-ready national assets.

Data centres: opportunity today, sovereignty tomorrow

While the Budget's tax incentives for data centres are expected to unlock immediate investment and job creation, some industry voices have flagged long-term strategic concerns around digital sovereignty.

Manoj Dhanda, Founder, Utho Platform, cautioned against over-dependence on foreign hyperscalers:

MANOJ DHANDA,
Founder, Utho Platform

"This policy will definitely create jobs and bring short-term benefits through data centre investments. But in the long run, India risks becoming only a reseller market—from email to AI, everything sold by foreign hyperscalers with limited control. Sovereignty, innovation, and future pricing power are real concerns. Indian cloud players are already investing without such incentives; with the right policy support, India can build sovereign cloud capital, export technology globally, and give businesses lock-in-free, risk-free platforms."

IT services and AI take centre stage

Large IT services players have welcomed the Budget's explicit recognition of technology—and AI in particular—as a core economic growth engine. Aparna Iyer, CFO, Wipro Limited, highlighted the

fiscal discipline and sector-specific reforms: "It is commendable to see the government meeting the fiscal deficit targets for FY'26 despite a very volatile external environment. The budget clearly articulates the Government's vision to promote the Indian IT services sector as a primary driver of India's economic growth, leveraging Artificial Intelligence as the force multiplier. By identifying AI as central to accelerating and sustaining economic growth, the government underscores its strategy to establish India as an AI-powered economic superpower. The proposal to provide long-term tax exemption for data centre services provided from India to foreign customers will help in establishing India as a data centre hub."

She further noted that structural tax reforms will materially ease operations for IT firms: "Combining IT services and R&D services into a single bucket, increasing the threshold limit for safe harbour, and providing a two-year timeline for conclusion of unilateral APAs will provide tax certainty and reduce the cost of compliance for companies operating in the sector. We also welcome the government's initiatives to further improve ease of doing business, which will support enterprises across sectors."

The Union Budget 2026–27 reinforces India's ambition to move beyond being a cost-efficient IT services destination toward becoming a digitally sovereign, AI-driven economy. While incentives for global players may accelerate near-term capital inflows, the next policy frontier will be balancing foreign investment with the nurturing of Indian cloud, AI, and platform ecosystems. For CIOs, CTOs, and digital leaders, the message is clear: India's tech runway is expanding—but strategic choices made today will define control, competitiveness, and resilience over the next decade.

APARNA IYER,
CFO, Wipro Limited

SACHIN KAWALKAR,
Chief Information Security Officer, Neeyamo

SAURABH BARJATIYA,
CTO, GBB and Co-Founder, Cyber Vigilens

Ransomware-Ready in 2026: Neeyamo & Cyber Vigilens on Closing the Last Mile

Cyber gap assessments are no longer the problem—execution is. In this New Year special edition of ITPV Channel Magazine Candid Chat, based on the Talks with Kalpna – CXO Spotlight series on CXO TV, Sachin Kawalkar, Chief Information Security Officer at Neeyamo, and Saurabh Barjatiya, CTO at GBB and Co-Founder of Cyber Vigilens, sit down with Kalpna Singhal to decode how enterprises can move from visibility to action, from tool sprawl to integrated defense, and what true ransomware readiness should look like in 2026.

When you look at today's enterprise landscape, if you had to describe cybersecurity operations in one word, what would it be – and why?

Sachin Kawalkar (SK):

Limiting it to one word is tough, but I'd say: "layered."

Technology is evolving at high velocity – cloud, AI, GenAI, hyper-digital operations. To stay in control, enterprises need layered use of advanced tools, strong processes, and skilled people. Tools alone don't save you. Awareness, skill, and the right use of technology—stacked in layers—get you closer to the security objectives you've defined.

KS: Saurabh, same question to you. One word that captures cybersecurity for you today?

Saurabh Barjatiya (SB):

For me, the word is "backups."

In the case of a highly sophisticated attack, even if multiple layers fail, good, tested backups are the last line of defense. They're what help you get back on your feet and restore business to a known-good state. Without that, all the maturity models look great on slides but fall flat in reality.

"Why enterprises identify gaps but don't close them"

KS: Enterprise teams often do a decent job of identifying gaps but struggle to close them quickly. From your global security lens at Neeyamo, what really slows execution?

SK: Almost every organisation tries to be compliant and secure. Some reach 90–95%, very few get close to 100%. In my experience, a core reason for the gap is lack of a true 360-degree view of the environment.

There are a few recurring themes:

- **Unclear scope and boundaries:** Thousands of APIs, integrations, and connectors hit enterprise environments every day. Many organisations don't have a complete inventory—which APIs exist, which apps are talking to what, where the data actually flows.
- **Third-party exposure:** The network and data path often extend into vendors, partners, and service providers. If their controls are weak, your environment becomes vulnerable by default. Third-party adherence to security and compliance is frequently under-assessed.
- **Superficial compliance:** Many claim to follow ISO 27001 or other standards, but the depth of enforcement is missing. If you follow a standard religiously and systematically, it forces you to look at HR, awareness, network security, legal, physical, cloud, application security – in a structured way.
- **No continuous PDCA cycle:** ISO 27001's Plan–Do–Check–Act (PDCA) is powerful. But it only works if it's ongoing. Doing a "security health check" once in five years is like doing a medical check-up once in ten. Continuous assessment, remediation, and re-assessment is what takes you from 70% to 95–98% readiness.

> "Organisations still running legacy signature-based antivirus are significantly more exposed to ransomware than those using next-gen endpoint security (EDR/XDR) based on behaviour, indicators of compromise, and process monitoring."

In short, asset visibility, third-party risk, and continuous compliance are the three big levers. If those are weak, execution will always lag.

"Turning visibility into execution"

KS: From the solution and architecture side, how do you see companies operationalising fixes faster?

SB: I fully agree with Sachin – visibility comes first. You must know:

- What infrastructure you have
- How it's really configured on the ground
- How your vendors and partners are following best practices

Once you have that, the next step is prioritisation. Don't just "buy tools" at random because the market is noisy.

You want to focus on controls that:

1. Cost less in terms of time and money,
2. Are simpler to implement with your current team and toolset, and
3. Deliver the maximum uplift in security.

A few things I see repeatedly on the ground:

- **Modern vs legacy endpoint security:** Organisations still running legacy signature-based antivirus are

significantly more exposed to ransomware than those using next-gen endpoint security (EDR/XDR) based on behaviour, indicators of compromise, and process monitoring.

- **"Next–next–finish" deployments:** A tool is purchased, installed quickly with default settings, and never tuned. The dashboards and reports exist, but nobody seriously reviews them or refines the policies. That's wasted budget.
- **Lack of second opinion:** No single team or vendor knows everything. Periodic external audits and independent reviews—from different specialists—consistently surface new gaps that internal teams may have missed.

So, the execution equation is: **Visibility →Prioritised actions → Deep deployment + regular review → External second opinions**. That's the fastest way to move from theory to real risk reduction.

"The skills and people side that often gets ignored"

KS: Sachin, you spoke about tools needing the right skills behind them. Where do you see the biggest gaps there?

SK: One of my favourite questions to ask at conferences is: "You bought the tool—but do you have the right people to drive it?"

You can deploy the "world's best" cloud security posture management solution or next-gen firewall, but:

- Are your internal teams deeply trained on it?
- Do they understand each module, each policy, each alert?
- Have they tuned it to your environment, not just run the default?

Otherwise, it's like buying a Rolls-Royce and not knowing how to drive.

> "As a CISO, you must know what information really matters—customer data, payroll, financials, IP, even paper-based KYC records in some sectors. Identify the crown jewels and chart where they sit and how they flow."

