

INDIA'S FRONTLINE IT MAGAZINE

VARINDIA

THE ULTIMATE *Voice* OF INDIAN VALUE ADDED RESELLERS



EASTERN INDIA INFORMATION
TECHNOLOGY FAIR 2025

THEME : CONNECTING THE
PHYSICAL AND DIGITAL WORLDS

5th SEPTEMBER 2025
HOTEL THE PARK, KOLKATA

SUBSCRIPTION COPY NOT FOR SALE

VOLUME XXVI ISSUE 11 JULY 2025 PRICE RS. 50



TP-Link: Building a Connected Future

BIJOY ALAYLO
COO & DIRECTOR
TP-LINK INDIA



Committed to the core for last **15+ years**
in securing and connecting Indians to the world,
and proudly **Made in India.**





World's First Pay-Per-Use Data Center Colocation for GPU Cloud Partners

India stands at the cusp of AI leadership, and businesses need scalable, sovereign digital infrastructure to seize this opportunity. Sify is poised to lead AI deployment at scale with the launch of the world's first Pay-Per-Use Colocation pricing model*, purpose-built for GPU and Neo Cloud companies.

AI Infrastructure Simplified:

-  First-of-its-kind hourly billed colocation service
-  Innovate on AI and scale on demand
-  Eliminates high CapEx investment risks
-  India's lowest-latency secured network to hyperscale clouds
-  End-to-end managed services



Know More

Contact us
marketing@sifycorp.com

INDIA'S FRONTLINE IT MAGAZINE

VARINDIA

THE ULTIMATE *Voice* OF INDIAN VALUE ADDED RESELLERS



23RD INFOTECH FORUM 2025
Theme - Balancing Innovation and Sustainability
4th July 2025, Hotel Hyatt Regency,
Bhikaji Cama Place, New Delhi

VOLUME XXVI ISSUE 11 JULY 2025 PRICE RS. 50 SUBSCRIPTION COPY NOT FOR SALE

INDIAN CIOs AND CXOs: NAVIGATING DISRUPTION, DIGITAL ACCELERATION, AND RESILIENCE

FOR MORE PAGE 22

Intel Reportedly Developing Gaming-Focused CPUs


Intel may be planning to launch gaming-specific CPUs, aiming to strengthen its position in the gaming



market, according to media reports. The move appears to mirror AMD's 3D V-Cache technology, which boosts performance by adding a larger, quickly accessible memory section for complex gaming tasks. This strategy could help Intel regain trust among gamers while enhancing processing capabilities for advanced gaming experiences, signaling a potential competitive shift in the CPU market.

Samsung Quietly Removes OEM Unlocking Option from One UI 8

Samsung's latest One UI 8 update, based on Android 16, has reportedly removed the OEM Unlocking option, preventing users from unlocking the bootloader to install custom ROMs. This change was discovered in the stable One UI 8 build on devices like the Galaxy Z Fold 7 and Galaxy Z Flip 7, as well as the One UI 8 Beta for the Galaxy S25 Ultra. According to reports from SammyGuru and XDA developers, the toggle has been completely removed from the firmware code, indicating a deliberate move by Samsung. Previously, OEM Unlocking allowed advanced users and developers to customize and flash their devices, a feature now inaccessible.




Empowering the Technology Industry to **OPTIMISE** and **ACCELERATE** the way they do business.

CONTEXT is a B Corp™ Certified company that specialises in providing market intelligence and analytics services for the technology industry.


We are a trusted partner for global technology leaders, delivering crucial insights that help shape strategic decisions and address business challenges.

Our advanced forecasting, analytics, and data management solutions are designed to integrate smoothly into the operations of major tech companies worldwide. This integration supports the monitoring of over £200 billion in annual sales transactions.


Our efforts are backed by a dedicated team of over 400 professionals, spread across more than 35 countries, with offices in key cities such as London, Berlin, Paris, Madrid, Milan, Warsaw, Johannesburg, Istanbul, Dubai, Chicago, Buenos Aires, São Paulo, Mumbai, Auckland, Singapore, Seoul, Taipei & Tokyo.



Certified



Corporation



www.contextworld.com



QUANTUM COMPUTING EMERGES AS THE NEXT FRONTIER

The global data centre industry is undergoing a profound transformation, fueled by the dual momentum of artificial intelligence (AI) and quantum computing. These two cutting-edge technologies are converging to redefine enterprise computing, ushering in an era that demands smarter, scalable, and future-ready infrastructure.

Quantum computing represents a radical departure from traditional computing methods. Unlike classical systems that use binary bits (0s and 1s), quantum computers utilize qubits, which can exist in multiple states simultaneously due to quantum principles like superposition and entanglement. This allows them to process a massive number of computations in parallel, enabling exponential speedups for certain complex tasks.

Quantum computing unlocks breakthroughs across sectors—optimizing supply chains, accelerating drug discovery, enhancing financial modeling, and enabling quantum-safe encryption. Quantum computing is advancing rapidly, with IBM, Google, and Microsoft leading R&D. Yet, scalable, fault-tolerant systems remain 5–10 years away. Meanwhile, booming AI workloads—especially from multimodal and generative AI—are fueling a projected 31.6% CAGR in the AI data centre market, set to reach \$933.76B by 2030.

Modern enterprise applications are becoming increasingly multimodal, integrating diverse data formats such as text, video, audio, and sensor inputs. This complexity necessitates data centres capable of supporting high-throughput, low-latency processing while maintaining energy efficiency. Colocation centres—facilities optimized for dense compute operations, smart power distribution, and cooling—are rapidly becoming the preferred model for hosting these advanced workloads.

Gartner estimates that by 2030, 80% of enterprise software will incorporate multimodal AI, a substantial leap from less than 10% in 2024. These AI systems are capable of synthesizing multiple data streams in real time to generate contextual, actionable insights. In industries such as manufacturing and logistics, such systems can enhance automation, improve safety, and optimize operations by interpreting data from video surveillance, IoT sensors, and human input simultaneously.

As AI models scale in complexity and capability, they are increasingly pushing the limits of classical infrastructure. While high-performance GPUs and TPUs like NVIDIA's H100 currently fulfill most AI processing needs, there's a growing interest in quantum computing as a long-term solution. Quantum systems excel at matrix operations and optimization problems—core to many AI algorithms—and could eventually complement classical computing in solving highly complex or resource-intensive tasks.

However, given the current limitations of quantum hardware, classical systems will continue to dominate AI deployments through the end of the decade. Nonetheless, the integration of quantum computing into specific high-value use cases—like drug discovery or materials research—is already underway. The foundation for quantum-augmented AI is being laid, with the expectation that, over time, these technologies will converge to unlock new possibilities in enterprise innovation.

India is emerging as a critical player in this global transformation. According to Savills India, the country's data centre capacity is expected to grow fourfold to 4 GW IT by 2030, registering a CAGR of 23%. In the first half of 2025 alone, 162 MW IT of capacity was added, with 212 MW IT absorbed—Mumbai and Chennai accounting for the majority share. At the same time, Kolkata leads in projected growth with a 48% CAGR, followed by Hyderabad and Ahmedabad.

Beyond Tier-I cities, India's Tier-II regions such as Bhubaneswar, Coimbatore, and Lucknow are fast becoming edge data centre hubs. These cities are expected to contribute more than 20% of national capacity by 2030, driven by regional demand, 5G rollout, and the need for localized content delivery.

India's digital infrastructure boom is being supported by strong government policies, increasing cloud adoption, and significant investment from hyperscalers and enterprise tech providers. This expansion is not just about meeting domestic demand—it's about positioning India as a global hub for data storage, processing, and AI innovation.

To stay ahead, India's next generation of data centres must be built to accommodate both advanced AI workloads and eventual quantum computing integration. This enables quantum computers to solve complex simulations and optimization problems beyond the reach of classical systems.

This requires designing facilities with high-density compute capacity, flexible scalability, and robust energy efficiency. As the AI landscape matures and quantum computing inches closer to viability, such infrastructure will be critical in supporting enterprise transformation.

Looking toward 2030, the convergence of AI, quantum computing, and intelligent infrastructure will redefine the digital economy. These technologies will collectively revolutionize how businesses operate, how data is analyzed, and how innovation is realized. For enterprises, governments, and investors alike, the time to act is now—aligning strategies to prepare for a future shaped by disruption, opportunity, and exponential technological advancement.

S. Mohini Ratna
Editor, VARINDIA
mohini@varindia.com

CABLES THAT DEFINE 4K CLARITY

DisplayPort™ to HDMI
and DisplayPort™ to DisplayPort™
Premium Cables



DPXTREME

CA-ADPHDC

Active DisplayPort™ Male to
HDMI Male Cable with Audio
Length: 2M, 3M.

DPXPRT

CA-DPCAB PLUS

DisplayPort™ to DisplayPort™
Cable with Audio
Length: 1.8M, 3M, 5M & 10M.



Warranty : rma@cadyce.com Online Chat : www.cadyce.com Email Support : support@cadyce.com Sales : sales@cadyce.com
Pune: 9226783571, 09322153959 | Mumbai: 09769726552, 09307742595 |
Maharashtra: 09890227701 | Gujarat: 09974800847 | Delhi: 09999071626, 82871 44075 | Bangalore: 9972534115, 09880660912 |
AP & TS: 09966194400, 88822 12998 | Tamil Nadu: 09500052809, 98408 94013 | Other Territories: 09699375712

Toll Free : **1800 266 9910**
Tech Support : **+91 9172212959**

Website: www.varindia.com

Publisher: Dr. Deepak Kumar Sahu
Editor: S Mohini Ratna
Executive Editor: Dr. Vijay Anand
Consulting Editor: Gyana Swain
Associate Editor: Samrita Baruah
Associate Editor: Syeda Beenish Khalid
Assistant Editor: Ramesh Kumar Raja
Art Director: Rakesh Kumar
Network Administrator: Ashok Kumar Singh
Visualizer: Ravinder Barthwal
Manager-IT: Subhash Mohanta
Manager-SEO: Santosh Kumar
Web Developer: Shivangi Mishra
SEO-Executive: Karan Arora

BUSINESS:
Commercial Manager: Amit Kumar Jha
Circulation Executive: Manish Kumar

CORPORATE OFFICE:
VAR House, A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road, New Delhi - 110030
Tel: 011-41656383, 46061809
Email: edit@varindia.com

Bangalore: Bureau office
Marketing Manager: S. Kamala kar
D-103 G.F., Ashish JK Apartments
Thubarahalli Extended Road
Bangaluru- 560066
Tel: 080-49530399 | Mobile:09886280836
E-mail: kamlakar@varindia.com

Mumbai: Bureau office
Regional Manager (West): Anil Kumar Sahu
Radha Krishna Complex, B/202, Plot no 24,
Sector-25, Kamothe, Navi Mumbai - 410206,
Maharashtra
Tel: 022-65561292, Mobile: 08108017479
E-mail: anil@varindia.com, mamta@varindia.com

Chennai: Bureau office
Branch Manager: K. Parthiban
F1, Meadows Green Apartments, 64, Chetty Street
1st Cross, Mel Ayanambakkam, Chennai - 600 095

Hyderabad: Bureau office
Branch Manager: Sunil Kumar Sahu
32-161/3, 202 Neha Paradise, Nr. Maissamma
Temple, Venketeswara colony
Ramakrishna Puram, Hyderabad - 500056
Telangana, Tel: 040-32989844/ Cell No. 08100298033
E-mail: sunil@varindia.com

Kolkata: Bureau office
Marketing Officer: Sunil Kumar
Correspondent: B Kiran Dutta
Haritasa Electronics Solutions Pvt Ltd
204 Tower- 2, PS Srijan Corporate Park,
Block EP-GP, Salt Lake, Sector - V, Kolkata - 700091
Mobile: 08100298033, E-mail: sunil@varindia.com
Mobile: 09903088480, E-mail: kiran@varindia.com

Bhubaneswar: Bureau office
Jagannath Warrior Residency, Suit No.A5/501,
Kaimatia Bhubaneswar-752054 | Cell No. 8100298033

Printed and Published by **Deepak Kumar Sahu** on behalf of
M/s. Kalinga Digital Media Pvt. Ltd. and Printed at Pushpak
Press Pvt. Ltd. Shed No. 203 - 204, DSIDC Complex, Okhla
Industrial Area, Phase-I, New Delhi-110020 and Published at
A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road,
New Delhi - 110030, Editor - S Mohini Ratna.

For Subscription queries contact: info@varindia.com
Subscription: Rs. 500(12 issues)Rs. 1000 (24 issues)

All payments favouring:
KALINGA DIGITAL MEDIA PVT LTD
© All rights are reserved. No part of this magazine may be
reproduced or copied in any form or by any means without
the prior written permission of the publisher. (1999-2024)

* All disputes are subject to the exclusive jurisdiction of
competent courts and forums in Delhi only.

CONTENTS

COVER STORY / 30pg



INFOTECH FORUM 2025: POWERING INDIA'S DIGITAL LEAP INTO THE FUTURE

REGULARS

Round About	10
Hot Bytes	12
On the Ramp	14
Voice N Data	16
Channel Buzz	18, 61
Cool Bytes	19
Movers & Shakers	62

CHANNEL GURU

8	TP-Link India: From a Hardware Vendor to a Trusted Digital Infrastructure Ally
---	--

FACE TO FACE

17	Boosting the Indian security industry with tailored solutions for diverse local needs
20	Securing The Future: Data Security In Hyperscale Ai-Ready Data Centers

LEAD STORY

22	Indian CIOs and CXOs: Navigating Disruption, Digital Acceleration, and Resilience
----	---

VAR SECURITY

21	CP PLUS Redefines National Security with India's Largest Range of STQC-Certified Surveillance Systems
61	Hikvision Powers Smarter, Sustainable Schools with Paperless Classrooms and Advanced Security Solutions

VAR SURVEY

28	THE GREAT SHAREPOINT BREACH: How Zero-Day Vulnerabilities Exposed Hundreds of Organizations Worldwide
----	---



Introducing PowerStore Prime

Get primed to deliver more
for you and your customers

Our completely new, integrated solution combines cutting-edge, all-flash storage advancements with valuable incentive programs so you compete with confidence and your customers can accelerate innovation.



More Efficiency

In today's business landscape, organizations need a solution that maximizes productivity while minimizing resource consumption



More Performance

With the rapid emergence of demanding AI workloads, performance and scalability are crucial competitive differentiators for organizations.



More Resiliency

The dynamic threat landscape means organizations require trusted infrastructure that's equipped to identify, prevent and recover from all sources of potential disruption.

The Future-Proof Advantage

Help your customers consume, scale and protect their storage investment their way to optimize IT lifecycles and focus on business outcomes.



GUARANTEES

- Three-year satisfaction
- 5:1 storage data reduction
- Cyber recovery
- Industry-best data protection deduplication



SOFTWARE

- Tech refresh and recycle
- Lifecycle Extension or ProSupport Plus
- Flexible payment solutions
- Never-worry data migration



MODERNIZE

- Dell APEX AI Ops
- All-inclusive software



IRIS GLOBAL

Please Contact

shivani.saini@irisglobal.in

Iris Global Services Pvt Ltd

1 Bypass Road, Mahipalpur, New Delhi, 110037

TP-Link India: From a Hardware Vendor to a Trusted Digital Infrastructure Ally

In the age of hyperconnectivity where digital infrastructure shapes how businesses function and how individuals live TP-Link India has emerged as one of India's most dependable and forward-thinking networking brands. Over the past decade, TP-Link India has steadily evolved from being known primarily as a consumer Wi-Fi brand to a comprehensive connectivity enabler.

TP-Link today caters to a wide spectrum of stakeholders - small businesses, co-working hubs, manufacturing clusters, educational institutions, and national ISPs. More than just connecting devices, TP-Link is actively enabling India's digital transformation with a unique blend of trust, scale, and local relevance.

"TP-Link's distinct advantage in the Indian ecosystem lies in its ability to seamlessly combine global R&D excellence with strong on-ground agility," states Bijoy Alaylo, COO & Director, TP-Link India. "As India progresses towards becoming a \$1 trillion digital economy, the need for resilient and secure networking infrastructure has moved far beyond metros. Tier 2 and Tier 3 cities are rapidly embracing digital transformation across sectors like education, retail, healthcare, and manufacturing. TP-Link's go-to-market strategy is purpose-built to address this shift—driven by a channel-first distribution model, strategic regional partnerships, and hyperlocal customization."

At the core of this outreach is TP-Link's multi-layered distribution model, which integrates direct sales teams, enterprise solution providers, system integrators, ISPs, and major e-commerce platforms. This hybrid approach ensures wide accessibility of its enterprise-grade solutions, while also supporting last-mile delivery, seamless onboarding, and dependable after-sales service. In many underserved regions, TP-Link has not just entered the market it has become a mainstay by offering proximity, performance, and presence.

A COMPREHENSIVE, FUTURE-READY PRODUCT PORTFOLIO

From a solutions standpoint, TP-Link's product portfolio is comprehensive and future-ready. Its flagship Omada SDN platform, a cloud-managed networking solution, is being adopted across educational

campuses, hospitality chains, warehouses, and healthcare facilities. The platform offers centralized control, advanced analytics, and high scalability meeting the needs of today's CIOs and IT heads.

Meanwhile, the AI-powered VIGI surveillance solutions are being used in smart campuses and industrial parks to deliver intelligent, real-time security. On the consumer and SOHO front, the Deco mesh system has emerged as a favorite, offering seamless plug-and-play connectivity tailored for hybrid work environments.

A ROBUST SUPPORT SYSTEM

A major, often underappreciated, strength of TP-Link India is its end-to-end support ecosystem. From pre-sales consultation and site assessments to post-deployment firmware updates and SLA-driven issue resolution, the company takes complete ownership of the customer journey. This full-lifecycle engagement is particularly beneficial for SMEs and educational institutions that often lack dedicated IT teams. Dedicated account managers ensure zero downtime for key accounts and are empowered to resolve escalations swiftly.

One of the company's most impactful initiatives has been the creation of a dedicated Key Account Management (KAM) team. These KAMs serve as single-point contacts for strategic clients, offering tailored deployment support and faster problem resolution.

"A notable example is a recent multi-campus deployment at an educational trust in South India. Following the rollout of Omada-based solutions across six locations, TP-Link implemented a 48-hour SLA model with both remote and on-site support. The result: a 30% increase in network reliability and a 25% reduction in support calls from faculty and students," explains Bijoy.

A STRONG CHANNEL BACK-UP

What makes TP-Link's channel model truly robust is its long-term investment in partner empowerment. The company conducts regular training, certification programs, and live demonstrations for its partners to ensure they stay ahead of the technology curve. It also provides co-branded marketing support, early product access, and performance-based incentives. This hands-on engagement has fostered deep trust within its partner network, resulting in high retention and consistent business growth.

TP-Link's close collaboration with ISPs has also emerged as a game-changer in regional markets. By offering custom firmware, competitive pricing, and expedited delivery cycles, the brand has helped small and mid-sized service providers scale more efficiently and deliver superior user experiences. This synergy is particularly critical in high-growth rural and semi-urban regions, where ISPs serve as vital enablers of last-mile connectivity.

KEY INFRASTRUCTURAL INVESTMENTS IN INDIA

Since the inception of business in India way back around a decade and a half, TP-Link has been steadily growing and has been continuously investing in infrastructure expansion. This has helped the brand immensely in terms of bringing in the right solutions and products for customers as well as helping the ubiquitous channel partners. These investments have been strategically carved to reach out the geographies which are the growth engines of the economy.

Aligning with India's national priorities, TP-Link's newly launched enterprise incubation and experience center in Mumbai is designed to support enterprise engagement, product testing, and regional solution customization.



BIJOY ALAYLO
COO & DIRECTOR
TP-LINK INDIA

Furthermore, the company is expanding its warehousing footprint and is actively exploring local assembly options to support the government’s ‘Make in India’ and ‘Atmanirbhar Bharat’ initiatives. These steps are not just operationally significant they signal TP-Link’s long-term commitment to India’s digital journey.

On the innovation front, TP-Link is already preparing for the next wave of networking. With Wi-Fi 7 on the horizon, the company is future-proofing its product line to support ultra-low latency, higher throughput, and seamless device management in high-density environments. Simultaneously, TP-Link is doubling down on cybersecurity by embedding multi-layered threat prevention and detection into its firmware and SDN architecture vital for data-sensitive sectors like BFSI, education, and healthcare. The brand is also exploring green networking solutions that enable enterprises to meet ESG goals through energy-efficient hardware and sustainable deployment practices.

GOING FORWARD

Going ahead, TP-Link India envisions itself not just as a hardware provider but as a strategic digital infrastructure partner.

“Our goal is to enable long-term digital resilience for Indian businesses, governments, and homes by offering integrated solutions that combine performance, simplicity, and value. In a fragmented networking ecosystem, TP-Link’s advantage lies in its unified approach: product innovation, consistent support, regional adaptability, and partner-led scale,” says Bijoy.

India is no longer just a promising market for TP-Link it is now central to its global growth and innovation roadmap. Whether it’s empowering a hospital in Tamil Nadu, supporting an ISP in Nagaland, or transforming a smart classroom in Pune, TP-Link is not just powering networks it’s powering India’s digital future.

“INDIA IS NO LONGER JUST A PROMISING MARKET FOR TP-LINK IT IS NOW CENTRAL TO ITS GLOBAL GROWTH AND INNOVATION ROADMAP. ITS GOAL IS TO ENABLE LONG-TERM DIGITAL RESILIENCE FOR INDIAN BUSINESSES, GOVERNMENTS, AND HOMES BY OFFERING INTEGRATED SOLUTIONS THAT COMBINE PERFORMANCE, SIMPLICITY, AND VALUE. IN A FRAGMENTED NETWORKING ECOSYSTEM, TP-LINK’S ADVANTAGE LIES IN ITS UNIFIED APPROACH: PRODUCT INNOVATION, CONSISTENT SUPPORT, REGIONAL ADAPTABILITY, AND PARTNER-LED SCALE.”

CAN WE PROVE ARNOLD TOYNBEE WRONG ON HIS PREDICTION OF CYCLICAL HISTORY?

Without ever realizing it, the world has completed a quarter of the 21st century. What was the most memorable event during the last twenty-five years? We started the century with a bang, realizing that a millennium was unfolding before us with its expectations, hopes, and anxieties. We celebrated the entry with a techie mindset by renaming it as 2K, the first time a year was named in a symbolic term. Many felt that it was a happy augury.

There were predictions about what the new century and millennium would unveil. Technocrats termed the unfolding of a new year, century, and millennium a turning point. It was widely believed that human ingenuity would traverse newer horizons, driven by the digital world of algorithms, unexplored innovations, and disruptions.

Every day, month, year, decade, century, and millennium has had its excitement, particularly at the embryonic stage or a little later. Sooner we realize that events more or less follow a statistical regularity. There will be events of all hues, good, bad, and ugly. Every timeframe is an approximation of linearity with some exceptions here and there. The time gone by has presented us with a mix of everything.

While digital leaps empowered us to communicate better and efficiently, we realized that the world was in the grip of a catastrophe when the pangs of Covid stared at us, snatching precious lives for no fault of ours. Millions lost their lives despite the medical breakthroughs that were boasted. That devastating period did not segregate people based on rich, or poor, advanced or primitive civilizations.

That was not the end of the tunnel. Before and after COVID-19, catastrophes took place at regular intervals, mainly from climate change, and the losses were more or less localized and were in the form of epidemics, floods, and droughts. Poor people living in continents like Africa, Asia, etc, bore the brunt of such developments. Despite these savory and unsavory developments, science continued to grow and flourish. Newer innovations, disruptions, and breakthroughs came at regular intervals.

What will be the next epoch-making breakthrough in the scientific world? Will it be in the digital world? Of course, there will be a string of discoveries and innovations in the digital space, and that will be mostly linear in nature, continuation, or logical extensions of the present technologies and equipment, which may not be as groundbreaking as it was in the case of the discovery of the internet.

Will there be any tectonic shift in medical science, such as ensuring longevity of life or strings of innovations that can address diseases like Parkinson's, Cancer, or a cure for diabetes or similar types of non-communicable diseases? Such medical breakthroughs happen at every point of time in history. Man has conquered many diseases over a period of time by finding a permanent or partial cure for such ailments. For instance, there have been considerable breakthroughs in the treatment of tuberculosis, cardiovascular diseases, and newer medicines and surgical interventions have been developed for such diseases with full or partial cure.

Yet, there are many ailments that are still engaging the attention of scientists and medical practitioners alike. Considerable research is being conducted in these areas to discern the basic reasons, and sooner or later, treatments for such ailments will become a reality with a fair degree of success. That is a continuous process. Mankind will conquer many diseases and ailments and will unravel the reasons for the occurrence of such diseases. It is nothing new; it is an ever-growing engagement and preoccupation. Perhaps, the only thing that may elude human ingenuity in the short and medium term is the prevention of ageing and consequent death. I do not know whether, in the long run, a solution may emerge for that, also.

Then, which is the area that can throw up surprises and excitement? I feel it is going to be in space science. A slew of



DR. ASOKE K. LAHA

Chairman-Emeritus and Founder, InterraIT

technologies and spacecraft will emerge in the coming years that can equip man to conquer space. Experiments are taking place in the most celebrated laboratories and research organizations to get more insights into space and unravel the dynamics of space and the mysteries of the universe. There are a good number of space scientists who believe that civilizations can be built in space, and another set of people believe that there are planets which can support life.

I am an ardent fan of the famous author and Historian Arnold J. Toynbee. He is best known for his 12-volume work, "A Study of History," which explores the rise and fall of civilizations and propounds a cyclical theory of history, suggesting that civilizations emerge, grow, and eventually decline in response to challenges and their ability to respond creatively. Importantly, another well-known author, D.C. Somervell abridged the monumental work of Toynbee. While reducing the work to one-sixth of its original size, he has succeeded in preserving its method and character.

Toynbee suggests that civilizations go through a life cycle: genesis, growth, breakdown, disintegration, and potentially a universal state before collapse. This pattern is not predetermined, and civilizations can potentially break the cycle through continued creative responses.

Toynbee's work is not without its critics. Yet, it offers a valuable framework for understanding the complexities of historical change and the factors that contribute to the rise and fall of civilizations. I agree with Toynbee on many points and disagree with him in equal measure in many places. This is not a piece to explain the points we agree and disagree. Yet, I must share that I am not as pessimistic as Toynbee was.

My major point of disagreement with Toynbee is when he claims history is optics, and civilizations, when they reach a certain stage, tend to create forces of their destruction. I feel the great historian has given a cautious path to tread to preempt such situations. People will have to think creatively and positively. What did he mean by that? To my understanding, he wanted mankind to keep the negative forces in check and maintain the balance of the planet. Disruptions to upset balance or block creativity will harm the human race. The result is acrimony, distrust, and war. All such misdeeds can destroy civilizations as it had done over millennia, when disruptive forces were generated from within. I wish our present crop of leaders do a soul search to avoid Toynbee's apocalyptic predictions and predilections.





TQ6702GEN2-R
Wi-Fi 6 AP
4.8Gbps Wi-Fi Performance
5Gbps Uplink Throughput
DPI Support



TQ7403-R
Wi-Fi 6E AP
4.2Gbps Wi-Fi Performance
5Gbps Uplink Throughput
DPI Support



x240-26GHXm
Multi-Gig PoE SW
24 x 1/2.5/5G Interfaces
280Gbps Throughput
PoE++ Support

Allied Telesis Wi-Fi Solutions

Next-Gen Speed, Zero Limits.

Allied Telesis wireless solutions provide security, reliability and unmatched roaming performance combined with lower running costs to meet the needs of modern digital organizations.

Your Wi-Fi and Connectivity issues are solved by the Allied Telesis Autonomous Wave Controller, empowered by AI.

- ✓ Optimized Channel and Radio Power Selection
- ✓ Automatic Interference Mitigation
- ✓ Self-Healing Wi-Fi Networks
- ✓ Improved Wi-Fi Performance

Learn more about AWC on our YouTube channel:



AWC
Autonomous
Wave Control



AWC-CB
Channel Blanket



CONTACT US

India's office:
B-417, Dattani Plaza, Opposite Telephone Exchange, Andheri Kurla Road,
Sakinaka, Andheri (E), Mumbai - 400 072
Tel: +91-080- 61480425



IBM launches Power11 server in India, built for AI-era enterprises

IBM has launched its most advanced Power server, IBM Power11, in India—engineered for real-time AI inferencing, hybrid cloud deployments, and resilient enterprise operations. Developed with major contributions from IBM's India Systems Development Lab (ISDL), Power11 is designed for mission-critical, data-intensive workloads in sectors like banking, telecom, healthcare, and government.

Power11 enables AI processing where data resides, ensuring compliance with India's data sovereignty laws. It will also support IBM's upcoming Spyre Accelerator for AI workloads, expected in Q4 2025. With 99.9999% uptime, near-zero planned maintenance, and sub-minute ransomware detection, it ensures business continuity.

The server delivers up to 2x performance per watt compared to x86 servers and offers a new Energy Efficient Mode for 28% better power efficiency. Equipped with NIST-approved quantum-safe cryptography and support for IBM's AI stack—including watsonx and Red Hat OpenShift AI—Power11 reflects India's growing role in designing secure, scalable, AI-first infrastructure.



Intel to spin off networking unit as part of strategic restructuring

Intel Corporation has announced plans to spin off its networking and communications division into a stand-alone company, aligning with new CEO Lip-Bu Tan's broader restructuring strategy. The move is aimed at streamlining operations, cutting costs, and sharpening Intel's focus on its core semiconductor business.

Intel has reportedly started identifying potential investors for the new entity, part of its effort to shed non-core assets and redirect resources toward high-growth areas like chip manufacturing, AI computing, and next-gen semiconductor technologies.

CEO Tan's roadmap includes scaling back investments, workforce reductions, and intensifying focus on innovation in semiconductor design and fabrication. Spinning off the networking unit—previously under the NEX segment—will allow Intel to prioritize data center chips, AI processors, and cutting-edge manufacturing. With this restructuring, Intel aims to become more agile and competitive in a rapidly evolving semiconductor market, dominated by rivals like AMD, NVIDIA, and TSMC.

Meta cracks down on predatory behaviour, removes 6 lakh accounts

Meta has taken down over 600,000 accounts from Instagram and Facebook as part of a major crackdown on predatory behaviour targeting minors. This enforcement action aims to enhance child safety across its platforms.

More than 135,000 accounts were removed for posting sexualized comments or soliciting explicit content, particularly targeting children or child-managed profiles. Another 500,000 accounts were flagged for inappropriate interactions, including links to previously identified exploitative content.

The move is part of Meta's broader commitment to digital safety, conducted in collaboration with the Tech Coalition's Lantern Program, which enables data sharing across platforms to prevent child abuse content from spreading. Meta is also investing in AI moderation tools, human review teams, and enhanced reporting systems. These measures support the company's wider goals of digital trust, user protection, and platform accountability, especially as children and teens increasingly engage with social media platforms.

Kaspersky uncovers 'GhostContainer' malware targeting Exchange servers in Asia

Kaspersky's Global Research and Analysis Team (GReAT) has discovered GhostContainer, a stealthy new backdoor malware targeting Microsoft Exchange servers in government and high-tech sectors across Asia. Uncovered during an incident response, GhostContainer appears to be part of a larger cyber-espionage campaign.

kaspersky

Built using multiple open-source components, the malware—detected as App_Web_Container_1.dll—is capable of modular downloads, granting attackers remote control for data theft, lateral movement, and proxy tunneling. It disguises itself as a legitimate server component and employs stealth techniques to avoid detection.

Sergey Lozhkin, Head of GReAT for APAC and META, highlighted the attackers' deep expertise and warned of a growing trend in malicious open-source use. Kaspersky urges organizations to adopt a multi-layered defence strategy, including real-time threat intelligence, EDR tools, and anti-targeted attack platforms. While the threat actor behind GhostContainer remains unidentified, its advanced design signals a serious risk to high-value institutional networks.

Draft telecom policy targets 100% 4G, 90% 5G coverage by 2030

The draft National Telecom Policy 2025 (NTP-25) outlines bold goals for India's digital future, including full 4G coverage, 90% 5G penetration, and the creation of one million jobs by 2030. The policy also proposes 80% fiberisation of telecom towers, 100 million fixed broadband connections, one million public Wi-Fi hotspots, and affordable access to smart devices for all.

Unveiled for public consultation, the policy introduces a new "Digital Bharat Nidhi" scheme to expand networks in underserved areas and accelerate fixed-line broadband through targeted incentives.

Described as a transformative roadmap, NTP-25 builds on the 2018 National Digital Communications Policy and aims to position telecommunications as a core driver of economic growth, social empowerment, and innovation. It also addresses future technologies like 6G, AI, IoT, satellite internet, and blockchain, with a strong focus on bridging the digital divide and establishing India as a global digital powerhouse.

24 apps and websites blocked for hosting obscene, vulgar content

The Ministry of Information and Broadcasting (MIB) has blocked 24 apps and websites for hosting obscene and vulgar content, directing all Internet Service Providers to disable public access. The action was taken in consultation with the Ministry of Home Affairs, Ministry of Women and Child Development, MeitY, Department of Legal Affairs, and experts in women's and child rights.

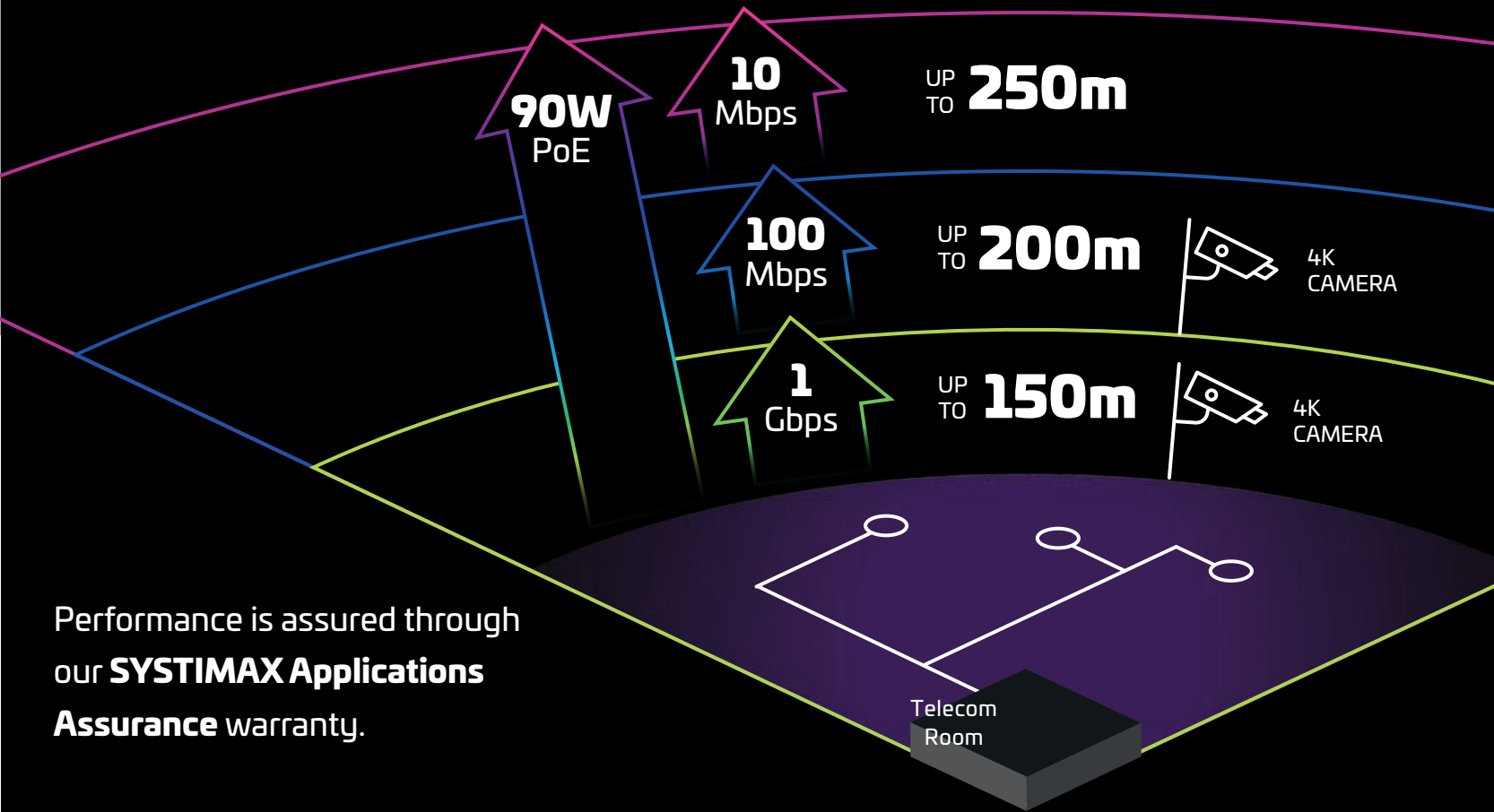
Platforms such as ULLU, ALTT, Desiflix, Gulab App, and others were found violating provisions under the IT Act, 2000 (Sections 67 and 67A), Section 294 of the Bharatiya Nyaya Sanhita, 2023, and the Indecent Representation of Women (Prohibition) Act, 1986.