The tool's potential remains unrealised, and you still have pockets of vulnerability.

So for every big-ticket solution, you need to budget for:

- Skills (training, certifications, hands-on practice)
- Time for fine-tuning rules, thresholds, and workflows
- Clear ownership of who is accountable for outcomes from that tool

Tools without skills are just expensive checkboxes.

"The CISO's top three priorities in 2026"

KS: If CISOs could fix only three things first, what should be at the top of the list?

SK: My top three would be:

- Visibility of crown jewels: As a CISO, you must know what information really matters—customer data, payroll, financials, IP, even paper-based KYC records in some sectors. Identify the crown jewels and chart where they sit and how they flow.
- Internal and external assets: Map both internal assets (endpoints, servers, apps, networks) and external dependencies (cloud providers, SaaS, third-party processors, partners). Your real attack surface is the sum of both.
- Right technologies + integration: Ensure you have the right mix of endpoint, cloud, perimeter, DLP, identity and monitoring tools, and that they are well integrated. A single consolidated view – a dashboard that actually makes sense – is important. Small signals missed in a siloed tool can become large incidents.

On top of that, there's a hygiene layer: staying updated with real-time advisories and vulnerabilities, and doing in-depth assessments with more than one vendor for critical assets. It's similar to getting a second medical opinion – sometimes a different "doctor" finds what the first one missed.

"Where's the maximum ROI with minimum effort?"

KS: Saurabh, based on what you see on the ground, where do CISOs get the highest security ROI with relatively less effort?

SB: If we look purely at bang-for-buck, three areas stand out:

- Endpoint security: Move away from legacy signature-based AV to next-generation endpoint security that analyses behaviour and indicators of compromise. Most compromises we see start with a non-technical user – someone in accounts, legal, HR clicking on a malicious link or attachment. Modern endpoint security dramatically changes that equation.
- Security awareness at the endpoint: Consistent security awareness and phishing simulations are not optional. Teach people

not to share passwords, not to click suspicious links, to double-check with IT, and to recognise social engineering. It's boring but extremely effective.

- Firewalls done right: Almost every organisation owns a firewall, but many don't leverage SSL inspection, proper segmentation, or directional rules. For example: my machine should be able to talk to a printer, but the printer doesn't need to initiate a connection to my machine. These basics, when implemented properly, give huge uplift without needing a fresh capex cycle.

So if an organisation starts with modern endpoints, realistic user awareness, and well-configured firewalls, the security posture jumps significantly with manageable effort.

"Securing endpoints at scale in a global, remote world"

KS: Neeyamo runs a global payroll business with distributed teams, remote work, and multiple regulatory jurisdictions. How do you secure endpoints at that scale?

SK: At Neeyamo, we see ourselves as a process-driven organisation across security, quality and privacy. We hold 10+ certifications, so our security has to be structurally robust.

For endpoints specifically, we focus on:

- **Strong policy & documentation:** Clear definitions of what's allowed, what's not, and how requests are handled.
- **No bypass of process:** Every exception or access—VPN, remote access, privileged access—must go through the service desk and ticketing system, with approvals and risk checks embedded.
- **Hardened endpoint builds:** We maintain standardised thin-client builds with:
  - Latest AV / EDR / ransomware protection
  - DLP controls
  - OS and configuration hardening as per best-practice benchmarks
- Multiple layers of defense: We don't rely on a single solution. We use three layers of defense at the endpoint and then additional layers at the perimeter. If something bypasses one layer, it is designed to be picked up in the next.
- Real-time monitoring: A very common gap in enterprises is: tools generate alerts but no one is watching. We ensure DLP, EDR and other tools are monitored in a way that is human-readable and actionable. Someone must be accountable to respond.

Deployment, enforcement and monitoring – all three have to be equally strong.

> "If we can bring in agentic AI or automation to correlate signals from multiple tools into one view of risk, even better. That's how you get real 360-degree visibility, not just a collection of licences.
>
> Reducing noise and getting one view of security."

"Too many tools, too little integration?"

KS: Does today's environment suffer more from "too many tools and too little integration"?

SK: The issue is less "too many tools" and more "too many tools without clarity of purpose and integration."

Each tool has a very specific core objective—AV, EDR, XDR, DLP, CSPM, ZTNA, SIEM, etc. Problems start when:

We expect one tool to magically do three or four jobs, or

We buy multiple tools but never integrate their outputs.

The right approach is:

Choose dedicated tools for critical functions

Ensure they talk to each other, directly or via a SIEM/ central platform

Aim for a single, meaningful console where security teams can see the story end-to-end instead of reading five dashboards in isolation

If we can bring in agentic AI or automation to correlate signals from multiple tools into one view of risk, even better. That's how you get real 360-degree visibility, not just a collection of licences.

"Reducing noise and getting one view of security"

KS: How can enterprises reduce alert noise and build that one consolidated view?

SK: It starts at the POC and vendor selection stage. Often we check features, pricing and basic fit, but ignore crucial questions:

Can this tool integrate with my existing stack?

Can it share and consume data from other tools?

How readable and actionable are its dashboards?

Your environment is already complex. You cannot rip and replace everything for one new tool, so interoperability is non-negotiable.

If, during POC, you

validate:

Integration with your current tools

Real-time data flow between them

Quality of the consolidated dashboards

then you can reduce alert fatigue and get a security view where your teams don't waste time jumping between consoles. With AI-driven correlation layered on top, you get clearer insight into where you're genuinely exposed and what to fix first.

"What does ransomware readiness look like in 2026?"

KS: One ransomware breach can nullify years of security work. What does "readiness" really look like in 2026?

SK: Readiness in 2026 is not one magic product. It's a combination of:

- Right selection of tools and vendors suited to your environment, with a long-term view
- Multiple standards and certifications (e.g., ISO 27001, privacy and sectoral standards) that force you to touch every control surface
- Continuous measurement – threat modelling, cyber risk assessments, regular scans, and multiple rounds of testing across layers
- Multiple lines of detection and validation – if one scan or tool misses a small vulnerability, another should catch it
- Backup strategy and recovery playbooks that are actually tested, not just documented

On the regulatory side, we're seeing stronger governance around data privacy, cybercrime, AI, and telecom. With EU GDPR, emerging AI regulations and India's own data and cyber frameworks, the message is clear: there will be fewer excuses and more accountability.

My bottom line for 2026: keep learning, keep deploying, keep optimising, and make sure you're actually using what you've invested in. Readiness is a moving target, but continuous motion keeps you close to it.

Rapid-fire: one-liners for the CISO playbook

KS: Time for a quick rapid-fire. One security habit every employee should adopt?

SK: Never share passwords. Not over email, not over chat, not verbally.

SB: I'd add: enable two-factor or multi-factor authentication wherever possible. It's one of the simplest, highest-impact controls.

KS: One tech investment you believe CISOs will never regret?

SK: Strong, well-implemented perimeter security – next-gen firewalls, web gateways, and segmentation aligned to your risk model.

> "AI is powerful and can be a massive accelerator—if adopted with the right guardrails, governance, and standards. Without that, it can introduce new risks faster than we can manage them. So it's a friend, but one that needs strict rules at home."

KS: One headline you'd like to see in the industry by 2026?

SK: Something as simple as: "Awareness. Awareness. Awareness."

If that mindset becomes mainstream, we've already won half the battle.

KS: One myth you want to kill forever?

SK: That cybersecurity is too complex and impossible to crack. With structured standards, the right mindset and continuous effort, you can build a very strong posture.

SB: For me: the myth that "security is the CISO's job."

Security is everyone's responsibility—from the frontline employee to the board. A few people carry the title, but unless the entire organisation participates, security will fail.

KS: AI in cyber – friend or risky friend?

SK: I'd call AI a "risky friend."

AI is powerful and can be a massive accelerator—if adopted with the right guardrails, governance, and standards. Without that, it can introduce new risks faster than we can manage them. So it's a friend, but one that needs strict rules at home.

"One actionable takeaway for CISOs"

KS: Before we close, one actionable takeaway for CISOs reading this in January 2026?

SK: Most CISOs already understand technology. My advice is:

Learn to get what you need from the board—budget, sponsorship, and patience.

Make sure you are leveraging every possible resource—standards, certifications, tools, vendors, assessments.

Use these not as checkboxes but as multipliers, and align them clearly to business risk.

If you can connect board-level understanding, the right tools, and continuous execution, you'll be in a much safer zone.

Union Budget 2026 Triggers Debate as Adani and Ambani Benefit from Cloud Incentives

India's Union Budget 2026–27 has triggered an industry-wide debate on cloud sovereignty and long-term value creation, as incentives for global cloud hyperscalers are expected to significantly benefit large domestic data centre operators. Under the Budget framework, foreign hyperscalers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud will be eligible for long-term tax incentives extending up to 21 years provided their cloud workloads are hosted within Indian data centres. The policy is aimed at accelerating data localisation, digital infrastructure creation, and employment generation.

Big-Ticket Infra Moves Set the Context

The debate comes against the backdrop of major infrastructure announcements made ahead of the Budget. In October 2025, the Adani Group announced a $15 billion partnership with Google to build large-scale, AI-focused data centre infrastructure in India. This was followed in January 2026, when Reliance Jio announced a 3-gigawatt data centre project in Jamnagar, one of the largest planned facilities globally. Both groups are building massive capacity positioned to host global cloud giants such as AWS, Google Cloud, and Microsoft Azure, effectively becoming long-term infrastructure partners for hyperscalers seeking local hosting to comply with India's policy and regulatory environment.

Concerns from Domestic Cloud Leaders

Industry veterans have cautioned that while the policy may deliver short-term infrastructure and employment benefits, it could have long-term structural implications. Manoj Dhanda, Founder of Utho Platforms, said the approach risks limiting India's control over its digital future. "This policy will definitely create jobs and bring short-term benefits through data centre investments. But in the long run, India risks becoming only a reseller market — from email to AI, everything sold by foreign hyperscalers with limited control. Sovereignty, innovation, and future pricing power are real concerns."

Hyperscaler-Aligned Viewpoints

On the other hand, technology industry bodies and multinational cloud players have defended the policy direction, stating publicly that long-term incentives are essential to attract capital-intensive investments and position India as a global hub for cloud and AI services. Proponents argue that hyperscaler-led growth strengthens the broader digital ecosystem, including startups, enterprises, and government platforms.

A Broader Policy Question

While the Budget underscores India's ambition to become a digital and AI-driven economy, critics note the absence of comparable long-term incentives for domestic cloud providers and Indian SaaS infrastructure players many of whom are already investing without similar fiscal support. As AI workloads, government platforms, and enterprise systems increasingly migrate to the cloud, industry leaders say the policy debate is no longer just about infrastructure, but about ownership, pricing power, and who captures long-term value in India's digital economy.

The Budget accelerates cloud infrastructure growth but it also raises a fundamental question: will India merely host global cloud platforms, or build sovereign digital capabilities it can own and export?

KONICA MINOLTA

EXPERIENCE THE COLOURFUL TRANSFORMATION

RETHINK COLOURS

RETHINK INTELLIGENT INNOVATIONS FOR WORKPLACE

PRINT I COPY I SCAN

A3 Colour & Mono Multifunctional Printers

bizhub i-Series

For more information: SMS "KM MFP" send to 52424 or Call: 1-800-266-2525.

Konica Minolta Business Solutions India Pvt. Ltd.
www.konicaminolta.in | marcom@bin.konicaminolta.in
Connect with us:

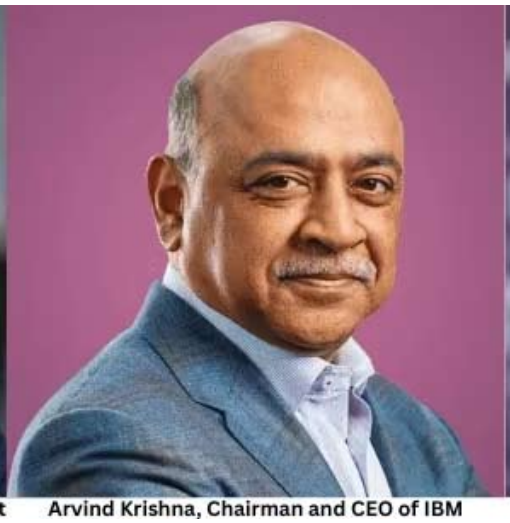
Giving Shape to Ideas

TRANSCON ELECTRONICS PVT. LTD.

205, 2nd Floor, Center Point Building, Hemanta Basu Sarani,
Opp. Lalit Great Eastern Hotel, Kolkata - 700001
Ph.: 22488118, 22488210, 22481620,
Mobile: +91-8337071326, Fax: 03322486604
Email: abhishek@transconelectronics.com,
Website: www.transconelectronics.com

Davos 2026: Global IT Leaders Say AI and IT Are Now the Operating System of the Economy


Sundar Pichai, CEO of Google and Alphabet


Arvind Krishna, Chairman and CEO of IBM


Elon Musk CEO of Tesla and SpaceX

At the World Economic Forum 2026, global technology leaders, policymakers, and enterprise executives converged around a clear message: information technology is no longer a back-office function—it is now the operating system of the global economy.

Across discussions on artificial intelligence, cloud infrastructure, cybersecurity, and digital public platforms, the focus shifted away from experimentation toward accountability, governance, and long-term resilience. For CIOs and technology leaders, Davos 2026 marked a turning point in how digital transformation will be measured and governed.

Artificial Intelligence Moves Into Core Enterprise Infrastructure

One of the dominant themes at Davos was the transition of artificial intelligence from pilot projects to enterprise-scale infrastructure. Executives aligned with the view frequently expressed by Satya Nadella , Chief Executive Officer of Microsoft, that AI must be embedded directly into productivity, decision-making, and operational workflows rather than treated as a standalone innovation initiative.Enterprise leaders emphasized that AI adoption in 2026 will be judged not by speed of deployment but by trust, explainability, and measurable outcomes.

Compute, Energy, and Physical Limits Shape the Next Phase of IT

As AI adoption accelerates, conversations at Davos increasingly focused on the physical realities of scale. The need for compute capacity, reliable energy infrastructure, and resilient data centers featured prominently—reflecting concerns often highlighted by Elon Musk CEO of Tesla and SpaceX, around the limits imposed by hardware, power, and supply chains. Technology leaders acknowledged that future IT strategies must account for sustainability, energy efficiency, and geopolitical dependencies alongside software innovation.

Enterprise Trust and Governance Take Center Stage

Trust emerged as a defining factor for enterprise technology adoption. Industry leaders echoed principles long advocated by** Arvind Krishna, Chairman and CEO of IBM, **stressing that AI and hybrid cloud systems will only scale in environments where security, compliance, and governance are designed into platforms from the outset. At Davos, CIOs discussed the growing importance of zero-trust security models, auditability, and regulatory readiness as competitive necessities rather than compliance obligations.