The decision aims to curb the spread of unlawful digital content and uphold digital ethics. Shiv Sena (UBT) MP Priyanka Chaturvedi welcomed the move, stating she had raised concerns about such platforms in a parliamentary committee, and appreciated the government's long-awaited action.

GigaREACH™ XL

Extend your reach, not your risk.

GigaREACH XL, the first Cat 6, UTP solution to ensure support for 100 Mbps/90 W up to 200 m, 1 Gbps/90 W up to 150 meters and 10 Mbps/90 W up to 250 m.



Performance is assured through
our **SYSTIMAX Applications**
Assurance warranty.



Warrantied performance

- 100 Mbps—200 m—90 W PoE
- 1 Gbps—150 m—90 W PoE
- 10 Mbps—250 m—90 W PoE

Performance is warrantied, supported by
CommScope's **SYSTIMAX Assurance** and backed
by our **25-Year Extended Product Warranty**

Learn more



Fortinet announces quantum-safe security within its FortiOS

Fortinet has announced expanded innovations within its unified operating system, FortiOS, that protect against quantum-computing threats to current encryption standards. The latest FortiOS capabilities help organizations with highly sensitive data deploy encryption algorithms and key distribution methods that can withstand quantum-powered attacks, stack algorithms for more robust protection, and easily transition to post-quantum security.

“At Fortinet, we’re committed to arming customers with cutting-edge technology to protect against new and emerging threats. As quantum computing advances, organizations can trust Fortinet’s technology innovation and leadership to safeguard their critical data and future-proof their infrastructures. Many enterprises are eager to take action to protect their networks from quantum-powered threats. That’s why we’ve made cutting-edge, quantum-safe features available today for FortiGate NGFW and Fortinet Secure SD-WAN customers, so they can confidently transition to post-quantum security,” says Michael Xie, Founder, President, and Chief Technology Officer at Fortinet.

Acer announces AI-driven Predator Helios Neo 16 series in India

Acer has unveiled its latest additions to the Predator gaming portfolio — the Predator Helios Neo 16 AI and Helios Neo 16S AI in India — targeting gamers, creators, and professionals seeking next-gen performance with AI integration. These high-performance laptops promise a powerful blend of hardware, visuals, and cutting-edge features, built for both immersive gaming and serious productivity.



The Predator Helios Neo 16 AI delivers desktop-class power in a traditional chassis, while the Helios Neo 16S AI is the slimmest Predator ever, measuring under 18.9mm, catering to users who demand portability without compromising performance. Both the models are powered by up to Intel Core Ultra 9 processors and NVIDIA GeForce RTX 4070 Ti Laptop GPUs, enhanced with AI features enabled through integrated Neural Processing Units (NPUs). These systems intelligently manage workloads like image generation, audio optimization, and background blur, ensuring smooth multitasking and lag-free gaming. Support for NVIDIA DLSS 4, Ray Tracing (Gen 4), and Reflex 2 enhances gameplay with ultra-smooth, responsive graphics.

Tenable announces AI-powered evolution in Vulnerability Prioritisation

Tenable has announced the next evolution of its industry-leading Tenable Vulnerability Priority Rating (VPR) to sharpen precision and focus on risks that pose the greatest threat. Powered by generative AI, enriched threat intelligence and context-aware scoring, Tenable VPR enables organisations to quickly understand vulnerability impact, weaponisation and precise remediation actions.

With these latest AI-driven enhancements, Tenable VPR delivers twice the clarity and precision by leveraging real-time data to pinpoint the critical 1.6% of vulnerabilities that represent actual business risk. These efficiency gains, combined with enhanced explainability and contextualisation, translate to faster mean-time-to-remediation, optimised resources, and strategically aligned security efforts with organisational priorities. “We’re taking our game-changing Tenable VPR to the next level with these AI-powered enhancements,” said Eric Doerr, chief product officer, Tenable. “Tenable VPR brings an unmatched precision and depth of threat intelligence, context and explainability to cyber operations.”

Dell brings Alienware 16 Aurora to India

Dell Technologies and Alienware have introduced the Alienware 16 Aurora laptop in India, targeting gamers seeking both high performance and portability. The device will be available exclusively during Amazon Prime Day from July 12 to 14, 2025, with a starting price of ₹129,990. Broader availability will follow from July 17 through Dell’s official website, Dell Exclusive Stores, and select retail partners including Croma, Reliance Digital, and Vijay Sales.



The Alienware 16 Aurora is the first laptop in the brand’s Aurora lineup. It features the latest Intel Core (Series 2) processors and NVIDIA GeForce RTX 50 Series GPUs, equipped with NVIDIA’s Blackwell architecture and AI acceleration. The laptop is designed to support demanding AAA titles, backed by Alienware’s Cryo-tech thermal architecture for sustained performance. With up to 115W Total Performance Power and 85W GPU power, it supports PCIe Gen 4 SSDs and upgradeable DDR5 memory slots.

HP announces OmniBook 3 and 5 with in-built AI features

HP has announced the launch of its latest lineup of laptops, the HP OmniBook 3 and HP OmniBook 5. Both models come with integrated AI features for an improved computing experience. These features include Windows Studio Effects for video calls and HP AI Companion as well as Microsoft Copilot+ integration. The OmniBook 5 is powered by the Qualcomm Snapdragon X Plus X1-26-100 processor, while the 14-inch and 15-inch variants of the OmniBook 3 are powered by the AMD Ryzen AI 300 series.

OmniBook 5 offers a battery life of up to 34 hours on a single charge. The laptop is also equipped with HP Audio Boost 2.0, meaning low-pitch sounds during video calls will be amplified, hence guaranteeing a clearer video call experience. This model also boasts a 2K OLED display, ensuring an appealing picture quality and fast response time. Both the OmniBook 3 laptops come with the HP True Vision camera, a dual mic system, and noise reduction technology.

HMD announces T21 tablet in India at ₹14,499

HMD has officially launched its first tablet, the HMD T21, in India—an affordable, durable, and performance-driven device that blends power, design, and innovation. Available exclusively on HMD.com, the T21 is priced at ₹15,999

with a special launch offer of ₹14,499 for a limited time. Designed for work, entertainment, learning, and creativity, the HMD T21 boasts a 10.36” 2K display, OZO audio, and an 8200mAh battery, making it one of the most versatile tablets in its class. The T21 features a 10.36” 2K display with SGS low blue light certification, OZO audio, 8MP front and rear cameras, and support for active pen input.

“The T21 is a versatile, durable tablet built for today’s hybrid lifestyle. It reinforces our commitment to direct-to-consumer innovation and builds on the success of our exclusive launches on HMD.com,” said Ravi Kunwar, VP and CEO, HMD India & APAC.



micron™

Micron 9550 NVMe® SSD: The ideal storage for AI

Keep hungry GPUs fed with
lightning-fast performance



Best for

AI workload training and
highest performance with best
in class power efficiency

Speed

Up to 14,000MB/s

Capacity

Up to 30.72TB

Warranty

5-year limited

Key features

- AI workload performance and power efficiency with Big Accelerator Memory (BaM) using NVIDIA® technology.
- Delivers up to 33% faster workload completion times
- 60% faster feature aggregation performance
- 14.0 GB/s sequential reads and 10.0 GB/s sequential writes
- Supports NVMe 2.0 and OCP 2.0, with OCP 2.5 for telemetry data logging
- Designed for end-to-end security, it safeguards data with features like SED, SPDM 1.2, SEE, and encryption.

Contact us – expert talk

Mr. Sanjeeo Singh
Manager – Enterprise Sales
Contact: +91 8800507776

Celebrate Friendship Day with Snapchat and Rashmika Mandanna

Snapchat is celebrating Friendship Day 2025 in India with a special treat for users — a free ‘Streak Restore’ feature, available for the first time globally. From July 30 to August 3, Indian Snapchatters can restore up to five Snap Streaks at no cost, making it easier to revive lost streaks without using the regular in-app purchase option.



Commenting on the campaign, Saket Jha Saurabh, Director - Content and AR Partnerships at Snap Inc India, said, “Friendship is the foundation of Snapchat. Partnering with Rashmika Mandanna, who embodies authentic connection, makes this celebration even more meaningful.”

This initiative is part of Snapchat’s collaboration with popular Indian actor Rashmika Mandanna, who is also promoting her lifestyle brand ‘Dear Diary’ through this campaign. Snap Streaks, one of Snapchat’s most popular features, symbolize the consistency of communication between two users. Losing a streak can be disappointing for many, and this limited-time offer gives users a chance to reconnect with friends and bring back their streaks effortlessly.

Cities to appoint CISOs as India boosts cyber defences

As Indian cities rapidly digitize core public services, the Union Home Ministry has called for the appointment of Chief Information Security Officers (CISOs) across all urban local bodies to safeguard municipal digital infrastructure and citizen data from rising cyber threats.

The directive was issued during a recent high-level review meeting on cybersecurity preparedness, led by Union Home Secretary Govind Mohan. Citing the growing complexity of digital services under the Smart Cities Mission, Mohan stressed the need for internal cyber leadership rather than relying solely on external vendors. “Cities must develop their own cybersecurity muscle. CISOs will be the first responders in an era where digital systems are critical public assets,” he said.

By embedding cybersecurity leadership within city administrations, the government aims to build a digitally resilient urban ecosystem—one that can protect public trust in the nation’s smart governance efforts.

Centre Launches Nationwide Tests for Real-Time Mobile Disaster Alerts

The Government of India, in collaboration with the National Disaster Management Authority (NDMA) and the Department of Telecommunications (DoT), has launched nationwide tests for a real-time mobile disaster alert system. These tests are part of a broader initiative to enhance emergency preparedness and public safety through rapid, location-specific alerts delivered directly to citizens’ mobile devices. This initiative is in line with global best practices and mirrors systems used in countries like the United States (FEMA alerts) and Japan (J-Alert).



India’s new Cell Broadcast-based emergency alert system delivers real-time disaster warnings for earthquakes, floods, cyclones, and tsunamis, even on congested networks. Geo-targeted and available in multiple regional languages, it complements the SACHET system, which has sent over 6,899 crore SMS alerts in 19 languages across all 36 States and Union Territories, using the Common Alerting Protocol (CAP).

Airtel to offer free AI-powered search Pro subscription

Bharti Airtel has announced a strategic partnership with AI-powered search engine Perplexity, offering a complimentary 12-month Perplexity Pro subscription to its entire customer base of over 360 million users across mobile, broadband, and DTH services.



Perplexity is an advanced AI-driven search and answer engine that delivers accurate, real-time, and well-researched responses in natural language. Unlike traditional search engines that list web pages, Perplexity provides concise, readable answers that users can refine through follow-up queries using its self-learning capabilities. Globally, a Perplexity Pro annual subscription is priced at ₹17,000.

Through this collaboration, Airtel becomes the first Indian telecom provider to bring Perplexity Pro to its user base at no cost. Eligible Airtel customers can activate their free subscription by visiting the Airtel Thanks app. This initiative is part of Airtel’s broader strategy to enrich its digital offerings with cutting-edge AI tools, providing enhanced value and productivity to users.

Tata Communications & AWS to Build AI-Optimized Network for India

Tata Communications has teamed up with Amazon Web Services (AWS) to deploy an AI-ready long-distance network across India, connecting AWS infrastructure in Mumbai, Hyderabad, and Chennai. This high-capacity, ultra-low latency backbone will power generative AI and machine learning workloads, enabling faster data processing and scalability for enterprises.

Marking one of Tata Communications’ largest network deployments, the initiative will integrate AWS’s two cloud regions and edge infrastructure through a resilient national network, supporting India’s growing demand for AI-driven innovations. This collaboration underscores a shared vision of accelerating India’s digital transformation, offering businesses next-gen connectivity for building and training advanced AI applications.

By leveraging Tata Communications state-of-the-art network, AWS will further empower Indian businesses to develop Gen AI applications and train AI models, with unprecedented speed and efficiency. The network will feature express routes with ultra-low latency, helping ensure seamless data transfer and processing capabilities essential for compute-intensive AI and ML workloads.

WhatsApp to Introduce Profile Photo Import from Instagram or FB

Meta is working on a new WhatsApp update that will let users import their profile photos directly from Instagram or Facebook, making it easier to keep display pictures consistent across its platforms. According to WABetaInfo, this feature has been spotted in the WhatsApp beta for Android (version 2.25.21.23) and is already available to some beta testers, with a broader rollout expected soon.

Once live, users will be able to go to their profile settings, click on edit, and choose to import a profile photo from Instagram or Facebook. Currently, WhatsApp only allows changing profile pictures using the camera, gallery, avatars, or AI-generated images. This new cross-platform profile sync aligns with Meta’s strategy to integrate its ecosystem, offering users a more seamless and unified social media experience. By reducing repetitive updates and streamlining profile management, this feature enhances convenience for users actively engaged across Meta’s apps.

Boosting the Indian security industry with tailored solutions for diverse local needs

Ashish P. Dhakan, MD & CEO, Prama Hikvision India shares his vision for the Indian physical security market while also explaining the strategic approach that the company has identified to cater to different market segments with varied challenges and demands -

How important is the India market for Hikvision India's growth strategy, both from a global and an Indian perspective?

The Indian physical security systems market is one of the important markets for Hikvision India. From Hikvision India's perspective, it is one of the fastest growing markets across the categories. The physical market ecosystem has one of the largest share of MSME players as channel partners, dealers, distributors, system integrators, installers, consultants and end-users.

The market is expected to reach US \$10.9 billion by 2033, growing at a CAGR of 5.2% from 2025 to 2033, driven by increasing concerns over safety and security in various sectors. The market is highly price-sensitive, with customers seeking affordable solutions. The diverse customer base is another differentiation. The market caters to a diverse customer base, including government, enterprise, and residential customers. The regional variation of physical security system is quite to India market. The key differentiating factors include regulatory environment, regulatory frameworks, market dynamics, technological advancements, infrastructure, geography, Cultural, and social Factors. Some of the dominant factors are Government initiatives; Growing demand for surveillance and security solutions, Competitive landscape and a Price sensitive market.

These factors combined create a unique Indian surveillance and security market that requires tailored solutions, innovative approaches, and a deep understanding of local needs and challenges.

How are you catering to the needs of the Tier-II, Tier-III and Tier-IV cities, as these are the key markets from where the next phase of growth will be coming?

We are catering to Tier-II, III, and IV cities that require a strategic approach. We recognize the unique challenges and opportunities in each tier, such as limited infrastructure, growing demand for security solutions, and increasing urbanization. We identify key industries and sectors driving growth in these cities, like manufacturing, IT, and healthcare.

We develop customized security solutions that meet the specific needs of businesses and residents in these cities. We offer scalable and flexible solutions that can adapt to the growing demands of these markets. We

also provide training and capacity-building programs for local businesses, residents, and law enforcement agencies.

How is Hikvision India localizing its AI-powered security solutions to meet India's unique security challenges?

Hikvision is optimizing its products with AI technology to facilitate security and business intelligence innovations in several ways. As the adage goes 'every picture tells a story', we dig deep to get the video insights.

Some of the key security innovations are as follows -

- **Advanced Video Analytics:** Hikvision's advanced video analytics can detect and recognize objects, people, and vehicles, enabling advanced security features like intrusion detection, people counting, and facial recognition.
- **Intelligent Alarm Systems:** Advanced alarm systems can differentiate between real threats and false alarms, reducing unnecessary responses and improving response times.
- **Smart Search and Forensic Analysis:** Smart search capabilities enable quick and accurate forensic analysis, helping investigators to identify and track suspects.

Some of the Business Intelligence innovations are as follows:

- **People Counting and Heat Mapping:** The people counting and heat mapping enable businesses to optimize store layouts, improve customer experience, and increase sales.
- **Queue Management and Analysis:** The queue management systems help businesses to optimize staffing, reduce wait times, and improve customer satisfaction.
- **Business Intelligence Dashboards:** Business Intelligence dashboards provide businesses with real-time insights into customer behavior, sales trends, and operational efficiency.

Could you explain how Hikvision India is spearheading its growth in the India market by aligning its goals with the "Make in India" initiative?

Hikvision India is committed to the 'Make-in-India' vision with a long term perspective. Our state-of-the-art manufacturing facility at Vasai is a living testimony of a phenomenal progress. This facility has the state-of-the-art video security product manufacturing plant.



ASHISH P. DHAKAN
MD & CEO,
PRAMA HIKVISION INDIA

The video security products are customized for Indian environment and conditions and specific local requirements. Our mission is aligned with the government of India's 'Make-in-India' program to transform India into a global design and manufacturing hub. Through the local state-of-the-art manufacturing plant, Hikvision India is manufacturing its wide range of products and solutions. We are setting a gold standard for security product manufacturing in India, while continuously upgrading technology, expanding capabilities and creating new benchmarks.

Hikvision India has contributed immensely to the growth of the Indian security industry since its inception as a joint venture partner. It has developed a Pan-India channel network, branches and RMA service support centers. It has created a robust foundation for the future growth.

What's next for Hikvision India over the next 2-3 years?

Hikvision India is working closely with end-users to offer innovative solutions to India-centric security challenges. Addressing unique security concerns related to various local, regional and vertical specific issues. We are offering customized solutions through R&D initiatives.

Some of the key technologies used by Hikvision to address India-centric security challenges include -

- **Video Security Solutions:** providing high-resolution video feeds and real-time monitoring across verticals.
- **Video Analytics:** Using Video Analytics to detect unusual activities and sending instant alerts to security personnel.
- **Integrated Security Solutions:** Integrating various security components onto a single management platform.
- **Incident Reporting and Response via Mobile Applications:** Allowing staff to report incidents in real-time and facilitating quicker responses to unsafe practices or security breaches.

PCAIT concludes a Night of Recognition, Rhythm & Relationships

The Progressive Channels Association of Information Technology (PCAIT) set a new benchmark for industry engagement with its first-ever Partners' Choice Awards Musical Night, hosted at the serene Taj Damdama Resort on July 19. Combining business networking, celebration, and recognition, the event marked a unique moment for India's IT ecosystem, bringing together over 100 PCAIT members—including system integrators, OEMs, distributors, Make in India partners, and ISV partners—alongside their families.

The evening was graced by Ms. Yogita Singh, Vice President, Delhi BJP, and Chairman, Central Zone, MCD, as Guest of Honor, whose presence highlighted the importance of the event for industry leaders.