Governments Shape the Digital Framework

Davos 2026 also highlighted the increasing role of governments in shaping digital ecosystems. India's digital public infrastructure model was frequently referenced, with policymakers pointing to frameworks championed by Ashwini Vaishnaw India's Minister for Electronics and Information Technology, that prioritize interoperability, inclusion, and national-scale platforms. For multinational enterprises, this signals a future where IT strategy must align closely with public digital infrastructure, data residency laws, and cross-border regulatory frameworks. Technology With Societal Responsibility Long-term perspectives on technology's societal role—often associated with Bill Gates— Co-chair of the Bill & Melinda Gates Foundation, resurfaced throughout Davos discussions. Leaders emphasized that innovation must translate into productivity gains, workforce enablement, and economic resilience, not just efficiency or automation. This outlook is reshaping how

boards evaluate technology investments in 2026 and beyond.

Complementing these perspectives, industry veterans such as Sundar Pichai, CEO of Google and Alphabet, pointed to the importance of responsible AI deployment at internet scale, while Andy Jassy, President and CEO of Amazon, highlighted the need for enterprises to rethink cloud cost structures, resilience, and operational discipline as digital workloads mature. Collectively, these viewpoints signaled a clear shift for CIOs and CXOs in 2026: IT strategy is now inseparable from business risk management, national policy alignment, and long-term value creation, marking a decisive evolution in how technology leadership will be measured in the years ahead.
What This Means for CIOs in 2026

The collective message from Davos is clear:

- IT strategy is inseparable from business strategy
- AI strategy is inseparable from governance
- Infrastructure decisions now carry economic and geopolitical implications

CIOs are increasingly expected to operate as enterprise risk managers, transformation leaders, and custodians of digital trust. As the World Economic Forum 2026 concludes, one conclusion stands out: the future of the IT industry will be defined less by rapid adoption and more by responsible implementation. For global enterprises, leadership in 2026 will belong to those who balance innovation with accountability and ambition with resilience.

India in 2026: Should Technology Nationalism Shape the Future of Cloud, AI and Security?

As geopolitical tensions between India and the United States continue to surface, technology is no longer sitting quietly in the background of diplomacy and trade. In 2026, cloud infrastructure, artificial intelligence and cybersecurity have moved firmly into the realm of strategic assets, raising a pressing question for policymakers and business leaders alike: should India actively promote technology nationalism to safeguard its digital future?

This debate is less about ideology and more about exposure. Over the past decade, India's rapid digitization has leaned heavily on global technology platforms headquartered overseas. That dependence has enabled scale and innovation, but it has also concentrated control over data, compute and security outside India's jurisdiction. In stable times, this arrangement appears efficient. In periods of geopolitical uncertainty, it begins to resemble a structural risk.Technology nationalism, however, need not imply isolation or rejection of global ecosystems. In 2026, the more relevant objective for India is balance. A resilient technology strategy allows a nation and its enterprises to adapt, renegotiate and recalibrate without disruption. Promoting domestic capability is therefore not about excluding foreign players, but about avoiding single-point dependence in systems that now underpin economic and national security.

Cloud infrastructure sits at the centre of this recalibration. As critical workloads migrate to the cloud, questions around data residency, legal control and operational sovereignty have become unavoidable. For regulated sectors such as banking, government services, healthcare and critical infrastructure, cloud decisions now carry long-term strategic consequences. Encouraging locally governed cloud platforms for sensitive workloads, while continuing to leverage global providers for scale and innovation, reflects a pragmatic middle path for India in 2026. Artificial intelligence presents a parallel challenge. AI is shaped not only by algorithms, but by the data it consumes and the compute environments it relies on. When these foundations are externally controlled, long-term dependency becomes embedded into innovation itself. A nationalist AI approach for India does not require competing directly with global AI giants. Instead, it calls for domestic stewardship of critical datasets, locally governed AI platforms for public-sector and national-use cases, and sustained support for homegrown research and startups.

Cybersecurity, meanwhile, leaves little room for ambiguity. Security tools and incident response systems depend on trust, transparency and jurisdictional control. In 2026, reliance on opaque or externally governed security stacks increases both enterprise and national risk. Strengthening indigenous security capabilities, local security operations centres and domestic response frameworks is increasingly viewed not as a preference, but as a necessity. For Indian CXOs, this conversation is already translating into boardroom decisions. Technology choices made today will determine how resilient organizations are to regulatory shifts, pricing pressures or geopolitical disruptions tomorrow. The defining question of 2026 is no longer which technology is the most advanced, but which technology mix best protects the business.

Microsoft Shares Drop 7% After Q2 Results as Record AI Spending Rattles Wall Street

Microsoft's stock suffered a notable sell-off in global markets this week despite reporting better-than-expected financial results for the second quarter of fiscal 2026, highlighting growing investor unease around capital spending on artificial intelligence and cloud computing growth. The tech giant, long viewed as a bedrock of enterprise IT and innovation, saw its share price slide as much as 10% in one of the steepest single-day value declines in recent years, wiping out roughly $360 billion in market capitalization.

The company delivered financial performance that exceeded Wall Street forecasts, posting quarterly revenue of approximately $81.3 billion, up around 17% year-over-year, alongside solid profit growth. Microsoft's Intelligent Cloud division—the unit that houses Azure and AI-related workloads once again posted strong results, crossing more than $50 billion in cloud revenue for the quarter.

Yet investors were quick to focus on other signals from the earnings release that tempered enthusiasm. Chief among the concerns was record capital expenditure, which surged dramatically compared with the prior year as Microsoft continued to build out data-centre capacity and invest in hardware, software and infrastructure needed to support generative AI workloads. This heightened spending comes at a time when the company's flagship cloud business Azure showed a marginal deceleration in growth metrics compared with prior periods.

Market participants also homed in on disclosures around future contracted revenue. Microsoft's remaining performance obligations—a proxy for contracted cloud and software revenue yet to be recognized—expanded substantially, with a notably large share tied to commitments from its long-standing AI partner OpenAI. Roughly 45% of the company's massive backlog is now connected to this relationship, a fact that some analysts say introduces concentration risk into what investors had viewed as a diverse future revenue stream.

The negative market reaction underscores a deeper shift in investor expectations for Big Tech. Strong earnings themselves are no longer sufficient; stakeholders are increasingly demanding clearer evidence that the massive capital outlays being directed toward next-generation computing especially artificial intelligence—will translate into durable margin expansion and consistent free cash flow growth. Analysts tracking the sell-off pointed to slowing Azure growth momentum and aggressive AI infrastructure spending as principal catalysts for the stock's underperformance.

The broader technology sector felt the ripple effects of Microsoft's retreat. Major U.S. equity benchmarks like the Nasdaq Composite and S&P 500 closed lower as software and cloud stocks bore the brunt of selling pressure, even as other segments such as consumer tech and industrials held firmer.

Management emphasized at the earnings call that Microsoft's strategy remains focused on long-term value creation through innovation and capacity expansion, especially in artificial intelligence. However, the current market reaction suggests that investors are placing a higher premium on more immediate monetization signals and sustainable near-term growth forecasts—especially in units such as cloud infrastructure that have historically driven premium valuations for the company.

Despite the stock decline, several Wall Street firms reiterated their longer-term confidence in Microsoft's leadership in enterprise cloud and AI. Analysts noted that while the stock's short-term performance reflects a repricing of risk, the company's entrenched position across software, productivity tools, and cloud adoption gives it structural advantages that could support recoveries in value over strategic time horizons.

The mixed reaction from markets encapsulates a larger tension gripping global technology sectors as AI transitions from early-stage hype to broad commercial deployment. Companies that once commanded investor confidence based on innovation leadership must now justify how that innovation translates into scalable, profitable businesses that deliver returns on investment in shorter cycles.

For Microsoft, the current episode marks a litmus test in balancing heavy investment with investor patience, setting the stage for a closely watched performance in upcoming quarters.

Nokia Explores New Global Capability Centre and R&D Expansion in Karnataka

Telecommunications major Nokia Corporation is looking to expand its presence in Karnataka by exploring the establishment of a Global Capability Centre (GCC) along with additional research and development facilities, according to the state's Industries Minister.