The day unfolded with networking sessions, icebreakers, and team-building activities, followed by "Soulful Strings," a live music hour, and a high-energy band performance that had attendees celebrating well into the night. PCAIT member Ranjan Chopra (Team Computers) captivated the audience with a special saxophone performance. Guests also enjoyed gourmet cuisine, cocktails, and candid conversations, creating valuable business connections.

The highlight of the evening was the inaugural Partners' Choice Awards, celebrating excellence across 19 categories, with winners chosen through votes from PCAIT members. Leading brands like HP, SentinelOne, Quick Heal, Zoho, TP-Link, Cisco, Dell, Canon, and Veeam were among the honorees, recognized for their exceptional product quality, support, and contribution to the IT channel community.

With rejuvenating surroundings, engaging performances, and authentic industry dialogue, PCAIT's first musical night has set the stage for future gatherings focused on collaboration, innovation, and growth for India's IT community.

Redington joins forces with NZXT to strengthen Red.Gaming portfolio

Redington Limited has announced a strategic partnership with NZXT, a globally renowned brand celebrated for its innovation and strong commitment to the gaming community. As part of the alliance, Redington will act as a non-exclusive distributor for NZXT, utilizing its expansive distribution network and strong go-to-market (GTM) capabilities to ensure the broad availability of NZXT's premium gaming components and peripherals across India.

Naqui Ahmad, Business Manager, South Asia, NZXT Inc., said, "India is one of the most dynamic and rapidly expanding PC gaming markets globally, fueled by a young, tech-savvy audience and a thriving community of creators and esports enthusiasts. We see this collaboration as a key driver in pushing the boundaries of gaming innovation and shaping the future of PC gaming in India."

NZXT aligns seamlessly with our vision for Red.Gaming — to serve as a catalyst in accelerating the growth of the gaming ecosystem in India. Through this partnership, we are thrilled to introduce NZXT's cutting-edge, high-performance gaming hardware and peripherals to India's rapidly expanding and highly engaged gaming community. NZXT already commands a strong cult following among Indian gamers, and with the country's digital infrastructure and economy accelerating, the brand is perfectly positioned for explosive growth," said Raghu Ram, Senior Vice-President, Redington Limited.

This partnership marks a significant milestone for Red.Gaming, Redington's dedicated initiative to empower the future of gaming. It will open new revenue streams within Redington's Lifestyle & Accessories portfolio, aligning with the company's broader ESG (Environmental, Social, and Governance) objectives by fostering innovation and accessibility in the gaming sector.

TP-Link Expands Footprint in Eastern India with New Office and Service Center in Kolkata

TP-Link India has announced a major expansion of its operations in Eastern India with the opening of a new service center and office in Kolkata. This strategic move aims to strengthen the company's regional presence and enhance customer support capabilities in West Bengal and the broader Eastern Indian market.

A subsidiary of TP-Link Systems Inc., USA, TP-Link India is a recognized leader in Wi-Fi routers and connectivity equipment. With the addition of this new facility, the company aims to streamline service delivery, boost operational efficiency, and consolidate its market leadership in networking solutions.

The newly inaugurated center in Kolkata will function as a central hub for business operations, technical support, and customer service across Eastern India. This expansion is part of TP-Link India's broader growth strategy to serve a growing customer base, which includes home users, small offices/home offices (SOHOs), and enterprise clients.

Mr. Bijoy Alaylo, Chief Operating Officer at TP-Link India, emphasized the importance of the expansion, stated, "This new facility reinforces our commitment to delivering faster service, deeper customer engagement, and seamless support across the region. It also underlines our broader vision of building smarter, more connected communities across the country."

TP-Link India has consistently focused on delivering end-to-end networking and security solutions that are not only reliable but also tailored to the needs of Indian consumers and businesses. From routers and range extenders to smart home products and enterprise-grade networking solutions, the company is continuing to evolve its offerings in line with India's growing digital infrastructure needs.

With the establishment of the Kolkata office and service center, TP-Link aims to enhance responsiveness, reduce turnaround times, and deepen market penetration in Eastern India. This move reflects the brand's commitment to delivering localized support and building long-term relationships with customers and channel partners across the region.



Iris Global Delivers helps STSPL successfully completes Federal Projects

Iris Global Services has successfully delivered ₹100 crore worth of Dell computing and APC power solutions for government and federal sector projects through its long-standing partner, Subha Technical Services (STSPL), based in Delhi.

The supply included high-end laptops, desktops, servers, and storage systems from global brands such as Dell, HP, and APC, fulfilling the growing demand for secure, scalable, and future-ready IT infrastructure in government, defense, and PSU institutions. A significant portion—40%—of the deployment was fulfilled via Dell and HP technologies, paired with advanced cloud and cybersecurity solutions. Iris Global also supplied APC power systems to support installations across multiple regions in India.

With increasing government investments in digital transformation and secure networks, Subha Tech has leveraged Iris Global's rapid response, product availability, and strong OEM partnerships to deliver robust, end-to-end IT solutions nationwide.

Founded in 2000, Subha Technical began as a SITC partner for Compaq and later HP. Its association with Iris Global began in 2014 and expanded in 2019 to include Dell. The company has now crossed Rs. 100 crore in revenue, driven by its focus on AI, machine learning, and federal engagements.

Oracle's Larry Ellison becomes world's second-richest amid AI boom

Larry Ellison, co-founder and CTO of Oracle, has climbed to the second spot on the Bloomberg Billionaires Index with a net worth of \$251.2 billion, surpassing Jeff Bezos and Mark Zuckerberg. Elon Musk remains the richest, with \$357.8 billion.

Ellison's rise is fuelled by Oracle's soaring stock, which has nearly tripled since late 2022, driven by global demand for AI infrastructure. Over the past three months alone, Oracle shares have jumped over 90%. A recent US policy easing semiconductor export restrictions to China further boosted tech stocks, with Oracle gaining 5.7% in a single day.

More than 80% of Ellison's wealth lies in Oracle stock and options. The company has secured major cloud contracts and is expanding its AI infrastructure, including its Stargate initiative with OpenAI and SoftBank. Ellison also announced a shift in his philanthropy focus toward the Ellison Institute of Technology, launched in 2023 with Oxford University.

Sam Altman warns financial industry of looming AI-driven fraud crisis

OpenAI CEO Sam Altman has raised serious concerns about the growing threat of AI-powered fraud in the financial sector, warning that artificial intelligence tools capable of mimicking human voices could soon render traditional security methods obsolete. Speaking at a Federal Reserve conference in Washington recently, Altman highlighted the vulnerability of voice-based authentication, calling it "crazy" that some institutions still rely on voiceprints for identity verification. "AI has fully defeated that," he cautioned.

Voice authentication became popular over a decade ago, particularly for high-net-worth clients who used it to access sensitive banking services. Customers were often required to speak a challenge phrase to verify their identity. However, with rapid advances in generative AI, voice and even video clones can now convincingly imitate real individuals, making older authentication systems increasingly unreliable. Federal Reserve Vice Chair for Supervision Michelle Bowman, who hosted the session, acknowledged the concern and expressed interest in collaborating on improved verification solutions.

Google removes 11,000 YouTube channels linked to China, Russia disinformation

Google has removed nearly 11,000 YouTube channels and related accounts in Q2 2025, targeting coordinated disinformation campaigns largely tied to China and Russia. Over 7,700 of these were traced to China, promoting pro-Beijing narratives and commenting on US policies in Chinese and English.

The campaigns often used trending hashtags, misleading titles, and AI-generated avatars to exploit YouTube's algorithm and appear authentic. Some content praised Chinese President Xi Jinping, aligning with state propaganda efforts. Google stated the removals are part of a broader strategy to safeguard its platforms from manipulation, especially ahead of major elections and geopolitical events. The company relies on machine learning and human review to detect coordinated inauthentic behaviour.

This crackdown underscores Big Tech's growing role in countering digital disinformation. With increasing regulatory scrutiny, Google reaffirmed its commitment to transparency and cooperation with governments and civil society to protect the online information space.

Amazon shuts down Shanghai AI lab amid rising geopolitical tensions

Amazon is closing its AI lab in Shanghai, aligning with a broader trend of US tech giants scaling back R&D in China due to rising geopolitical tensions. The lab, part of Amazon Web Services (AWS) since 2018, was instrumental in driving machine learning innovation and published over 100 research papers. It also developed a machine learning framework that generated nearly \$1 billion in sales.

Scientist Wang Minjie confirmed the closure via WeChat, citing "strategic adjustments." The move mirrors similar actions by Microsoft and IBM, who have also reduced their Chinese R&D footprints. Although Amazon hasn't disclosed job impacts, the lab played a key role in developing enterprise-grade AI solutions.

The shutdown reflects Amazon's global shift toward core priorities like cloud computing, generative AI, and enterprise services, amid growing US scrutiny of AI research links with China that could have national security implications.



US Defence turns to Amazon Kuiper for Golden Dome amid SpaceX concerns

Amid concerns over SpaceX's dominance, the Trump administration in the US is widening its search for partners to develop the Golden Dome missile defence system, exploring options like Amazon's Project Kuiper and major defence contractors. This strategic shift aims to reduce reliance on Elon Musk's company, despite SpaceX's strong track record with over 9,000 Starlink satellites launched and experience in government contracts.

While SpaceX remains a front-runner for key roles, especially launches, the Pentagon has approached Kuiper—despite it having launched only 78 of its planned 3,000 low-Earth orbit satellites. This reflects growing interest in integrating commercial space firms into US defence infrastructure.

Golden Dome is envisioned as a large-scale missile shield similar to Israel's Iron Dome, but with more layers and wider satellite coverage. A US official noted, "Kuiper is a big one," highlighting its potential role in building this complex national defence system.

Apple faces EU ruling over App Store changes amid DMA scrutiny

Apple is under European Commission scrutiny as it awaits a ruling on whether its updated App Store policies meet the EU's Digital Markets Act (DMA) requirements. To comply, Apple has reduced in-app transaction fees—now 20% for most developers and as low as 13% for small businesses.

In a major shift, Apple now allows developers to direct users to external payment systems, bypassing Apple's own billing. A new tiered fee structure applies, ranging from 5% to 15%, depending on the business size and payment method used. The company has also removed restrictions on external links, offering developers more freedom to promote alternative payment options.

As a designated "gatekeeper" under the DMA, Apple faces potential multi-billion-euro fines if found non-compliant. The EC's upcoming decision could reshape digital commerce rules across Europe, influencing how apps operate and monetize within the EU's tightly regulated tech ecosystem.

SECURING THE FUTURE: DATA SECURITY IN HYPERSCALE AI-READY DATA CENTERS

ROOPESH KUMAR
Head, Data Center Projects, Sify Infinit Spaces Ltd



As AI workloads grow, hyperscale data centers must scale in size, speed, and intelligence. Above all, their primary mission is to protect data, the lifeblood of modern enterprises, rich in value and risk. In this context, security is essential. Meeting today's threats and anticipating tomorrow's requires a security architecture that is intelligent, comprehensive, and proactive.

The Unique Security Challenges of Hyperscale AI Data Centers

The complexity and sheer scale of hyperscale AI-ready data centers create unique challenges, including:

- 1. Larger Footprint with Strong Network Connectivity**
Thousands of interconnected systems create a vast threat landscape, with each server, app, and endpoint posing a potential risk requiring constant defence.
- 2. Data Sovereignty Concerns**
AI workloads often cross borders, forcing hyperscale operators to navigate complex data protection laws like GDPR, CCPA, and India's DPDP Act—or face legal and reputational fallout.
- 3. AI-Specific Risks**
AI depends on large volumes of sensitive data—PII, financial, and proprietary information. Breaches can erode trust, skew algorithms, and compromise competitiveness.

Innovations in Real-Time Threat Detection

To navigate this evolving threat landscape, hyperscale data centers are adopting next-generation security models that prioritize speed, intelligence, and adaptability.

- AI-Driven Threat Monitoring**
Artificial Intelligence is now integral to real-time security. AI engines analyze billions of network traffic data points, identifying pattern deviations that may signify a breach or a zero-day exploit. This proactive monitoring significantly reduces time needed for detection and response.
- Behavioral Analytics**
Unlike traditional signature-based defenses, behavioral analytics systems continuously observe user and system behavior. Suspicious activity—such as irregular login times or unusual data transfers—is flagged and investigated automatically.
- Zero Trust Architecture**
In a Zero Trust model, every access request, whether internal or external, is verified, authenticated, and encrypted. This ensures tighter control over who accesses what, from where, and under which conditions.
- Predictive Analytics**
Historical data and threat intelligence, help AI models predict where vulnerabilities may emerge, enabling operators to implement preemptive controls rather than reactive fixes.
- Automated Response Systems**
In a breach, speed is vital. AI-powered systems can quickly isolate threats, shut down compromised endpoints, and contain the damage.
- Adaptive Defense Mechanisms**
Machine learning systems adapt to evolving threats, keeping defenses dynamic and responsive to sophisticated attacks.

Sify's 10-Tiered Physical and Electronic Security Framework

Sify's AI-ready hyperscale data centers follow a security-first approach, with strict control, monitoring, and auditing at every access point. Their 10-tiered framework combines physical security, intelligent surveillance, and digital governance for a secure-by-design ecosystem.

Layer 1: Premise Boundary Security

The outermost layer has a K8-rated perimeter wall built to resist vehicle intrusions, reinforced by:

- Vehicle Rejection Systems:** Capable of halting high-speed truck threats.
- Automatic Road Blockers:** Deployed in real time for immediate response to unauthorized vehicle entry.
- Under Vehicle Surveillance Systems (UVSS):** High-resolution scanning of vehicle undersides detects contraband or threats.
- Perimeter Intrusion Detection System (PIDS):** Real-time alerts for perimeter breaches, powered by vibration and motion detection sensors.

Layer 2: Guarded Perimeter Checkpoints

Trained security staff operate 24/7, aided by smart surveillance. Visitor access includes DFMD screening and ID checks at every entry point.

Layer 3: Baggage & Package Scanning

All carry-in items are X-ray scanned at the entrance to detect metals, explosives, or hidden electronics.

Layer 4: Personal Screening

Trained staff use Handheld Metal Detectors to frisk all visitors and staff, preventing entry of unauthorized items.

Layer 5: Full-Height Turnstile Access

With badge and biometric checks, this high-security entry blocks tailgating and piggybacking

Layer 6: Elevator Access Turnstile

Before elevators, individuals pass through half-height turnstiles with access controls, preventing forced entry and anti-passback breaches.

Layer 7: Floor-Specific Elevator Access Control

Elevators are programmed for role-based access, restricting movement to authorized floors and minimizing lateral risk.

Layer 8: Floor-Level Security

Each floor is guarded with controlled access doors, monitored by:

- Physical security personnel
- Handheld detectors
- Smart access logs, which track and timestamp every entry and exit

Layer 9: Server Hall Access

Dual-factor authentication (biometric + RFID) is required for server hall access, ensuring identity verification and traceable entry via centralized logs.

Layer 10: Server Cage Access Control

Tenant server cages use biometric locks and custom access rights, ensuring physical isolation essential for multi-tenant cloud security.

Integrated Digital Security and Surveillance Software

Beyond physical layers, Sify augments security with an advanced software layer:

- AI-Powered Video Analytics:** Real-time facial detection, license plate recognition, movement heat maps, and object tracking for proactive anomaly detection.
- Facial Recognition Systems:** Seamlessly integrated with access control to ensure that only enrolled personnel gain entry.

- **Integrated Visitor Management:** Digitally logs visitor credentials, entry/exit time, host mapping, and visitor zone limitations.
- **Real-Time Access Control Dashboards:** Unified dashboards offer real-time visibility into access logs, behavior patterns, and intrusion alerts.
- **Contactless Palm Readers:** Enable biometric authentication with no physical touch, enhancing hygiene and minimizing spoofing risks.

Sify's Differentiator: Intelligence-Driven Physical Security

Sify's AI-augmented security unifies cameras, access points, and controls into an intelligent command center. This ensures:

- Faster threat detection and response
- Granular access control down to the server rack level
- Seamless compliance with internal policies and external regulatory requirements

Sify's zero-incident record proves the strength of its multi-layered security, offering a trusted, assured infrastructure.

Ensuring Data Sovereignty and Compliance

Security is only one half of the trust equation. Compliance—especially in a global, AI-intensive context—is the other.

- **Localized Data Management**
Sify's infrastructure localizes data storage and processing, upholding sovereignty and regional privacy expectations.

- **Auditable Security Processes**
Every transaction, access attempt, and anomaly is logged, monitored, and available for audit—empowering enterprises to maintain compliance across standards and industry verticals.
- **Proactive Compliance Updates**
AI and real-time tracking keep our systems aligned with global regulations, ensuring timely compliance and reporting.

Sify's adherence to SOC 1 Type 2 and SOC 2 Type 2 certifications confirms its commitment to industry-recognized standards for security, availability, and confidentiality

Conclusion

In the AI-driven digital era, data is our most valuable asset—demanding more than firewalls. It needs intelligent orchestration, Zero Trust, and a partner like Sify to secure your future.

At Sify, we don't just host your data. We protect what it stands for.

Author:
Roopesh Kumar
Head, Data Center Projects
Sify Infinit Spaces Ltd



VAR SECURITY

CP PLUS Redefines National Security with India's Largest Range of STQC-Certified Surveillance Systems

CP PLUS is revolutionizing security with the largest portfolio of STQC-certified IP surveillance systems in the country. These next-generation systems go beyond traditional CCTV cameras, offering cyber-secured, tamper-resistant, and encrypted solutions designed to protect both physical spaces and critical data.

STQC certification, awarded by the Government of India's Standardisation Testing and Quality Certification Directorate, ensures these surveillance products meet rigorous standards for cybersecurity, encryption, and hardware reliability. This certification has become the gold standard for government, corporate, and smart city projects, positioning CP PLUS as a trusted partner in national security.

Built entirely in India at the company's state-of-the-art Kadapa facility, CP PLUS cameras integrate advanced safeguards like secure boot protocols, end-to-end encryption, trusted hardware components, and full compliance with cybersecurity norms. These features make them ideal for deployment across police stations, metro systems, safe city projects, airports, schools, toll plazas, and residential complexes.

As India pushes forward with Digital India, Smart Cities, and integrated governance initiatives, CP PLUS's STQC-certified solutions are vital in countering both physical and digital threats. By ensuring secure, hack-proof video feeds, CP PLUS addresses growing concerns around cyber intrusions in surveillance infrastructure.

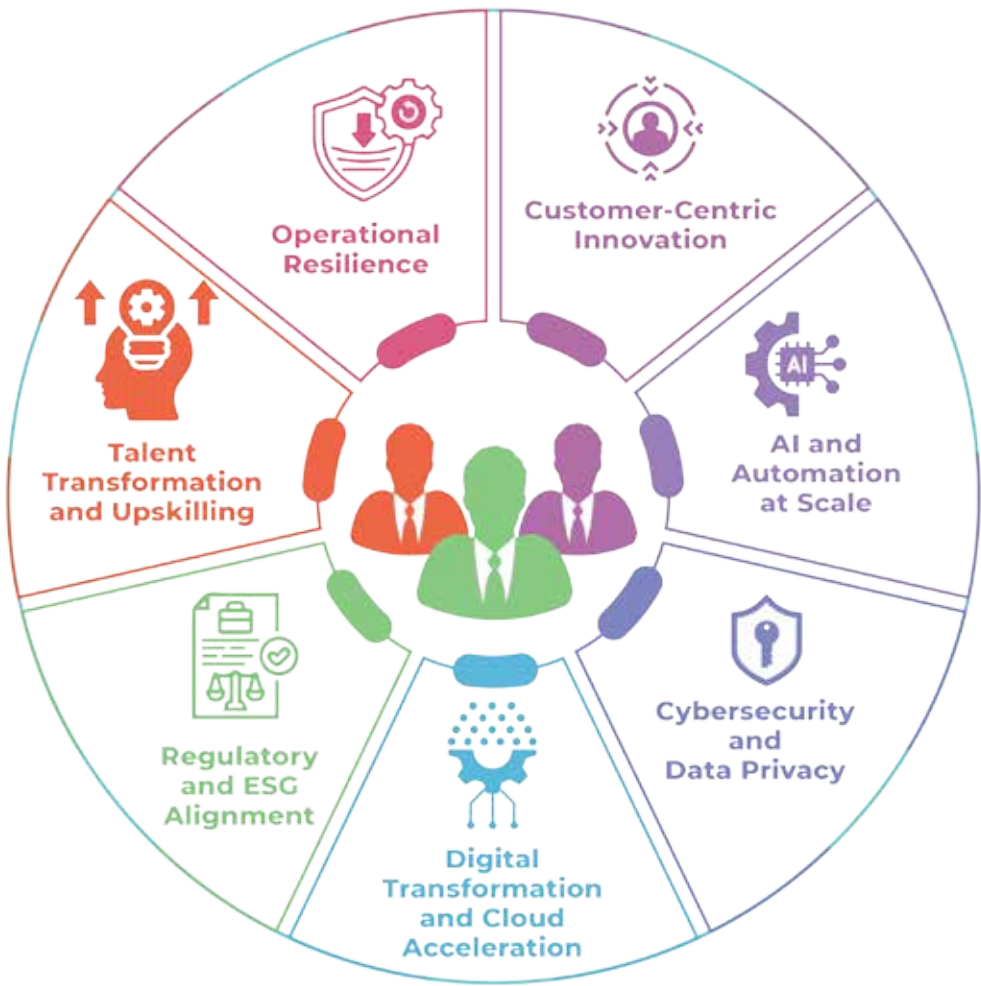
More than just a product portfolio, this initiative represents "Make in India" at its finest—creating indigenous, world-class surveillance solutions tailored for Indian conditions while aligning with global standards. In an era where data integrity and video evidence are critical, CP PLUS's cyber-fortified cameras are strengthening India's security backbone, ensuring that surveillance is not just about watching—it's about protecting with trust, innovation, and national pride.



Indian CIOs and CXOs:

Navigating Disruption, Digital Acceleration, and Resilience

In today's era of rapid digital transformation, escalating cybersecurity risks, and constant market disruption, CIOs and CXOs have evolved far beyond traditional technology oversight. They are now the driving force behind business growth, resilience, and customer trust. VARINDIA explores how these leaders are navigating the challenge of balancing speed, scale, and security — all while steering their organizations toward being future-ready and globally competitive.



India's rapidly evolving business landscape, driven by technological transformation, geopolitical uncertainty, and a hypercompetitive market, has redefined the priorities for Chief Information Officers (CIOs) and Chief Experience Officers (CXOs). The role of these leaders has shifted from traditional IT oversight and operational management to becoming core strategists and growth enablers. In today's environment, marked by economic headwinds, the rise of AI-driven innovation, stringent data privacy mandates, and a digital-first customer economy, the CIO and CXO agendas are no longer back-office priorities — they are boardroom imperatives shaping the future of Indian enterprises.

For CIOs, the mandate has expanded from managing IT infrastructure to becoming architects of digital transformation and business resilience. Indian organizations, whether large conglomerates or nimble startups, are embracing cloud-native architectures, edge computing, artificial intelligence (AI), and automation to drive efficiency and competitive differentiation. Yet, these opportunities come with rising

risks — cybersecurity breaches, ransomware attacks, and regulatory complexities are at unprecedented levels. As a result, strengthening cyber resilience, enabling hybrid and remote work securely, and building scalable, agile IT ecosystems have emerged as non-negotiable priorities.

For CXOs, the focus is equally multifaceted. India's consumer market is experiencing exponential digital adoption, with over 800 million internet users and a surge in mobile-first commerce. This puts customer experience (CX) and digital engagement at the center of competitive strategy. CXOs are under pressure to design frictionless, omnichannel experiences, powered by data insights, personalization engines, and AI-driven predictive analytics. Moreover, they must ensure business sustainability, balancing profitability with environmental, social, and governance (ESG) commitments, which are becoming key metrics for investors and regulators alike.

Amid this transformation, several themes dominate the Indian CIO/CXO agenda:

- Digital Transformation and Cloud Acceleration** – Migrating to hybrid and multi-cloud infrastructures to scale operations, enhance speed to market, and improve cost efficiencies.
- Cybersecurity and Data Privacy** – Adopting Zero Trust frameworks, strengthening endpoint defenses, and ensuring compliance with India's Digital Personal Data Protection Act (DPDPA).
- AI and Automation at Scale** – Harnessing generative AI, robotic process automation (RPA), and machine learning (ML) to drive smarter decisions, reduce costs, and accelerate innovation.
- Customer-Centric Innovation** – Using real-time analytics to power personalized, immersive customer journeys across industries, from BFSI to e-commerce.
- Operational Resilience** – Designing systems and supply chains that withstand disruption, whether from cyberattacks, natural disasters, or geopolitical shifts.

Talent Transformation and Upskilling
– Preparing the workforce for a digital-first economy through AI literacy, cybersecurity skills, and cloud certifications.

Regulatory and ESG Alignment
– Navigating overlapping compliance mandates while embedding sustainability and governance into business strategy.

INDIAN ENTERPRISES

For India’s enterprises, the stakes are enormous. Digital transformation alone is expected to contribute over \$150

billion to India’s GDP by 2030, according to NASSCOM. However, only those organizations that successfully balance innovation with resilience will capture this value. CIOs and CXOs must therefore collaborate closely, not only to deploy technology, but to deliver trust, elevate customer experience, and drive measurable ROI.

At the core of these agendas lies one defining principle: resilience. The future of business in India will not be shaped by avoiding disruption, but by leveraging it

as a catalyst for growth. The leaders who thrive will be those who embrace AI, cloud, and automation; fortify cybersecurity; align with ESG imperatives; and empower their workforce — all while fostering agility in the face of uncertainty.

For CIOs and CXOs in India, the challenge is no longer whether to transform — it is how quickly and effectively they can act to build organizations that are innovative, trusted, and future-ready. Below are the inputs from industry’s eminent CIOs..

Building a Culture of Vigilance with Security Everyone’s Job

ARCHIE JACKSON
VP - CIO & CISO, INCEDO INC.

In 2025, India’s CXOs and CTOs are transforming businesses into resilient, AI-powered enterprises rather than just managing technology. Artificial Intelligence and Machine Learning now drive efficiency, automating operations, enabling predictive analytics, and boosting decision-making. Agentic AI — autonomous systems executing complex tasks — is enhancing workforce productivity, while edge computing and quantum innovations are revolutionizing real-time data processing for industries like logistics, retail, and financial services.

With cyber threats growing more sophisticated, security has become a core business priority. AI-driven threat detection, automated response, behavioral analytics, and Zero-Trust frameworks — where every user and device is continuously verified — are now essential to protect hybrid environments.

CXOs are championing enterprise-wide security awareness through gamified training, real-time simulations, and department-wide security champions, ensuring data protection is a shared responsibility.



Redefining Success with Speed, Trust & Intelligence!

DR. ARINDAM SARKAR
HOD & ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ELECTRONICS, RAMAKRISHNA MISSION VIDYAMANDIRA, BELUR MATH

In 2025, India’s CXOs and CTOs are steering enterprises beyond IT management to drive strategy, innovation, and resilience. Their priorities center on emerging technologies like AI, which has become a core decision-maker, powering predictive analytics, automation, and personalized customer engagement, while ethical AI governance ensures responsible innovation.

Quantum computing is edging toward real-world applications in cybersecurity and finance, and edge computing is accelerating logistics and manufacturing with localized, real-time processing. Cybersecurity is now a boardroom focus, with Zero-Trust frameworks, AI-driven threat detection, behavioral analytics, and automated responses protecting organizations proactively.

Companies are embedding security-first cultures through gamified training, awareness programs, and performance-linked KPIs, making employees “human firewalls.” CIOs, CTOs, CISOs, and DPOs collaborate via “Digital Trust Councils” to align innovation, compliance, and ESG goals, creating agile, future-ready enterprises.



Reinforcing Cybersecurity as a Core Business Imperative

ASHISH GUPTA
CIO & CISO, NEC CORPORATION INDIA

In 2025, Indian CTOs and CXOs are steering enterprises through a fast-evolving digital era, where technology drives competitiveness, customer trust, and sustainable growth. Artificial Intelligence (AI) and Machine Learning (ML) have moved from trials to core adoption, powering smarter decision-making, automating operations, and elevating customer experiences. Cloud-native and composable enterprise models are enhancing agility, enabling rapid adaptation in dynamic markets.

With cyber threats and stringent data regulations like the Digital Personal Data Protection Act (DPDPA) rising, Zero-Trust architectures, AI-driven threat detection, and identity-centric controls are now central to IT strategies. Cybersecurity is no longer confined to IT; gamified training and awareness programs make security a company-wide responsibility. CIOs, CTOs, CISOs, and DPOs are aligning on innovation, compliance, and resilience, ensuring enterprises remain secure, agile, and future-ready.



Ensuring agility & security while embracing tech-driven growth

FARMAN KHALID
HEAD – IT/ CHIEF DIGITAL OFFICER, EMAAR INDIA



In 2025, India’s CIOs have evolved from IT managers into strategic growth architects, driving enterprise transformation. Their core focus is aligning every technology initiative—whether Agentic AI, Generative AI, or automation—with business growth and operational efficiency. By integrating AI, automation, and flexible consumption-based models, CIOs are enabling agility while optimizing costs.

With the demand for data and cybersecurity skills rising, CIOs are also champions of workforce upskilling, ensuring businesses thrive in a data-driven world. Security remains critical, as they embed zero-trust frameworks, AI-powered threat detection, and behavioral analytics to defend against cyber risks.

Beyond IT, CIOs are boardroom influencers, shaping strategy, monetizing data, and steering change management, making technology a cornerstone of competitiveness and sustainable growth.

Indian CTOs: Driving Digital Transformation at Scale

GOLOK KUMAR SIMLI
CTO, PASSPORT SEVA PROGRAMME, MINISTRY OF EXTERNAL AFFAIRS, GOI



In the post-COVID era, technology has reshaped how services are delivered and accessed, transitioning from face-to-face interactions to seamless, mobile, and remote experiences for everything from government services to retail. For Indian CTOs, the top priority is enabling secure, resilient, and mobile workspaces, ensuring services and workloads remain accessible anytime, anywhere without compromising cybersecurity or performance.

Data governance is now central to digital leadership, with DPDP laws driving CTOs to ask critical questions about data collection, purpose, and protection. Building trust through transparent governance, strong frameworks, and advanced technologies is as crucial as driving innovation. Given India’s massive scale—1.45 billion people across diverse conditions—CTOs must harness AI, partnerships, and scalable ecosystems to deliver inclusive, transformative solutions that simplify access and ensure no citizen is left behind.

AI at the Core of Indian CTOs’ Agenda

J. P. DWIVEDI
CIO, RAJIV GANDHI CANCER INSTITUTE & RESEARCH CENTRE, ROHINI



In 2025, India’s technology leadership is being redefined as AI becomes the foundation of enterprise transformation. Generative AI, Machine Learning, Robotic Process Automation, and advanced analytics are no longer optional tools—they’re essential drivers of efficiency, innovation, and competitive advantage.

For CTOs, the focus is on creating robust, scalable, and secure technology ecosystems to power this AI-driven shift. While CIOs are evolving into strategic business enablers, CTOs are tasked with building the resilient digital backbone that scales seamlessly while ensuring security and reliability.

Equally vital is cultivating a security-first culture. As threat vectors grow, structured awareness programs, refresher training, and frameworks like ISO 27001 help mitigate risks. CTOs now shape the core technology and security strategies that fuel agility, growth, and resilience.

Indian CTOs, Scaling Smarter with AI, Cloud, and Cyber Resilience

KRIPADYUTI SARKAR
CIO, AMBUJANEOTIA



In 2025, Indian CTOs face unprecedented expectations as they steer enterprises through a rapidly evolving digital era. GenAI-driven automation, ERP and CRM integration, edge computing, IoT expansion, and secure, modern networks are reshaping operations. Cloud-native and hybrid infrastructures now form the backbone of scalability, flexibility, and cost efficiency, while sustainability—from energy-efficient data centers to carbon tracking—is a growing mandate.

Security remains paramount, with Zero-Trust Architecture, continuous authentication, behavioral biometrics, and SIEM/SOAR frameworks at the core. AI and automation power predictive analytics, threat hunting, and patch management, driving efficiency while demanding rigorous governance to prevent data leaks, especially with public AI tools. CTOs are also embedding security-first cultures through leadership-driven training and real-time awareness, ensuring Indian enterprises stay resilient, sustainable, and globally competitive.

Accelerating Digital Transformation and AI Adoption



NITIN DHINGRA
CHIEF TECHNOLOGY OFFICER, INDIRA IVF HOSPITAL LTD.

In 2025, Indian CXOs and CTOs are steering enterprises through a fast-changing digital landscape where technology drives growth, efficiency, and resilience. Their strategies center around four priorities. Artificial Intelligence (AI) and Machine Learning (ML) are now core to decision-making, workflow automation, and actionable insights, powering competitiveness across sectors from customer engagement to healthcare and operations.

To combat escalating cyber threats, enterprises are adopting Zero-Trust architectures with continuous user verification, strict access controls, AI-driven threat detection, and robust cloud security. Building a security-first culture is also key, with ongoing employee training, phishing simulations, and real-time risk assessments to reduce vulnerabilities and meet compliance standards. Meanwhile, CIOs, CTOs, CISOs, and DPOs are converging roles, working together to balance innovation, speed, security, and regulatory adherence.

Today's CTOs are Pioneering India's Tech Evolution



PANKAJ MITTAL
FOUNDER & CEO, DIGIZEN CONSULTING

Today, Indian CTOs are at the forefront of a transformative technology wave, driving innovation, security, and sustainability. AI and Machine Learning dominate enterprise strategies, with Generative AI automating content creation, AI-powered coding assistants enhancing productivity, and Explainable AI (XAI) ensuring ethical, transparent decision-making. Beyond AI, CTOs are embracing quantum computing, edge computing powered by 5G and 6G, and hybrid cloud-native infrastructures to deliver scalable, agile, and immersive customer experiences.

Cybersecurity remains a core priority, with Zero-Trust frameworks, AI-driven threat detection, and post-quantum cryptography becoming essential to counter escalating cyber risks. Sustainability is equally crucial, as energy-efficient data centers, green cloud solutions, and AI-enabled carbon tracking integrate into business strategies. CTOs now act as ecosystem architects, leveraging blockchain, autonomous systems, and XR/metaverse tools while collaborating with CIOs, CISOs, and DPOs to balance innovation, compliance, and resilience.

Harnessing Emerging Technologies is a top priority for CTOs



PRADIPTA PATRO
HEAD CYBER SECURITY AND IT, KEC INTERNATIONAL LIMITED (AN RPG GROUP COMPANY)

Indian CTOs are driving transformation by integrating disruptive technologies to boost efficiency, innovation, and resilience. Artificial Intelligence (AI) and Machine Learning (ML) are central, enabling predictive analytics, real-time insights, and personalized customer experiences through automation, chatbots, and virtual assistants.

IoT is powering smart manufacturing and real-time supply chain management, with connected sensors monitoring operations, predicting maintenance, and optimizing logistics. Edge computing complements these innovations by processing data at its source, ensuring low latency, security, and instant analytics for applications like smart cities and autonomous systems.

With 5G delivering ultra-fast connectivity, AR/VR collaboration and new business models are accelerating. Blockchain is adding trust with secure, transparent transactions and tamper-proof supply chains, helping CTOs build scalable, future-ready enterprises.

CTOs Reinventing the Enterprise



PRASENJIT MUKHERJEE
AVP (HEAD IT & DIGITAL), JWIL INFRASTRUCTURE LTD.

The role of the CTO has evolved from IT oversight to strategic business leadership. Today's CTOs are tasked with driving growth, agility, and resilience while ensuring seamless digital experiences. Technology is no longer a support function—it's the foundation of business operations. As digital transformation accelerates, cybersecurity has become a critical priority. CTOs are embedding a security-first culture through structured frameworks, regular audits, and employee training, making cyber hygiene a shared responsibility.

AI, automation, and zero-trust architectures are also central to enterprise IT strategies. While automation drives efficiency, CTOs must ensure secure integration, clear IT/OT separation, and data governance—especially when using public AI tools. As businesses aim to scale with leaner operations, future-ready CTOs will lead innovation, aligning tech with business outcomes for sustainable growth.

The Future-Ready CIO: Key Priorities Shaping Enterprise IT in 2025

RAMKUMAR MOHAN
SENIOR VP & CIO, AIR WORKS INDIA ENGINEERING PVT. LTD.



CIOs have evolved from IT managers to strategic growth enablers, driving innovation, resilience, and compliance across enterprises. Their top priority is digital transformation, leveraging AI, automation, and intelligent systems to streamline operations, enhance decision-making, and deliver personalized customer experiences. Cloud-native and edge architectures now power scalable, agile business models.