The discussions took place on the sidelines of the World Economic Forum (WEF), where Nokia engaged with the Karnataka government, signalling continued confidence in the state's technology ecosystem. Nokia already operates its largest global research centre in Bengaluru, marking over 25 years of sustained presence in the region.

As part of the proposed expansion, the Karnataka government has assured Nokia of full support, including facilitation for new operations in Bengaluru as well as potential expansion into Tier-2 cities across the state. The move aligns with the state's broader strategy to attract high-value technology investments beyond the capital city and strengthen regional innovation hubs.

Industry observers note that Nokia's plans reflect a growing trend among global technology firms to deepen their India operations through GCCs that support research, engineering, global delivery, and enterprise services. Karnataka, with its mature talent pool, startup ecosystem, and strong policy backing, continues to remain a preferred destination for such investments.

Through this expansion, Nokia aims to tap into local engineering talent and innovation capabilities to strengthen its global R&D and delivery footprint. The initiative is also expected to reinforce Karnataka's position as a strategic hub for advanced telecommunications, enterprise networking, and next-generation technology development.

Further details on timelines, investment size, and locations are expected to emerge as discussions progress.

As enterprises move into 2026 under sustained cost pressure and heightened accountability, B2B events are undergoing a fundamental reset. What was once driven by executive networking, brand visibility, and high-profile CXO gatherings is now being evaluated through a far sharper lens: direct revenue impact and regulatory compliance. Across boardrooms, the defining question has changed. It is no longer "How many CXOs attended?" but "What measurable business outcome did this event deliver?" For marketers and event leaders, this shift represents both a challenge and a turning point.

CIOs Reset Expectations: From Engagement to Outcomes

CIOs and CXOs today operate under intense scrutiny from boards and CFOs, with technology and marketing spend increasingly tied to measurable business value. Events are no longer viewed as discretionary brand exercises but as commercial investments expected to influence pipeline, accelerate deals, or support account expansion. This mindset reflects a broader enterprise philosophy articulated publicly by global technology leaders.

Satya Nadella, Chairman and CEO of Microsoft, has repeatedly emphasized that technology investments must focus on "creating real value for customers and measurable business outcomes." That principle is now shaping how CIOs assess marketing-led initiatives, including events. As a result, events that cannot demonstrate a credible path to revenue are increasingly being reassessed during budget approvals.

SATYA NADELLA,
Chairman and CEO, Microsoft

CFO Discipline Tightens Event ROI Scrutiny

The growing influence of CFOs in marketing and technology decisions has further accelerated this change. Andy Jassy, President and CEO of Amazon, has publicly stated that Amazon evaluates investments through the lens of long-term return and operational efficiency, stressing that spending must deliver "clear customer and business value." For marketers, this means event budgets are no longer protected by legacy assumptions. CIOs now expect events to:

- Influence active sales pipelines
- Accelerate buying decisions
- Support renewals or account expansion

Large-scale conferences built primarily around visibility or executive presence are finding it harder to justify their cost unless they can

demonstrate downstream revenue impact.

Indian IT Leaders Reinforce the Outcome-Driven Shift

India's IT services leadership has echoed this results-focused approach. Salil Parekh, CEO of Infosys, has stated in public forums that go-to-market initiatives and client engagements must remain outcome-focused, aligned to business value rather than activity volume.

Government Signals: Impact Over Optics

From a policy standpoint, the emphasis on outcomes over optics is consistent with statements from** Ashwini Vaishnaw,** India's Minister for Electronics and Information Technology, who has repeatedly stressed that digital initiatives—public or private—must demonstrate measurable impact and economic value, not just participation or presence.

This thinking is now influencing public-private industry events as well, where government participation is more closely aligned with investment, innovation, and ecosystem outcomes rather than ceremonial presence.

DPDP Act Adds a New Layer of Complexity

Alongside revenue pressure, event marketers in India face another major constraint in 2026: data protection compliance under the Digital Personal Data Protection (DPDP) Act. The Act introduces stricter requirements around consent, purpose limitation, transparency, and lawful data usage. Personal data must be collected with clear, informed consent, and any sharing of attendee information with sponsors must be explicitly disclosed.

These requirements have fundamentally changed how event registrations and attendee databases are built and managed.

Shift Toward Consent-Compliant Attendee Sourcing In response, enterprises are increasingly favouring first-party and consent-compliant data sources, including established media platforms and owned communities, for event attendee sourcing. This approach provides clearer consent trails and reduces legal and reputational risk.

While this shift may limit scale, it improves data quality and compliance—factors that are becoming non-negotiable for CIOs, legal teams, and enterprise buyers. Scale Gives Way to Precision

The combined pressure of revenue accountability and data protection has made large, open-invite events harder to justify. Event Marketing Managers now face higher acquisition costs, longer planning cycles, and closer coordination with legal and sales teams.

As a result, many organizations are moving toward fewer, more focused events designed to engage defined buying groups rather than broad audiences. Closed-door, high-intent formats aligned with account-based marketing (ABM) strategies are increasingly preferred over mass conferences.

ASHWINI VAISHNAW,
Minister, Electronics and Information Technology, India

Events Become an Extension of Sales Strategy

To meet CIO expectations, marketers are redesigning events as extensions of sales strategy, not standalone brand platforms. This includes:

- Pre-identified target accounts and buying groups
- Invitation-only or closed-door formats
- Integration with CRM and pipeline systems
- Post-event revenue attribution and performance tracking

As CIOs become co-owners of go-to-market success, marketing teams are expected to operate with the same revenue discipline as sales.

A Changing Role for Event Marketing Leaders

This evolving landscape is also redefining the role of Event Marketing Managers. Success in 2026 increasingly requires:

- Alignment with sales and revenue teams
- Understanding of data governance and consent frameworks
- Ability to track post-event commercial impact

Event leadership is moving beyond logistics and branding toward commercial and compliance accountability.

The New Reality for 2026

The shift underway does not signal the end of B2B events—but their evolution. In 2026:

- Events without revenue accountability will struggle to secure approval
- Visibility must support conversion, not replace it
- CIO–CMO alignment will define success

As Bill Gates has noted in public discussions on technology investment, progress is meaningful only when it translates into real-world impact. That principle now governs how enterprises evaluate events.

For CIOs and CXOs, this transformation brings greater confidence that events align with enterprise priorities. For marketers, it represents a challenging but necessary evolution toward credibility, accountability, and sustainable business impact.

How Indian Distributors Can Get Ahead in 2026: Strategy Lessons from ANZ, Adapted for India

As global distribution evolves rapidly in the cloud and AI era, Indian technology distributors are uniquely positioned to lead the next wave of growth if they adopt strategic practices now seen shaping markets abroad. A recent industry analysis highlighted that distributors must deliver scalable reach, reduced risk, and value-added services to remain the most cost-effective route-to-market for vendors and partners. Their ecosystems accelerate partner productivity and enable faster market expansion by combining technical enablement, financing, digital marketplaces, and orchestration.

India's IT distribution landscape is already substantial and growing, with key players such as Redington, Supertron, Savex Technologies, RP Tech, and Iris Computers collectively serving tens of thousands of channel partners nationwide and helping propel the country's burgeoning tech ecosystem. To navigate 2026 successfully, distributors in India must build "next-generation intermediary models" that reflect both deep local market understanding and the global shift toward platform-centric, services-oriented distribution.

First, expand beyond product delivery to strategic enablement. Traditional distribution must give way to value-added services from marketing support and training to lifecycle services and digital commerce enablement. As industry research abroad has shown, clear goal alignment, transparent communication, and jointly developed growth plans between distributors and their OEM partners help prevent margin erosion and strengthen long-term alliances.

Indian distributors are already moving in this direction. Redington, for example, has been gradually transforming from a hardware-centric player into a broader technology solutions provider, emphasizing cloud, software, and AI-driven innovations, while deepening partner engagement in tier-2 and tier-3 markets. Mainstreaming such a transition across the distribution community will help capture value beyond traditional hardware margins and align distributor success with the digital transformation priorities of enterprise customers.

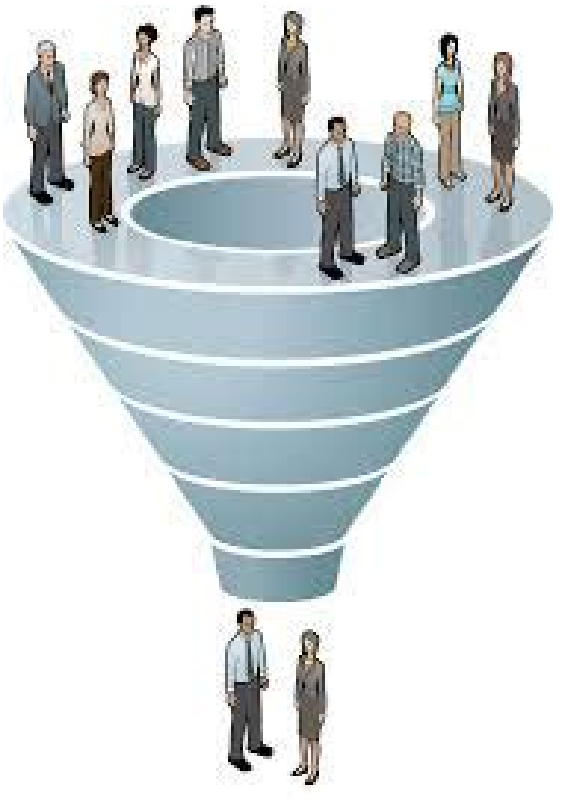
Second, digital enablement and data-driven operations can be differentiators. Modern distribution strategy calls for robust digital platforms, real-time visibility into inventory and demand, and data-backed decision frameworks that improve operational efficiency and responsiveness. This trend is resonating globally and is highly relevant in India, where demand cycles are tightening and enterprise adoption of cloud and AI solutions continues to accelerate.

Third, deepen partner ecosystems with targeted vertical and regional plays. Redington ,RP Tech and Savex, with their extensive nationwide networks, are examples of distribution houses that can build specialized segment offerings—for instance, in enterprise networking, storage, and modern workspace solutions by working closely with local system integrators and MSPs. Surpertron and Iris Computers, often strong in niche verticals and regional geographies, can leverage their domain depth to co-create solutions that are tooled for specific customer segments, whether in healthcare, education, or manufacturing.

Finally, focus on execution and strategic discipline. Industry commentary highlights that distributors often stall not for lack of ideas but because strategy execution lags. Indian distributors that combine strategic clarity with operational excellence prioritizing execution on growth initiatives, partner enablement, and digital transformation—will be well placed to capture market share as others fall behind.

As distribution continues to shift from a transactional model to a strategic go-to-market engine for technology suppliers, Indian distributors that embrace this evolution blending scale, service, digital maturity, and partner-centricity will lead the channel in 2026 and beyond.

Deal Registration vs Direct Approach: Why the Friction Is Growing



As vendor go-to-market models evolve, deal ownership is becoming a governance issue .Deal registration has long been positioned as the foundation of trust between technology vendors and their channel partners. In theory, it protects partner investments in prospecting, solution design, and customer engagement. In practice, as vendors scale faster and pursue aggressive growth targets, the line between partner-led deals and direct sales motions is becoming increasingly blurred. Across the technology ecosystem, channel partners are raising concerns that deal registration frameworks are not always enforced consistently particularly in large, strategic, or high-value opportunities. Instances where vendors engage customers directly, despite registered partner involvement, are creating friction that goes beyond commercial disagreements and into governance territory.

Why Deal Registration Matters More Than Ever

Today's channel partners are not merely resellers. They are responsible for deal shaping, local execution, integration, and post-sales accountability. Registering a deal is often the trigger for partners to commit resources—technical teams, presales effort, certifications, and sometimes financial exposure. When a registered opportunity is later approached directly by a vendor's field sales team, partners report:

- Loss of deal confidence
- Margin uncertainty
- Delays in customer decision-making
- Strained partner–vendor relationships

More critically, this dynamic can impact the customer experience, as overlapping vendor and partner engagement often leads to confusion around ownership and accountability.

Why Vendors Are Increasing Direct Engagement

From the vendor perspective, direct engagement is often driven by:

- Pressure to close large or strategic deals within a quarter
- Global account alignment requirements
- Cloud and subscription revenue models that demand tighter control
- Customer requests for direct vendor involvement

However, when these direct approaches bypass or dilute registered partner participation, they undermine the very trust structures that channel ecosystems depend on.

The CXO Impact: From Channel Friction to Enterprise Risk

For enterprise buyers, deal registration conflicts are rarely visible—but their consequences are. Misaligned engagement models can result in:

- Slower procurement cycles
- Unclear delivery ownership
- Escalation challenges post-sale
- Increased total cost of ownership

As a result, deal registration and direct sales overlap are no longer internal channel issues. They are increasingly viewed by CIOs and procurement leaders as vendor governance risks.

What Strong Governance Looks Like

Vendors that are managing this transition effectively are focusing on:

- Clear rules of engagement between direct and partner sales teams
- Enforced deal protection mechanisms
- Transparent escalation paths for disputes
- Joint accountability models for large enterprise accounts
- Consistent communication to customers on ownership and delivery roles

These measures are becoming differentiators as channel partners prioritise predictability and trust when deciding where to invest.

Looking Ahead

As vendor ecosystems continue to scale in 2026, the balance between direct sales ambition and partner trust will define long-term success. Deal registration cannot remain a symbolic process—it must function as a governance commitment. For vendors, the question is no longer whether to work directly or through partners, but how to do both without eroding trust. For channel partners and enterprise buyers alike, predictability and alignment are becoming as important as pricing and product capability.

Why Enterprise AI Governance Has Become a Boardroom Imperative

Enterprise AI governance has moved from policy decks to boardroom priority as organizations accelerate AI adoption across business-critical functions. What was once treated as a compliance checkbox is now being reframed as a strategic operating layer—one that determines whether AI delivers sustainable value or becomes a source of reputational, regulatory, and operational risk. As AI systems increasingly make or influence decisions, enterprises are realizing that innovation without governance is no longer defensible.

Speaking at the World Economic Forum, Satya Nadella, Chairman and CEO of Microsoft, underscored the responsibility that comes with deploying AI at scale. He noted that trust is the foundational requirement for AI adoption, emphasizing that technology companies and enterprises alike must ensure AI systems are secure, explainable, and aligned with human values. Microsoft has since positioned responsible AI governance as a prerequisite for enterprise-scale deployment, not an afterthought.

This sentiment is echoed across the broader technology ecosystem. During Google I/O and subsequent public forums, Sundar Pichai, CEO of Google, has repeatedly stated that AI must be developed and deployed responsibly, highlighting the need for clear guardrails as AI capabilities advance rapidly. Pichai has warned that without thoughtful governance, the pace of innovation could outstrip society's ability to manage its consequences—particularly in areas such as bias, misinformation, and decision accountability.

Within enterprises, AI governance is no longer limited to data privacy and model accuracy. It now spans model lifecycle management, auditability, human oversight, and ethical use. According to Gartner, organizations that fail to establish formal AI governance frameworks risk regulatory penalties, brand erosion, and internal resistance to AI adoption. Analysts note that governance is becoming a key enabler of scale, allowing enterprises to deploy AI confidently across regions, business units, and regulatory environments.