Amid escalating cyber threats, CIOs are embedding zero-trust frameworks, AI-driven threat detection, behavioral analytics, and automated incident response into enterprise strategies. Building a security-first culture through continuous employee training, phishing simulations, and strict access controls remains vital to address human vulnerabilities.

With India's DPDP Act in force, data governance is central, balancing innovation with regulatory compliance. CIOs now collaborate closely with CTOs, CISOs, and DPOs, creating future-ready, compliant enterprises built to thrive in a digital-first economy.

CTOs Brace for AI-Driven Cyber Onslaught in 2025

DR. RAKSHIT TANDON
CYBER SECURITY EVANGELIST



With cybercrime surging by 900% in four years, Indian enterprises face an unprecedented security crisis in 2025. Ransomware, AI-powered phishing, deepfakes, and advanced malware are exploiting weaknesses, while Generative AI, though transformative, is also helping hackers craft sophisticated attacks, even targeting AI algorithms to spread misinformation and erode trust.

For CTOs, reactive defenses no longer suffice. Security must be embedded by design, integrating protection into every product and service from inception. With India's DPDP Act imposing penalties up to ₹250 crore, compliance, continuous testing, and proactive audits are critical.

CTOs must also counter supply chain compromises and trusted contact attacks, deploying Security Operations Centers (SOCs), Data Loss Prevention (DLP), and regular penetration testing as essentials. Vigilance, AI-driven defenses, and strong governance will define resilient enterprises in 2025.

CTO prioritizes, driving enterprise transformation!

RAVI RAZDAN
DIRECTOR – IT & HR, JYOTHY LABS



In 2025, Indian CTOs face a landscape shaped by Generative AI, Industry 4.0 and 5.0, and Spatial Computing, all driving automation, smart systems, and immersive applications in sectors like manufacturing, real estate, and workforce training. Cybersecurity has become a central priority, with IT and OT threat intelligence converging to protect increasingly connected enterprises.

CTOs and CIOs must shift from technology custodians to strategic partners, using predictive systems for trend forecasting while selectively adopting emerging technologies based on organizational readiness. A security-first culture is critical, built on awareness, ongoing training, strong cyber hygiene, VAPT testing, and secure platform deployment.

To safeguard AI-driven operations, CTOs are championing Zero-Trust Network Access, AI-based threat detection, SOAR systems, and endpoint protections, while collaborating with CISOs and DPOs to ensure compliance with the DPDP Act.

CTOs Driving AI, Automation, and Zero Trust for Enterprise Security

SAURABH GUGNANI
GLOBAL HEAD OF CYBERSECURITY ENGINEERING, PROJECTS AND ARCHITECTURE, TMF GROUP



In 2025, CTOs are leading enterprises through a volatile cyber landscape with a three-pronged defense strategy built on AI-driven security, automated response via SOAR/XDR, and Zero Trust frameworks.

AI-powered threat detection is now central, with machine learning analyzing user, device, and AI agent behavior to flag anomalies like unusual logins or excessive data transfers. These systems predict threats such as phishing or lateral attacks while triggering just-in-time authentication and automated lockdowns.

SOAR and XDR platforms accelerate response by correlating data across endpoints, networks, and cloud systems, instantly isolating compromised assets and executing playbooks.

Zero Trust architectures further strengthen defenses through micro-segmentation, least-privilege access, and continuous verification, ensuring resilient, real-time protection across human, machine, and IoT ecosystems.

AI is now both shield and sword for CTOs

DR. SUBROTO KUMAR PANDA
CIO & CTO, ANAND AND ANAND

Indian enterprises must evolve beyond hype, embedding emerging technologies into secure, sustainable, and adaptive ecosystems. Generative AI has revolutionized automation and innovation, but Agentic AI—autonomous agents driving workflows and decisions—is the next frontier, demanding vigilant oversight for reliability and ethics. AI for Governance and Compliance is becoming indispensable, automating regulatory processes and minimizing human error in increasingly virtual operations.

Cybersecurity is now the ultimate battleground, with AI acting as both defense and weapon. Adversaries use it for deepfakes, malware, and algorithmic exploits, forcing organizations to adopt Zero Trust frameworks, AI-driven threat detection, and unified defense strategies.

Alongside this, cloud-native and multi-cloud architectures, sustainable computing, 5G, and immersive XR are reshaping enterprises. CTOs must balance speed, security, and compliance, creating digital ecosystems built to thrive.



CTO's Agenda is all about AI and Cybersecurity

VIJAY SETHI
CHAIRMAN, MENTORKART AND CRAFTSOL TECHNOLOGIES

CIOs and CTOs are pivotal to enterprise transformation, evolving from IT managers to strategic growth enablers. Artificial Intelligence leads this shift, advancing beyond automation to power predictive analytics, hyper-personalized engagement, and operational efficiency across sales, HR, finance, and production. Generative AI and Agentic AI—autonomous agents handling workflows—are reshaping processes, analytics, and content creation, making technology central to decision-making.

However, AI also heightens cyber risks, with threats like model poisoning, AI-driven attacks, and sensitive data leaks via generative tools. Cybersecurity must be embedded into organizational DNA, combining zero-trust frameworks with a culture of awareness and accountability where employees act as “human firewalls.” Beyond AI, leaders must drive IoT, RPA, and data-driven ecosystems, integrating technology seamlessly into core business strategies.



AI, Hyperautomation and Cyber Resilience to Drive Enterprise Growth

VINOD KUMAR GUPTA
CISO & DATA PROTECTION OFFICER, PAYTM MONEY

Indian CTOs are evolving into strategic leaders, driving enterprise growth, resilience, and innovation beyond traditional IT management. Artificial Intelligence and Generative AI now anchor this transformation, powering predictive analytics, automation, and personalized customer engagement while enhancing decision-making and operational agility.

CTOs are advancing Edge Computing and IoT to enable real-time insights across manufacturing, logistics, and healthcare, while early quantum computing pilots explore cryptography and optimization. Hyperautomation, blending RPA, AI, and low-code platforms, has become essential for streamlining processes and boosting efficiency.

Cybersecurity is now a board-level priority, with Zero-Trust frameworks, AI-powered threat detection, and behavioral analytics at the core. Continuous employee training, phishing simulations, and cyber drills strengthen “human firewall” cultures, as CIOs, CTOs, CISOs, and DPOs unite to ensure secure, agile, and future-ready enterprises.



CTOs in 2025: Driving AI, Security, and Innovation at Scale

YOGENDRA SINGH
HEAD - IT & SAP, BARISTA

Indian CTOs in 2025 are reshaping enterprises around five key priorities. Generative and Predictive AI have shifted from trials to strategic assets, driving decision-making, automation, hyper-personalization, and content creation across finance, HR, and supply chains. Hyperautomation, integrating AI, RPA, and process mining, is streamlining operations, reducing costs, and minimizing human reliance.

Cybersecurity is critical, with AI-driven threat detection, behavioral analytics, and Zero-Trust frameworks delivering adaptive, real-time protection. Organizations are embedding a security-first culture using gamified training, phishing drills, and targeted programs, making employees active “human firewalls.”

Edge computing and IoT are powering real-time insights in logistics, healthcare, and manufacturing, while ethical AI, bias audits, and transparent governance ensure compliance as GDPR and India’s DPDP Act reshape data practices.



THE GREAT SHAREPOINT BREACH:

How Zero-Day Vulnerabilities Exposed Hundreds of Organizations Worldwide

Nation-state actors and ransomware groups exploit critical flaws in Microsoft's enterprise collaboration platform, triggering an urgent modernization imperative

The cybersecurity world was jolted awake in late July 2025 when researchers at Eye Security discovered something alarming: a sophisticated campaign targeting Microsoft SharePoint servers had been quietly compromising organizations worldwide. What started as routine threat hunting quickly revealed one of the most significant zero-day exploitation campaigns of the year, affecting hundreds of companies, government agencies, and critical infrastructure operators across the globe.

At the heart of this digital siege was CVE-2025-53770, a critical vulnerability with a maximum CVSS score of 9.8 that allowed attackers to execute code remotely on vulnerable SharePoint servers without any authentication. But this wasn't just another security flaw—it was a devastating bypass of patches Microsoft had released just weeks earlier, demonstrating how quickly threat actors can adapt their tactics to stay ahead of defensive measures.

THE SCOPE OF DEVASTATION

The numbers paint a sobering picture of the attack's reach. Eye Security tracked more than 75 breaches, including compromises at US federal and state agencies, energy companies, universities, and an Asian telecommunications provider. Reports indicate hundreds of organizations were ultimately affected, with victims spanning from European government agencies to a state legislature in the eastern United States.

The breach campaign caught the attention of the highest levels of US cybersecurity leadership. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) was made aware of the exploitation by a trusted partner and immediately reached out to Microsoft to take action, according to Acting Executive Assistant Director for Cybersecurity Chris Butera. The urgency was evident when CISA added CVE-2025-53770 to its Known Exploited Vulnerabilities (KEV) catalog on July 20, 2025, signaling immediate risk to critical infrastructure.

THE TECHNICAL ANATOMY OF TOOLSHALL 2.0

The attack campaign, dubbed "ToolShell," represents a sophisticated evolution of exploitation techniques that security researchers first observed at the Pwn2Own hacking competition in Berlin in May 2025. CVE-2025-53770 is a bypass of the fix for CVE-2025-49704, while CVE-2025-53771 is a bypass of the fix for CVE-2025-49706—both vulnerabilities that Microsoft had patched in their July 2025 Patch Tuesday release.

The attack chain operates in two devastating stages. First, attackers send a

POST request to `/_layouts/15/ToolPane.aspx` using a crafted Referer header to bypass authentication. Then, with authenticated access to the vulnerable endpoint, they exploit an insecure deserialization vulnerability by submitting a malicious payload in the POST body.

What makes this attack particularly insidious is its persistence mechanism. The malicious activity involves delivering ASPX payloads via PowerShell, which is then used to steal the SharePoint server's MachineKey configuration, including the ValidationKey and DecryptionKey, to maintain persistent access. As cybersecurity expert Jake Williams noted, "With these keys in hand, attackers can craft forged `__VIEWSTATE` payloads that SharePoint will accept as valid—enabling seamless remote code execution. This approach makes remediation particularly difficult—a typical patch would not automatically rotate these stolen cryptographic secrets, leaving organizations vulnerable even after they patch."

STATE-SPONSORED ACTORS AND RANSOMWARE GROUPS JOIN THE FRAY

The exploitation campaign attracted a rogues' gallery of threat actors that reads like a who's who of global cybercrime. Microsoft observed two named Chinese nation-state actors, Linen Typhoon and Violet Typhoon, exploiting these vulnerabilities targeting internet-facing SharePoint servers. Additionally, another China-based threat actor, tracked as Storm-2603, was observed exploiting these vulnerabilities to deploy ransomware.

This convergence of nation-state actors and cybercriminals underscores the vulnerability's strategic importance. SharePoint's deep integration with Microsoft's platform, including services like Office, Teams, OneDrive and Outlook, makes it especially valuable to attackers because a compromise doesn't stay contained—it opens

the door to the entire network.

The ransomware angle adds another layer of urgency to the threat landscape. Security researchers have documented how Storm-2603 exploited these vulnerabilities to distribute Warlock ransomware, demonstrating how zero-day vulnerabilities can quickly become weapons in ransomware arsenals.

THE MODERNIZATION IMPERATIVE

For Richard Harbridge, Microsoft MVP and migration strategist at ShareGate, the breach represents more than just a security incident—it's a clarion call for organizational transformation. "Today's Microsoft breach is a critical reminder for organizations still relying on legacy SharePoint systems," Harbridge emphasized. "If you're running SharePoint Server 2016, 2019, or SPSE and haven't patched, the first step is immediate isolation and emergency remediation."

Harbridge's assessment of the situation is stark: if the telltale `spinstall0.aspx` file is present on a system, organizations should "assume full compromise." This means taking servers offline, rotating all service credentials and machine keys, scanning for persistence tools like ToolShells, and rebuilding any machines showing signs of tampering.

But Harbridge sees an opportunity in this crisis. "The cloud version of SharePoint isn't vulnerable to this," he noted. "Every hour an organization remains on-premises increases its exposure and the operational burden on IT. It's time to treat modernization as part of your incident response strategy, not just a future initiative."

The migration path he advocates involves moving to SharePoint Online, which benefits from "real-time threat detection, automated logging, and continuous patch cycles that outpace adversaries." Tools like ShareGate's migration suite can facilitate this transition by moving terabytes of content with full fidelity, including metadata and permissions, with zero downtime.



For **RICHARD HARBRIDGE**, Microsoft MVP and migration strategist at ShareGate, the breach represents more than just a security incident—it's a clarion call for organizational transformation. "Today's Microsoft breach is a critical reminder for organizations still relying on legacy SharePoint systems," Harbridge emphasized. "If you're running SharePoint Server 2016, 2019, or SPSE and haven't patched, the first step is immediate isolation and emergency remediation."

THE RANSOMWARE CONNECTION

Cynthia Kaiser, SVP of Halcyon's Ransomware Research Center and former Deputy Director of the FBI's Cyber Unit, brings a law enforcement perspective to the crisis that's particularly sobering. "Right now, people should be just as worried about what happened as what happens next," Kaiser warned. "Once these vulnerabilities are discovered, we have historically seen ransomware groups quickly operationalize them against victims."

Kaiser's concern extends beyond the immediate exploitation. "Once these criminals are in a network, they can hide, lie in wait, and cause untold damage to a company," she explained. Her recommendation focuses on behavioral detection: "Organizations should be thinking seriously about whether they have the right tools that detect and stop ransomware activity at the behavioral level before disruption occurs."

This perspective aligns with broader industry observations about the evolving threat landscape. Unit 42 and other organizations, including Microsoft, have observed widespread active exploitation of these vulnerabilities, with telemetry revealing a clear evolution in the SharePoint ToolShell attack campaign progressing through two distinct phases.

DETECTION AND RESPONSE CHALLENGES

The SharePoint vulnerabilities present unique challenges for detection and response teams. The Canadian Centre for Cyber Security noted that AMSI may not consistently offer comprehensive protection against this form of exploitation, as threat actors frequently adapt their methods to evade detection.

Organizations are urged to look for specific indicators of compromise, including the presence of the file C:\PROGRA1\COMMON1\MICROS1\WEBSE1\16\TEMPLATE\LAYOUTS\spinstall0.aspx and network logs showing scanning or exploitation attempts from specific IP addresses, particularly since July 17, 2025.

Microsoft has provided detailed hunting queries for organizations using their security tools, focusing on the creation of the spinstall0.aspx file and process creations where w3wp.exe spawns encoded PowerShell involving suspicious file paths.

THE BROADER SECURITY IMPLICATIONS

The SharePoint breach illuminates several critical trends in the cybersecurity landscape. First, the speed at which threat actors can bypass vendor patches demonstrates the arms race between defenders and attackers. Microsoft patched CVE-2025-49704 and CVE-2025-49706 in the July 2025 Patch Tuesday release, but threat actors recently found new paths to exploit the same core logic, prompting Microsoft to assign new CVEs and release emergency fixes.

Second, the incident underscores the strategic value of enterprise collaboration



CYNTHIA KAISER, SVP of Halcyon's Ransomware Research Center and former Deputy Director of the FBI's Cyber Unit, brings a law enforcement perspective to the crisis that's particularly sobering. "Right now, people should be just as worried about what happened as what happens next," Kaiser warned. "Once these vulnerabilities are discovered, we have historically seen ransomware groups quickly operationalize them against victims."

platforms to threat actors. SharePoint servers often serve as gateways to broader corporate networks, containing sensitive documents, user credentials, and connections to other critical business systems.

Third, the involvement of multiple nation-state actors and ransomware groups in exploiting the same vulnerabilities highlights how quickly valuable exploits proliferate across different threat actor communities.

MICROSOFT'S RESPONSE AND REMEDIATION

Microsoft's response to the crisis evolved rapidly as the scope of the threat became clear. The company released security updates that fully protect customers using all supported versions of SharePoint affected by CVE-2025-53770 and CVE-2025-53771, urging customers to apply these updates immediately.

The company's remediation guidance emphasizes multiple layers of protection: applying the latest security updates, configuring Antimalware Scan Interface (AMSI) integration in SharePoint, deploying Microsoft Defender Antivirus on all SharePoint servers, and rotating SharePoint server ASP.NET machine keys and restarting IIS.

For organizations unable to immediately patch, Microsoft recommends disconnecting affected servers from the internet until updates can be applied, or implementing authentication gateways to limit unauthenticated traffic.

LESSONS FOR THE INDUSTRY

The SharePoint breach offers several critical lessons for organizations and the cybersecurity industry as a whole. First, the incident demonstrates that patch bypass vulnerabilities are becoming increasingly common and sophisticated, requiring organizations to think beyond traditional patch management cycles.

Second, the rapid exploitation of these vulnerabilities by multiple threat actor groups underscores the need for behavioral detection capabilities that can identify malicious activity even when using novel techniques.

Third, the incident highlights the security advantages of cloud-native solutions over on-premises infrastructure, particularly for collaboration platforms that are frequent targets of attack.

Looking Forward: The Cloud Imperative
As organizations assess the damage and plan their response, many are reaching the

same conclusion as Harbridge: the future lies in cloud migration. The SharePoint incident serves as a powerful case study in the security benefits of moving away from on-premises infrastructure that requires constant vigilance and rapid patching.

Cloud-based SharePoint Online demonstrated its resilience during this crisis, remaining unaffected by vulnerabilities that devastated on-premises deployments. This immunity stems from Microsoft's ability to implement protections and patches across its cloud infrastructure more rapidly and comprehensively than individual organizations can manage on their own systems.

For Chief Information Security Officers and IT leaders, the breach presents an opportunity to accelerate digital transformation initiatives that may have been progressing slowly due to cost or complexity concerns. The potential impact of a successful SharePoint compromise—including data theft, ransomware deployment, and lateral movement throughout corporate networks—may justify the investment required for cloud migration.

THE BOTTOM LINE

The SharePoint zero-day exploitation campaign represents more than just another cybersecurity incident—it's a fundamental challenge to how organizations think about infrastructure security and modernization. With hundreds of organizations compromised and nation-state actors actively exploiting these vulnerabilities, the incident serves as a stark reminder that legacy on-premises systems present increasingly untenable risks in today's threat landscape.

For organizations still running on-premises SharePoint servers, the message from security experts is clear: immediate patching is essential, but long-term security requires a fundamental shift toward cloud-based solutions that can provide the rapid response and comprehensive protection that modern threats demand. As Harbridge noted, "It's not just about recovering from CVE-2025-53770—it's about making sure the next zero-day doesn't land on your doorstep."

The race between attackers and defenders continues to accelerate, but this incident has shown that organizations with the right architecture and response capabilities can weather even the most sophisticated attacks. The question now is whether other organizations will learn from this crisis and take the steps necessary to protect themselves against the next inevitable wave of attacks.

INFOTECH FORUM 2025:
POWERING INDIA'S DIGITAL LEAP INTO THE FUTURE



(Pictures from L-R): Dr. Deepak Kumar Sahu, Publisher & Editor-in-chief-VARINDIA, Mr. Sridhar S- Executive V.P- SSG, Redington Limited, Mr. Ronald Fernandes - Country Manager-Context World, Mr. Pranab Mohanty, Chief Business Officer- Data Safeguard India, Lt. Col. Sarthak Bhuyan, Director- Catalytx technologies, Mr. Varun Garg, Co-Founder & CEO- Quantum Technology Systems, Mr. Sandeep Sengupta, Founder & Director-ISOAH Data Securities, Dr. Arindam Sarkar, HoD & Asst Prof. Computer Science & Electronics at Ramakrishna Mission Vidyamandira, Belur Math, Dr. Sandip Chatterjee, Sr. Advisor, SERI(USA) and Ex-Scientist G & Group Coordinator, Meity, Govt. of India, Dr. Sanjay Kumar Das, Addl. Sec. (Science & Technology & Bio Technology Dept.) & State CISO- Government Of West Bengal, Mr. Mylaraiah J N, V.P.- Enterprise Sales, India & SAARC- Commscope, Adv (Dr.) Prashant Mali, Ph.D. in Cyber Law, Practicing Lawyer Bombay High Court, Ms. S Mohini Ratna, Editor-VARINDIA

Once again, the VARINDIA InfoTech Forum 2025 set a new benchmark in industry engagement, combining deep insights, strategic foresight, and unmatched networking opportunities, solidifying its stature as a premier thought leadership platform for India's ICT community.

The 23rd edition of the VARINDIA InfoTech Forum Leadership Summit 2025 unfolded with remarkable energy and enthusiasm, cementing its status as a premier platform for insight, innovation, and recognition within India's dynamic ICT ecosystem. Organized by Kalinga Digital Media Private Limited, the summit convened an elite assembly of technology leaders—including CIOs, CTOs, CISOs, policymakers, industry veterans, marketing heads, and senior executives spanning the entire ICT value chain.

Centered around the theme “Balancing Innovation and Sustainability,” the summit focused on the vital convergence of digital acceleration, responsible technology adoption, and the ethical imperatives of innovation in building a future-ready digital economy.

The day-long event was thoughtfully curated into morning, afternoon, and evening sessions, featuring keynote addresses, thought-provoking panel discussions, exclusive research launches, the grand unveiling of the annual coffee table book ‘Brand Book’, and distinguished award ceremonies honoring the

most trusted companies and eminent CIOs.

The event also saw enthusiastic virtual participation, with attendees sharing their insights on social media using the #ITForum2025.

The proceedings began with a ceremonial welcome, marked by the traditional lighting of the lamp—symbolizing the start of a day dedicated to knowledge-sharing, inspiration, and collective growth.

The opening address was delivered by Dr. Deepak Kumar Sahu, Editor-in-Chief of VARINDIA. He emphasized the need for India's \$250 billion IT industry to increase domestic investment to truly lead in the AI era. As AI continues to revolutionize industries and cybersecurity, he highlighted how the Brand Book celebrates the spirit of technological innovation that is propelling India's digital growth, resilience, and the creation of a secure, sustainable, and borderless future.

The welcome address was delivered by Adv. (Dr.) Prashant Mali, a distinguished Cyber Law expert, offered valuable insights

into the rise of AI-enabled cybercrimes and their far-reaching implications for both businesses and individuals in India. His session effectively set the tone for a deeper exploration of cybersecurity challenges in the digital era.

Following this, the keynote address by Dr. Sandip Chatterjee focused on critical aspects of IT Asset Disposal (ITAD), data vulnerability, and the legal consequences tied to data management. These opening sessions laid a strong and insightful foundation for the day's deliberations.

The event continued with a series of compelling corporate presentations, featuring thought-provoking sessions by industry leaders that includes names of Mr. Varun Garg, Co-Founder & CEO of Quantum Technology Systems, who shared insights on AI and data center acceleration. Mr. Sridhar S., Executive Vice President of the Software & Security Business Group at Redington Limited, spoke about leveraging technology to build a digital future. Mr. Ashwani Narang, Vice President & Head of Finance & Spend Management at SAP Indian Subcontinent, discussed intelligent enterprise

solutions powered by cloud and AI. Meanwhile, Mr. Gaurav V. Saxena, Director of Channels & Alliances for India & SAARC at Veeam Software, presented his views on AI ethics and responsible innovation.

The morning session concluded with a vibrant panel discussion moderated by Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA. Titled "AI and the Future of Work," the panel included esteemed CIOs namely Mr. Ashis Rout, Sr. Vice President (IT), Ex-HDFC Bank, Mr. Vijay Sethi, Chairman, Mentorkart and CrafSol Technologies, Mr. Bharat B Anand, Group CIO & CTO, Contec Global, Mr. Anil Nama, CIO, CtrlS Datacenters & Cloud4C and Mr. Sandeep Sengupta, Founder & Director, ISOAH Data Securities who explored how AI and cloud are redefining the workplace, enhancing human capabilities, and demanding new skill sets across sectors.

The afternoon session kicked off by honoring 25 exceptional Value-Added Resellers (VARs) and technology partners with the "Most Promising Partner of the Year 2025" award. These organizations were recognized for their excellence across five distinct categories. These partners were applauded for their consistent efforts in enhancing customer experience and driving digital adoption at scale.

The event then witnessed the unveiling of the "Made in India Research Report" by Mr. Gyana Ranjan Swain, Consulting Editor, VARINDIA. Based on insights from over 30,000 Indian VARs, the report captured the dynamism, challenges, and immense opportunities within the indigenous tech product ecosystem. Strongly aligned with the "Make in India" initiative, the report reaffirmed India's emergence as a global hub for technology manufacturing and innovation.

Following this, the forum continued its deep dive into pressing technology themes. Dr. Arindam Sarkar, HOD and Assistant Professor, Department of Computer Science & Electronics, Ramakrishna Mission Vidyamandira, Belur Math, delivered a powerful session on combating synthetic fraud through AI-powered solutions like FaceOff AI. His insights into neural and GAN cryptography provided a fresh and timely perspective on the evolving threat landscape. The session also marked the official unveiling of FaceOff AI (FO AI)—a significant step forward in the fight against deepfake and identity-based fraud.

Dr. Sanjay Kumar Das, Additional Secretary (S&T and Biotechnology) with the Government of West Bengal, then took the stage to discuss Privacy Enhancing Technologies (PETs) and their strategic value in enabling secure data innovations. He emphasized the need for secure-by-design architecture in public digital infrastructures.

A standout panel discussion on "Accelerating the Future: 5G, AI & IoT Advancements" was moderated by Ms. S. Mohini Ratna, Editor, VARINDIA. Thought leaders including President- Cyber Security Corporation, Mr. Deepak Kumar, Global Head - Cyber Defense- Infogain India, Mr. Dhananjay Rokde, CISO & Director- iMan-edge Services, Dr. Rakshit Tandon, Cyber Security Evangelist, Mr. Jaspreet Singh (Partner) - Grant Thornton Bharat, Mr. Pradipta Patro, Head of cyber security & IT Platform- KEC International Ltd., and Mr. Nabendu Misra, Sr. AI Architect- EY, shared how these converging technologies are transforming infrastructure, enhancing citizen services, and opening new business models.

The panel discussion was followed by two impactful corporate presentations, one from Mr. Jithesh Chembil, Head Channels-India, Pure Storage who spoke on the concept of an autonomous Enterprise Data Cloud and how organizations can manage data intelligently in the AI era. Second presentation was from Mr. Kapil Rana, Account Executive - Architecture- Cisco India & SAARC who shared insights on building AI-ready data centers to support scalable and resilient digital transformation.

The third and the last panel discussion of the day tackled a timely and vital issue: "Safeguarding Brand Trust in the Deepfake Era." Moderated by Mr. Gyana Ranjan Swain, the session brought together marketing and cybersecurity experts to address the growing risks of misinformation, manipulated media, and privacy violations. The panelists included, Mr. Sanjay Chaudhary, Head of Enterprise Marketing- SAP, Mr. Ritesh Dhawan, Marketing Head (India)- Redington Ltd., Ms. Vinny Sharma, Marketing Director for APJ & MEA- Securonix, Mr. Arvind Saxena CMO- NEC India. They emphasized the need for AI-powered detection tools, clear privacy policies, ethical marketing practices, and public awareness campaigns to safeguard brand integrity in an era of rising digital manipulation.

A key highlight of the evening session at the VARINDIA Infotech Forum 2025 was the grand launch of the 14th edition of the Brand Book 2025, now live on www.mybrandbook.co.in. The prestigious unveiling was graced by former Member of Parliament, Shri KC Tyagi, adding gravitas to the event.

Many dignitaries from the IT industry along with Shri Prashant Kumar, Deputy Director General, Telecom Engineering Centre, Ministry of Communications, Government of India, joined him to launch this widely regarded book. As a trusted industry resource, the Brand Book offers in-depth white papers, CXO interviews, and expert analysis of evolving market dynamics. This edition provides valuable insights

into emerging technology trends, strategic leadership, and brand innovations that are transforming the enterprise landscape—making it an essential guide for VARs, corporate leaders, and CXO decision-makers.

This was followed by the last round of engaging corporate presentations from Mr. Sanjeev Kumar, Regional Sales Director, India & SAARC- SonicWall who shared the perspective on cyber resilience strategies for the Digital India vision. He was followed by Mr. Rajesh Chhabra, GM (India & South Asia)- Acronis who discussed an integrated approach to cybersecurity. Mr. M.A. Johar, President- CP Plus focused on the safe and intelligent infrastructure for security and surveillance. Last but not the least, Mr. Atul Kumar, Director-DSCI elaborated on the evolving cybersecurity narratives amid rapid tech advancements.

The final segment of the awards ceremony commenced with the prestigious presentation of the Lifetime Achievement Award to Dr. Gulshan Rai, Former National Cyber Security Coordinator and Director General, CERT-IN. The forum reached a defining moment as it celebrated Dr. Rai's remarkable career spanning over 48 years. His pioneering contributions include the development of ERNET, the establishment of key e-Governance frameworks, and the formulation of India's foundational cybersecurity policies and legislation.

Thanking VARINDIA, he talked about India's cybersecurity priorities in the context of a rapidly digitizing economy.

This was followed by the recognition of the Top 11 Most Influential CMOs in India 2025, highlighting marketers who are redefining brand engagement and customer experience in the digital age. This was followed by the felicitation of 102 Eminent CIOs, CTOs, and CISOs from across industries for their role in driving enterprise transformation and digital excellence.

Next VARINDIA recognized the 25 Most Trusted Companies followed by 50 Most Admired Brands in India's ICT ecosystem. These organizations were selected through rigorous evaluation of brand performance, market reputation, and customer trust. This recognition serves as a testament to their resilience, innovation, and dedication to excellence in serving India's digital economy. These awards, grounded in both qualitative feedback and industry benchmarks, reinforce VARINDIA's commitment to recognizing merit and integrity in the tech world.

The event concluded with a vote of thanks by Ms. S. Mohini Ratna, who expressed gratitude to all speakers, partners, attendees, and supporters for making the 23rd Infotech Forum a resounding success. She highlighted VARINDIA's ongoing mission to catalyze meaningful discussions and to spotlight those leading India's digital journey.



23RD INFOTECH FORUM

Theme - Balancing

4th July 2025, Hotel Hy



SUPPORTED
BY

nixi
Empowering Networks

Redington

SAP

FACEOFF
OPINION MATTERS

CISCO **PURE**

veeam

CP PLUS

A

TECH FORUM 2025

by Innovation and Sustainability

Watt Regency, Bhikaji Cama Place, New Delhi



India must scale tech investment to lead the AI Era

DR. DEEPAK KUMAR SAHU
EDITOR-IN-CHIEF, VARINDIA

“The INFOTECH FORUM has firmly established itself as a cornerstone event for technologists, OEMs, and select strategic partners. This year’s forum is designed to be a transformative experience—fostering collaboration, inspiring innovation, and driving impactful discourse. India’s \$250 billion IT industry commands global attention, largely due to software service exports, but domestic IT spending accounts for just 1% of the global total—a critical shortfall. Global compute spending, currently at \$250 billion annually, presents a \$1 trillion opportunity over four years. By investing in this space, India has the potential to unlock innovation in healthcare, education, agriculture, and climate resilience, while also supporting its renewable energy ambitions.

We are entering an era defined by AI, hybrid cloud, and purpose-driven technology. This transformation is not only about digital tools—it’s about elevating human potential. AI is not here to replace us; it’s here to elevate us. This is not just digital transformation—it is human transformation. AI-powered operations are already transforming enterprises today. We are moving from product-centric models to immersive “Storyworlds,” from rigid funnels to dynamic ecosystems, and from mere metrics to meaningful outcomes. At the heart of this shift lies a truth: while technology is reshaping our world, it’s the stories we create with it that build trust and deliver lasting impact. As the demand for AI workloads grows, so does the need for high-density compute environments—straining existing data center infrastructure, especially in cooling. This presents a timely opportunity for VARs and partners.

Amid this transformation, we are proud to launch the 14th edition of the Brand Book, a celebration of the remarkable growth of India’s technology sector. This edition showcases how leading tech companies are redefining innovation and driving the country’s digital transformation. AI is also reshaping cybersecurity—delivering faster threat detection (60%), quicker incident resolution (70%), and improved phishing detection accuracy (up to 98%). But with opportunity comes risk, as attackers also harness AI to scale sophisticated threats. In this rapidly evolving landscape, AI is no longer optional—it is essential. Let us build a secure, borderless digital future and protect the data powering our interconnected world.”



From 64Kbps to 6G: The Quantum Leap in India’s Tech Journey

DR. GULSHAN RAI
FORMER NATIONAL CYBER SECURITY COORDINATOR
AND DIRECTOR GENERAL, CERT-IN

“It is a privilege to stand before this distinguished gathering of veterans and visionaries who have shaped the very foundations of our digital and security ecosystems. Tonight isn’t about my personal journey—it’s about our collective one. The recognition I receive is a tribute to the shared work, planning, and resilience of all of us who’ve brought this ecosystem to where it stands today.

As Atul highlighted earlier, our journey began in simpler times. And today, we find ourselves navigating an era of unprecedented complexity. These aren’t futuristic challenges—they’re here. Just last month, data traffic between two of the world’s most advanced nations was hijacked for hours every day over a full week. Post-quantum cryptography, state-level actors, and sophisticated hijacks are not on the horizon—they’re happening now.

Think about how far we’ve come. In 2000, we were building backbones with 64K lines, planning 565 Mbps copper networks—numbers that now feel quaint. Today, homes enjoy gigabit speeds; 5G is here; 6G is emerging. With that explosion in connectivity, our security challenges have multiplied exponentially.

To face this reality, we need more than tools—we need smart solutions for smart problems. Adaptive, integrated systems that protect economies, businesses, and citizens while keeping pace with forces like AI, deepfakes, and quantum threats.

But solving this requires four essentials:

- Comprehensive systems tailored to real business needs and emerging threat vectors.
- Skilled talent to design, scale, and evolve these solutions.
- Regulatory harmony—because today, conflicting rules slow us more than they protect us.

Collaboration, where government transitions from driver to facilitator, empowering the industry that holds the expertise to lead.

Technology’s acceleration cannot be stopped. AI, deepfakes, post-quantum computing—they’re inevitable. Our task isn’t to resist but to harness them—securely, responsibly, and innovatively.

I extend my deepest gratitude to Dr. Sahu for this honor and to everyone who has built the platforms, partnerships, and resilience we stand on today. Let’s continue working together—not just to keep up with the future, but to secure it.”



Privacy enhancing technologies are a means to protect individual privacy and personal data

DR. SANJAY KUMAR DAS
ADDITIONAL SECRETARY (S&T AND BIOTECHNOLOGY)
WITH THE GOVERNMENT OF WEST BENGAL

“Secure Multi Party Computation (SMPC) is one of the privacy enhancing technologies (PET). So why does PET matter? So we understand that the basic features extracted out of the data from the data sets are being computed. And these computations are being done in a competent, collective and a collaborative format in a completely neutral location. So this secure multi party computation is actually leading us specifically to a point where we are looking at zero knowledge proof and homomorphic encryption. We are today looking at computing on encrypted data. The GAFAM members namely Google, Amazon, Facebook, Apple and Microsoft were hit hard by GDPR, and they collectively paid hundreds of billions of dollars over the years as a privacy driven non-compliance penalty. Then they realized that even if they want everyone to come to a SAS model or a subscription-based model, they cannot use one's data without their consent. Most of us are paying Google today for our mail storage space. But even if we are paying Google, they cannot use my data without my explicit permission. So now Google is doing computation on encrypted data. It allows for processing information without needing to decrypt the data, thus maintaining privacy. Computing on encrypted Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) requires specialized techniques like homomorphic encryption or secure multi-party computation. So my AADHAAR number or voter ID card number is my PII, while information like the medicine that I take in the morning to keep my pressure at a certain level is my SPII data. Both PII and SPII have connectors to respective identification and if they are extracted, they actually lose the value of connection. So when these data nodes are extracted, these connectors get snapped. Without these connectors, there is no threat to your privacy being exposed.

As a CISO, you should understand the core PET concept, because ultimately, you cannot be a data zero organization but have to be a data minimized organization. So when you allow somebody to fill up a form, remember to take only those data that you require, then give back the data which you don't require. Next, PET actually tells us to create noise around the data, so that somebody who is creeping into the data sometimes falters to identify the sensitive data lying before. So Secure Multi Party Computation actually makes Faceoff a beautiful product that it is today and is a good ambassador of PET.

Ultimately, even if you have all the data and information, you may not possess all the knowledge. Because information percolates laterally, while knowledge is generated vertically. So you have all the data, but you don't have the connectors, and so you don't have the knowledge.”



CISOs must tackle AI risks beyond compliance and controls

ADV (DR.) PRASHANT MALI
PH.D. IN CYBER LAW, PRACTICING LAWYER,
BOMBAY HIGH COURT

“AI has no feelings, and that's precisely what makes it both powerful and dangerous. It no longer just supports cybersecurity—it has become a weapon. From deepfake frauds and AI-generated malware to autonomous phishing and synthetic identities, AI is now automating the entire attack chain. Earlier, a human actor had to deploy and negotiate ransomware attacks, but today AI handles everything—from multilingual phishing emails to morphing digital signatures. CISOs are facing a battlefield that has evolved from compliance to combat. If you don't understand the legal framework—DPDPA, Section 66 of the IT Act, or the emerging concept of 'liar's dividend' where truth itself can be denied as AI-generated—you're not just at risk, you're exposed.