The financial services sector has been among the earliest adopters of enterprise AI governance, driven by strict regulatory scrutiny. In a public interview, Jamie Dimon, CEO of JPMorgan Chase, acknowledged both the transformative potential of AI and the need for strong controls. He has emphasized that while AI can dramatically improve productivity and risk management, it must be implemented with rigorous oversight to avoid unintended consequences in highly regulated environments.

From a risk and ethics perspective, global institutions are also weighing in. Brad Smith, President of Microsoft, has been one of the most vocal advocates for AI governance, calling for clear rules, transparency, and accountability mechanisms. In multiple public statements, Smith has argued that AI governance is not about slowing innovation, but about ensuring that innovation earns and retains public trust.

At the enterprise level, AI governance is increasingly being treated as a cross-functional mandate rather than an IT-only responsibility. Legal, compliance, risk, HR, and business leaders are being brought into governance councils to define acceptable use, escalation paths, and accountability models. A global CIO at a CXO roundtable summarized the shift succinctly: governance is no longer about saying "no" to AI, but about defining how to say "yes" safely and repeatedly.

The urgency is further amplified by emerging regulations such as the EU AI Act and evolving data protection laws worldwide. These frameworks are pushing enterprises to document AI decision logic, ensure human-in-the-loop controls, and maintain traceability across AI systems. For multinational organizations, consistent governance has become essential to avoid fragmented compliance approaches across regions.

For CXOs, the message is becoming clear: enterprise AI governance is not a barrier to innovation—it is the foundation that allows innovation to scale. Organizations that invest early in governance frameworks are finding it easier to deploy AI responsibly, earn internal and external trust, and respond quickly as regulations and technologies evolve. As AI becomes embedded in core business decisions, governance is emerging as the quiet force that separates sustainable AI leaders from those exposed to long-term risk.

HOW AI is destroying Consulting ?

The consulting industry is entering a structural reset, and artificial intelligence is no longer a peripheral tool—it is actively hollowing out the traditional consulting value chain. This shift became impossible to ignore when McKinsey & Company confirmed workforce reductions of roughly 10%, a move widely reported and interpreted as part of a broader recalibration rather than a cyclical slowdown. As McKinsey stated in internal communications quoted by multiple media outlets, the firm was "adjusting capacity to better align with demand and new ways of working," a phrase that, read plainly, signals automation and AI-led efficiency replacing human-heavy delivery models.

Data backs this up. According to Forbes, consultants spend close to 19% of their time on research, 4–6 hours per day on strategy writing, and 5–10 hours per week on financial analysis—all activities now routinely executed by large language models in minutes. Junior consultants, long tasked with slide production, reportedly spend up to 70% of their time preparing and polishing presentations, a function increasingly automated by AI-powered tools that generate brand-aligned decks instantly. Even senior managers and partners, who traditionally justify their leverage through synthesis and judgment, spend 2–3 hours per week reading reports, a task now reduced to near-zero through AI summarization engines that extract key findings, risks, and recommendations on demand.

What makes this moment different from past productivity waves is that AI doesn't just accelerate consultants—it replaces entire layers of billable effort. Research workflows can be executed end-to-end using structured prompts; financial models can be interpreted, stress-tested, and narrated by copilots; and strategy documents can be drafted, refined, and scenario-tested without armies of associates. As one former Big Four partner told Forbes, "Clients are no longer paying for effort—they're paying for outcomes. AI exposes how much of consulting was effort masquerading as insight."

This doesn't mean consulting is disappearing—but it is shrinking, polarizing, and becoming unforgiving. The pyramid model that sustained the Big Four for decades depends on large junior teams doing repeatable work. AI collapses that pyramid. What remains valuable is judgment, accountability, stakeholder management, and decision ownership—capabilities that cannot be fully automated but can no longer be propped up by bloated teams. McKinsey's layoffs are not proof that consulting is dead; they are proof that the old consulting operating model is no longer defensible. The firms that survive will be smaller, more senior, more AI-native—and brutally focused on measurable impact rather than billable hours.

Digital Transformation Isn't the Problem–Slow CXO Decision-Making Is Killing ROI

Global enterprises are investing in digital transformation at an unprecedented scale, yet a growing body of evidence shows that returns on these investments continue to lag expectations not because technology is failing, but because corporate decision-making is failing to keep pace.

According to IDC, global digital transformation spending is projected to reach nearly $3.9 trillion by 2027, driven by rapid adoption of cloud platforms, AI, automation, cybersecurity, and data analytics. However, Gartner estimates that close to 70% of digital transformation initiatives fall short of their intended ROI, and nearly half stall after pilot or early deployment stages. This widening gap between digital capability and organizational execution has become a defining issue across global boardrooms. CXOs increasingly acknowledge that technology is moving at real-time speed, while enterprises are still governed by quarterly mindsets, multi-layered approvals, and risk frameworks built for a pre-digital era.

Microsoft Chairman and CEO Satya Nadella has repeatedly highlighted in public forums and LinkedIn reflections that digital transformation fails when organizations do not change how decisions are made, owned, and incentivized, stressing that culture and operating models—not tools—are the real constraints.

Google Cloud CEO Thomas Kurian has similarly noted in public remarks that enterprises no longer struggle to access advanced technology but struggle to align leadership, risk, and business teams quickly enough to act on it. Data supports this view. McKinsey research shows that companies with fast, data-driven decision-making are five times more likely to outperform peers financially, yet fewer than 30% of enterprises say they can approve critical digital investments within weeks. Instead, decisions are trapped in steering committees, budget cycles disconnected from product roadmaps, and fragmented ownership between IT, finance, compliance, and business units. This structural delay often results in missed market windows, underutilized platforms, and diluted outcomes, after which digital initiatives are blamed for failing to deliver ROI.

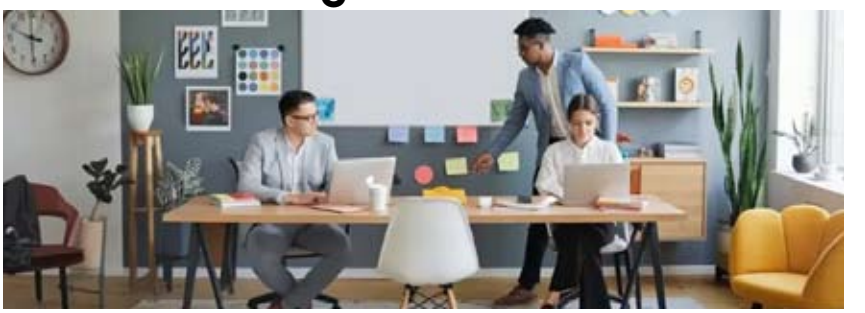
Kalpana Singhal Editor and Co-founder ITPV shared " that by the time approvals are secured, the market opportunity has already shifted, and technology is unfairly held responsible for delays rooted in human and organizational inertia". A global financial services CDO echoed this sentiment on X, observing that many digital programs are still governed using legacy quarterly review structures while competing in markets that move weekly, if not daily. Boston Consulting Group estimates that nearly 60% of digital value leakage stems from slow decision-making and unclear governance, compared to only 20% caused by technology limitations, underscoring that ROI erosion is primarily a leadership and execution problem.

Salesforce Chair and CEO Marc Benioff has publicly stated that companies fail at digital transformation when they treat innovation as a project rather than an operating model, emphasizing that decision velocity is now a core competitive advantage rather than a soft leadership attribute. The issue has become even more visible with the rise of AI. While AI models can be deployed in weeks, PwC data shows that only 18% of organizations have moved beyond AI pilots into scaled deployment, despite 73% of executives believing AI will fundamentally reshape their businesses. NVIDIA CEO Jensen Huang has pointed out in widely circulated industry commentary that the biggest limiter to AI adoption is not compute power, but organizational readiness and the ability of leaders to make timely decisions. AI, in effect, has exposed the deeper crisis of enterprise decision-

making, revealing how risk aversion, unclear accountability, and outdated governance slow down value creation. World Economic Forum analysis indicates that fewer than 35% of organizations have modernized governance frameworks to support agile, product-led digital delivery, leaving most enterprises attempting to run exponential technologies through linear approval systems. In contrast, high-performing digital organizations are redesigning decision rights, delegating authority closer to execution, aligning KPIs around outcomes rather than activities, and funding digital initiatives dynamically rather than annually. Research from MIT Sloan shows that digitally mature companies deliberately reduce decision latency and treat governance itself as a product that must be continuously optimized. A global manufacturing executive shared on LinkedIn that the company's biggest digital breakthrough did not come from new platforms but from reducing decision timelines from 90 days to under two weeks, enabling teams to capture value while opportunities were still relevant. For CXOs and boards, the implications are increasingly clear and uncomfortable.

Digital transformation is no longer primarily a technology challenge; it is a leadership, governance, and operating model challenge. Boards continue to demand rapid innovation while maintaining control structures designed to prevent risk, creating an inherent contradiction. As one global CHRO noted in a public post, organizations cannot expect innovation outcomes from systems designed to avoid uncertainty. Measuring digital ROI on quarterly cycles while operating in real-time markets further compounds the issue, leading to premature judgments and stalled momentum. In this environment, digital becomes the scapegoat for deeper organizational dysfunction. The next phase of transformation, CXOs now argue, must focus on fixing decision-making before fixing tools. Enterprises that align decision velocity with digital velocity are already pulling ahead, while those that do not will continue to see delayed returns, rising frustration, and eroding competitiveness. In an economy defined by speed, adaptability, and continuous disruption, the ability to decide quickly and act decisively has become as critical as the technology itself. Until corporate decision-making catches up, digital transformation will remain stuck in neutral capable of delivering value, but consistently prevented from doing so by the very organizations that invested in it.

Inside Tech Marketing's Growth Paradox: Why Legacy Comfort Is Holding Revenue Back



Across the IT industry, a quiet contradiction is playing out behind closed boardroom doors. While tech companies speak the language of innovation, AI, and scale, many continue to run their marketing engines on legacy talent models and comfort-driven vendor relationships. An internal review across multiple enterprise and mid-market firms reveals a recurring pattern: growth ambitions are rising, but marketing structures remain designed for stability, not speed.

At the center of this paradox is how tech companies define "safe" marketing. Budgets are repeatedly routed to the same agencies, the same partners, and the same execution playbooks often with little scrutiny beyond surface-level activity metrics. Performance is inferred, not proven. Pipeline attribution remains opaque. In several cases, sales teams inherit leads without clarity on quality, intent, or conversion probability, while marketing success is declared based on volume rather than revenue impact. The result is predictable: rising CAC, slower pipeline velocity, and diminishing returns disguised as continuity.

What's notably missing from this equation is the next generation of marketers professionals fluent in AI optimization, experimentation frameworks, performance analytics, and real-time feedback loops. Unlike traditional roles centered on campaign execution, these marketers approach growth with a P&L mindset, questioning not just "what ran" but "what converted, scaled, and compounded." They are comfortable challenging vendor performance, replacing static retainers with outcome-linked models, and using technology to benchmark partners against hard revenue metrics rather than relationships.

Interviews across the ecosystem suggest that resistance to this shift is cultural, not technical. Young marketers are often excluded from strategic conversations, confined to execution, and evaluated on output rather than impact. Yet paradoxically, they are the ones best equipped to operate modern growth stacks connecting AI-driven content discovery, intent signals, automation, and sales enablement into a single revenue narrative. When empowered, they don't see marketing as a cost center; they see it as a scalable revenue function. The investigative takeaway for CXOs is uncomfortable but clear. Growth leakage is rarely due to lack of tools or budget it stems from who is allowed to challenge the system and how success is measured. Tech companies that continue optimizing for comfort will keep buying familiarity. Those that invite next-gen marketers into ownership roles, tie marketing decisions to pipeline economics, and let performance not tenure decide scale will unlock a very different growth curve. The choice, increasingly, is between inherited momentum and engineered growth.

Channel Point

From Policy to Protection: The Year of Execution

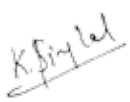
The Union Budget 2026–27 signals more than fiscal intent—it reflects India's evolving digital doctrine. As explored in our cover story, the conversation is no longer about isolated investments in IT. It is about infrastructure, cloud, cybersecurity, and AI governance converging into a unified digital economy strategy. The real test now lies in execution.

This issue moves from policy to practice.

In our New Year special candid chat, I speak with Sachin Kawalkar, CISO at Neeyamo, and Saurabh Barjatiya, CTO at GBB and Co-Founder of Cyber Vigilens, on what true ransomware readiness should look like in 2026. Their insights cut through complexity: layered defense, tested backups, skilled teams, integrated tools, and continuous assessment are not optional—they are foundational. Visibility without execution, as they rightly point out, is a dangerous illusion.

Across both conversations, a common thread emerges: tools alone do not deliver outcomes. People, partnerships, and disciplined execution do.

As we step into 2026, the ecosystem's challenge is clear—move from ambition to accountability, from dashboards to decisions, and from compliance checklists to operational resilience.



KALPANA SINGHAL, Editor, ITPV Channel Magazine
(E-mail: kalpana@techplusmedia.co.in)

TECHPLUS MEDIA

EDITOR: KALPANA SINGHAL
CONTENT HEAD: Amit Singh
CONSULTING EDITOR: Rajneesh De
NEWS ANALYST: Ishita Gupta
CORRESPONDENT: Bhawna Thapliyal
NEWS REPORTER: Anindita Majumder, Urmi Saha

INTEGRATED MARKETING COMMUNICATION:
Arunim Agrawal, Mamta Kapoor

ASSOCIATE ANALYST
Shaithra S

SALES:
Anushikha Singh | Pratap Jana

PRODUCTION HEAD:
Aji Kumar

WEBSITE:
Gaurav Rana

PROMOTION:
Amit Pandey, Nikita Gurung

CIRCULATION:
Pratap Ram

FINANCE:
Inder Pal

HEAD OFFICE:
370A, Sant Nagar, East of Kailash, New Delhi
Tel: 41625763, 26237405, 41620042
Email - kalpana@techplusmedia.co.in

MARKETING OFFICE:
10 UF, West Wing, Raheja Tower,
MG Road, Shanthala Nagar, Ashok Nagar,
Bengaluru, Karnataka-560001

Delhi: 91-8178321837 | **Mumbai:**91-98997 01316
Kolkata & Guwahati: 91-9331072026
Bangalore: 91-8851119532

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL Printed at Modest Graphics Pvt. Ltd., C 52-53, DDA Shed, Okhla Industrial Area, Phase - I, New Delhi-20, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, Editor- Anuj Singhal

LAPCARE®
INDIA

LAPCARE
DHURANDARR
is baar zyada maar

2026
Program

Exciting prizes

Dhurandarr lucky draw 2026 bigger rewards for bigger performance.

For more details contact :

dhurandarr@lapcare.com | +91-84487 50030 | www.lapcare.com

*T&C Apply

Postal Registration No. - **DL(S) 01/3377/2019-21 Posting Date - 13-14, 27-28**
Registered with Registrar of Newspapers of India under RNI No. **DELENG/2010/32787**

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, EDITOR: Anuj Singhal