The challenge now is that AI-generated threats are not just technological—they're legal, evidentiary, and organizational. Courts struggle to verify deepfake videos or AI-generated documents because the chain of custody is easily broken, and forensic reports are often inadmissible. AI responses are dynamic and person-specific—what an AI chatbot tells one user could differ for another. So when evidence varies by user or time, how can it stand in court? We still lack table-screen setups, SOPs for AI evidence verification, or proper electronic evidence management frameworks. Even in major breaches, like the Cosmos Bank heist, evidence gets contaminated because there's no clear policy on who collects it first. Without formal AI audit trails, signed forensic reports, or awareness in lower judiciary, we risk undermining justice in AI-fuelled cybercrimes.

CISOs must now prioritize AI-specific clauses in vendor contracts, employee conduct codes, and incident response plans. Boardrooms must wake up—not just to AI's investment hype but to its governance risk. Deepfake detection should be an annual IT budget mandate, and AI threat modelling must become part of security drills. Embed AI in IS audits, mandate vendor AI declarations, and preserve the chain of custody for all AI evidence. Because in a world where AI can impersonate voices, spoof identities, and even manipulate truth, organizations must move beyond slogans like 'zero trust' and prove their cybersecurity maturity with real, defensible documentation. AI is not just a tool—it's a force. Use it wisely or risk being outmanoeuvred by it.”



Secure IT disposal crucial to prevent data breaches and legal risks

DR. SANDIP CHATTERJEE
SR. ADVISOR - SERI, USA, AND FORMER SR. DIRECTOR
& GROUP COORDINATOR - MEITY, GOI

"After my MeitY tenure, I joined SERI USA, focusing on sustainable electronics and the critical issue of IT asset disposition. Over the past decade, India's digital push—driven by infrastructure like DigiLocker, BharatNet, and UPI—has propelled our economy to \$4 trillion, with 25% of that growth powered by digital innovation. But this growth comes with responsibility. We've created a data-driven economy, yet we must ensure that our progress remains inclusive, affordable, and sustainable. As we shift from an IT-based to an AI-driven economy, our electronics are becoming more resource-intensive—phones now use up to 69 elements from the periodic table. But even the best refineries can recover only a fraction of those. This material limitation, coupled with increasing e-waste, demands that we prioritize refurbishment before recycling and promote circular use of electronics.

The real danger lies in data: we wrongly assume that formatting or deleting removes it, but 60% of global devices still leak sensitive information after disposal. In India, 71% of tested devices retained recoverable data—banking info, Aadhaar details, even passports. I helped draft the DPDPA Act, which will hold companies accountable with penalties up to ₹250 crore, but until its rules are finalized, we rely on moral obligation. That's not enough. From Morgan Stanley's \$60 million fine to India's local vulnerabilities, it's clear—improper data disposal is a massive threat. Techniques like degaussing, overwriting, or cryptographic erasure must be applied based on device type, especially since many physical destruction methods are ineffective or outdated. Simply hammering a hard drive won't protect you anymore.

What we need is adherence to global best practices—standards like R2 certification that ensure traceability, compliance, and proper sanitization. This isn't just about protecting privacy—data loss is business loss. Studies show 94% of companies suffering severe data loss never fully recover. We must make secure IT disposal the norm, not the exception. France already mandates refurbishment before recycling—we should, too. Our goal should be sustainability with accountability: maximize the life and value of devices, follow global regulations like GDPR and NIST, and ensure secure, eco-friendly IT practices. If we care about how we use technology, we must care just as much about how we retire it."



In case of synthetic fraud, the victim remains oblivious of the deceit unless made aware

DR. ARINDAM SARKAR
HOD AND ASSISTANT PROFESSOR, DEPARTMENT OF
COMPUTER SCIENCE & ELECTRONICS-RAMAKRISHNA
MISSION VIDYAMANDIRA, BELUR MATH

"Talking about synthetic fraud, we understand that forces are trying to create fictitious identities and are trying to fabricate the data. They are trying to blend real and fake personal information. The problem is that no real person is affected directly. That is why victims stay unaware, and we do not have the technology to check whether a video is real or fake. All of us are aware that we have used our VID (Virtual ID) to save our Aadhaar information. I can break the VID and can gather all your information. This information is actually being taken for data connection purposes. After collecting the data, I can fabricate the identity and then apply for the loan. I can build credibility and then after taking the loan, I will default.

So what are the different types of synthetic frauds? It starts with credit card fraud, where the fraudster will build the credit history and then default on a large amount. Then there is employment fraud, where the fraudster will create fake identities for jobs and trick a person looking for a job into believing it. Likewise, there are several different frauds which includes government benefit frauds for pension account holders insurance or healthcare frauds, or the SIM card fraud in the telecom industry where fake identities are created for issuing dubious SIM cards. The challenge behind these frauds is the inability to detect the real fraudster or the victim. There is also the problem of data silos which means we are not able to gather all the data together. Suppose you know the machine learning and deep learning algorithm and the fuel for this is the data. So if you collaborate all the data together, only then you will be able to proceed to train your machine or deep learning algorithm. But the problem is, let's say in the case of FinTech, data is distributed and you are unable to collect all of it from different parts of your institute. And that is when the problem of zero day attacks arises. The tagline for deep fake would be – Naqli Chehra, Asli Khel, Suraksha ka ho gaya Fail!

So how can we tackle this whole problem of deep fake? The first is to detect the Identification Method; second is doing Psychological or Physiological Liveness check; and the third is Audio Analysis. So presenting before you the Faceoff – a Revolutionary AI Platform for Digital Authenticity and Deepfake Detection. Under this platform we have eight different modules. Faceoff addresses the challenges of deepfake attacks, digital fraud, and authenticity challenges through advanced multimodal AI capabilities that analyze multiple behavioral and biometric indicators simultaneously, delivering unprecedented accuracy in digital authenticity verification."



AI, Digital Vulnerabilities, and Policy Gaps Are Fueling a New Era of Cybercrime!

ATUL KUMAR
DIRECTOR - DSCI

In a compelling talk on the evolution and future of cybersecurity, he offered a broad perspective on how emerging technologies are reshaping the cyber landscape. He shared that while discussing emerging technologies, we often focus on IoT, AI, and cloud, but I believe we also need to look at adjacent fields like material sciences, which are quietly but significantly shaping cyber innovation. For instance, Microsoft’s Majorana quantum chip was celebrated as a quantum breakthrough, but behind it was a major material science innovation—supported in its final phase by generative AI models, which expedited the 20-year research.

This illustrates how interdisciplinary advancements are pushing cybersecurity forward, and also widening the scope of threats. With the digital economy expanding, we’re facing increased vulnerabilities, attack surfaces, and sophisticated threat actors exploiting gaps in systems and processes—financial or otherwise. The disparity in cyber awareness across individuals, SMBs, and large enterprises adds to this complexity.

Adversaries are now using the same tech—AI, crypto, cross-platform tools, even the dark web—to launch polymorphic malware and adaptive threats like those from Salt Typhoon or Lazarus groups. These attacks evolve during deployment, making them harder to detect. The crimes born from this tech misuse span personal, societal, and even geopolitical dimensions, touching on terrorism, separatism, and extremism.

A major challenge lies in the gap between fast-moving tech and slow-moving policy. Legal frameworks, infrastructure readiness, and cyber skills are often outdated. With AI, quantum computing, 6G, and over 200 zettabytes of data expected by 2025, we’re entering an age of “harvest now, decrypt later” threats—especially concerning for encrypted healthcare and biometric data. Combined with deepfakes and synthetic media, the risks to electoral systems, diplomacy, and biosecurity are real and growing.

Even export controls are no longer foolproof, as open-source models like China’s DeepSeek enter global supply chains unnoticed. This raises the importance of a resilient and innovative cybersecurity ecosystem. Fortunately, India is emerging as a global hub, with over 450 cybersecurity product firms. Our architecture, policies, and awareness strategies must evolve in sync with the pace of both innovation and adoption.

In conclusion, while the landscape is daunting, the answer lies in responsible innovation, cross-disciplinary thinking, and collective vigilance. The more we nurture this ecosystem, the stronger and safer our digital future will be.



VARINDIA Driving ICT Innovation through collaboration

MS. S. MOHINI RATNA
EDITOR, VARINDIA

“Welcoming the esteemed dignitaries and distinguished guests, and passionate technology evangelists, she thanked for their presence making this annual gathering truly special. I take this opportunity to reflect on the enduring legacy of VARINDIA and the Brand Book, both proud flagships of Kalinga Digital Media. For over 26 years, VARINDIA has remained India’s most trusted and influential source for technology news, offering credible insights and consistent value to the ICT ecosystem.

Equally significant is the Brand Book, which highlights the strategic vision and leadership of India’s top technology brands. Today, I am proud to unveil the 14th edition, a tribute to both legacy and innovation, celebrating brands that continue to shape the future of Indian IT.

This morning, during the Infotech Forum, we witnessed enriching conversations among policymakers, industry thought leaders, and tech professionals. CIOs, CTOs, CISOs, and CMOs engaged across three thought-provoking panel tracks centered on the theme “Balancing Innovation and Sustainability.”

Our survey findings from the Eminent CIOs of India project reveal the changing priorities of digital leaders. Their focus is now firmly on cybersecurity, AI integration, data analytics, and talent management in response to the ongoing digital transformation. Emphasis is being placed on Zero Trust models, proactive threat intelligence, and compliance with evolving data protection laws. At the same time, responsible AI adoption, automation, and legacy modernization are shaping more secure and efficient enterprises.

I’m delighted to share that we would be in few minutes officially unveiling the Brand Book 2025—a beautifully designed coffee table book that showcases the excellence of India’s leading tech brands. This edition also includes inspiring profiles of 100 Eminent CIOs, spotlighting the leaders who are driving transformation with vision and resilience.

We are also celebrating the achievements of the Most Trusted Companies and Most Admired Brands of 2025–26, who play a vital role in India’s digital progress.

Thank you all for your vibrant participation, thoughtful questions, and insightful discussions. Your presence and engagement have been the true highlights of today’s event. She concluded by saying, “Let’s continue to collaborate, innovate, and shape the future of India’s tech landscape together. I wish you all meaningful interactions and fruitful new business opportunities.”



Veeam delivers unified, AI-powered data resilience for enterprises

GAURAV V SAXENA
DIRECTOR, CHANNELS & ALLIANCES - INDIA & SAARC, VEEAM SOFTWARE



“At Veeam, we are proud to serve as the first line of defense for organizations navigating the complex challenges of modern data protection. With over \$1.8 billion in ARR and a presence in more than 155 countries, Veeam delivers enterprise-grade, software-defined, and hardware-agnostic solutions that support over 550,000 customers globally—including 8,000 in India alone. Our comprehensive platform protects workloads across on-premises, cloud, SaaS, and hybrid environments, while our partnerships with hyperscalers like Microsoft ensure seamless backup and data recovery through offerings like Veeam Data Cloud. As threats become more advanced, we are embedding AI and cybersecurity into the core of our platform to help detect, respond to, and recover from ransomware and other malicious attacks. Our acquisition of Coveware further strengthens our cyber resiliency offerings with support across pre-, during-, and post-incident scenarios.

The path forward demands more than just technology—it requires a mature, strategic approach. That’s why we’ve introduced the Data Resilience Maturity Model, built in collaboration with McKinsey and MIT experts, to guide organizations in aligning people, process, and platforms for smarter data protection. With cyber threats increasingly targeting backup repositories and 74% of enterprises still relying on manual recovery processes, our mission is clear: to empower businesses with a unified, intelligent, and agile data resilience strategy that keeps them secure and future-ready.”

The growing adoption of AI is driving up infrastructure workloads

KAPIL RANA
ACCOUNT EXECUTIVE – ARCHITECTURE – CISCO INDIA & SAARC



“Cisco has created a complete ecosystem by partnering with Pure Storage, where the infrastructure – essentially the AI compute, the storage and the networking stack – everything is integrated. That helps our customers get a deep visibility and network observability into what is happening inside the infrastructure or how the entire AI workload is running. The good part is the entire ecosystem is well documented in a Cisco validated design.

AI today is changing everything in the industry and the world around us. This acceleration for AI adoption is also happening very fast. So we need a system which can respond to that speed and that requirement. Irrespective of the vertical and the size, every organization today is adopting AI in their day to day job and identifying new revenue streams. We have use cases with almost every vertical, be it health care, education, government, defense, and financial services, of using AI. This creates a lot of pressure as data centers today are not only catering to the traditional workload but they need to cater to your AI workload as well. The data centers, which were running traditionally on a seven or eight kW per rack power provisioning is not sufficient today. While we need to provision everything, we also have an opposing force in terms of the cost pressure from every organization and the business demand. Today's demands require AI to deploy and scale rapidly. At the same time, it's essential to address the evolving threat landscape, which expands alongside the growing use of AI. So, the design philosophy at Cisco is to cater to your secure AI data center needs through a unified approach which is secured and also scalable.”

Legacy data storage platforms have now reached the stage of a breaking point

JITHESH CHEMBIL
HEAD CHANNELS, INDIA - PURE STORAGE



“Today everybody wants to build a data cloud in order to have all these high end performing applications working really well. If you look at the manually driven data centers, they need a lot of manual intervention and also have a lot of complexities. They are very similar to your cars, which if you don't maintain can break down anytime. Similarly, if you don't maintain the manual data center or any legacy data storage for that matter, there are high chances of getting into cyber-attacks. These legacy data storages are a breaking point, where you will find the data in silos. You have separate silos because years back, you had an application for which you had a storage, and now a new application came in for which you bought a separate storage. So there are a lot of data silos piling up, resulting in operations becoming very complex with multiple systems, multiple operating systems, and multiple applications. And adding more to that are the cyber-attacks which are happening. You need to build an architecture which has to be cyber resilient. It is also leading to escalating costs because of having to maintain so many different applications and OS and the forklift upgrades that need to be done every three years. The other thing is forced migration because of constant change in platforms and operating systems. The exponential growth in data is adding another level of complexity. All these problems are arising with the current, old legacy systems. Almost 80% of the budget is spent to manage these outdated systems. So what can be the solution? The answer to this is the automated future - an Intelligent enterprise data platform designed for the AI era.”

India must rethink data centers to lead global AI race



VARUN GARG
CO-FOUNDER & CEO -
QUANTUM TECHNOLOGY SYSTEMS

“Globally, the AI industry is expected to reach nearly \$10 trillion by 2030—more than twice India’s current GDP of \$4.22 trillion. With over 8,000 data centers and 55,000 AI companies operating worldwide, it’s clear the future belongs to intelligent infrastructure. India’s momentum in AI and data centers is accelerating, but to truly lead, we must shift from outdated models to advanced architectures—1 MW GPU racks, direct-to-chip and immersive cooling, high-speed interconnects, and modular, AI-managed systems that support scalability and sustainability. Data centers need to be designed not for the past, but for the AI-powered demands of tomorrow. As workloads increase, ultra-low latency, containerized edge computing, and self-healing operations will be essential, especially as cyber threats escalate and resource constraints persist.

India accounts for less than 3% of global AI penetration despite holding 20% of the world’s data. This gap signals enormous potential. The Indian government’s efforts—from Digital India and the AI Mission to PLI schemes and AI-centric SEZs—are commendable, especially with growing focus on Tier 2 and Tier 3 cities. But realizing this opportunity will require building a cohesive national ecosystem, not isolated state-level silos. At Quantum Technology Systems, we’re committed to supporting this growth by bringing in advanced cooling, robotics, and infrastructure innovations to power India’s AI journey and make it a global AI powerhouse.”

Redington curates AI evolution from enablement to ecosystem orchestration



SRIVIDHAR S
EXECUTIVE VP, SOFTWARE & SECURITY BUSINESS
GROUP, REDINGTON LIMITED

“We’re witnessing a relentless evolution in technology—from AI to GenAI, and now agentic AI—and cybersecurity is a prime example of this shift. Traditional perimeters have dissolved, identity has become the new boundary, and now AI is battling AI in real-time, with humans merely orchestrating responses. The urgency to build cyber intelligence dashboards, automate ESG reporting, and leverage personalized AI-driven content is redefining how organizations operate. Every sector—from retail to healthcare to manufacturing—is seeing tangible gains through predictive AI, automation, and real-time data processing, from reducing wastage to enhancing treatment to lowering maintenance costs. The integration of AI across verticals like R&D, procurement, CRM, and HR demonstrates how AI is no longer a futuristic concept but an operational necessity.

At Redington, we’re not just watching this transformation—we’re curating it. As a distributor, our role is shifting from mere technology enabler to ecosystem orchestrator. Through our AI Practice, we are aggregating real-world use cases—from deepfake detection and WhatsApp-based digital journeys to legal and HR automation—and connecting them with the right ISV solutions. Our goal is to overcome technology, implementation, and access frictions by delivering availability, accessibility, and usability of AI for every customer. Technology has always existed; what matters now is pairing it with the right intelligence—human or artificial—to drive outcomes, not just functionality.”

Building intelligent enterprises amid disruption with SAP, cloud and AI



ASHWANI NARANG
VP & HEAD, FINANCE & SPEND MANAGEMENT, SAP INDIAN SUBCONTINENT

“In today’s volatile global landscape, disruption is the only constant—from the COVID-19 pandemic and supply chain shocks to trade wars, AI breakthroughs, and geopolitical conflicts. These events are no longer isolated; they are interconnected and constant. To survive and grow in this environment, organizations must evolve into intelligent enterprises powered by cloud and AI. It’s no longer enough to collect data—we need actionable insights. Whether it’s predicting supplier risks, automating tax compliance, enabling AI-driven cash flow forecasting, or tracking workforce costs beyond payroll, the message is clear: we can’t run businesses based on outdated models or manual processes. AI and automation must become core to operations, not just experimental add-ons.

What SAP is enabling is the shift through an integrated business technology stack—combining ERP, data clouds, and Business AI. Our AI assistant, Joule, empowers enterprises to interact with their systems conversationally and contextually, delivering instant insights and executing tasks from invoice generation to contract validation. CXOs across functions—finance, HR, procurement, and supply chain—now recognize that technology-led transformation is central to profitability, sustainability, compliance, and employee experience. This isn’t about the future; it’s already happening. With 77% of global GDP touching SAP systems, chances are your day has already intersected with our platform. Intelligent enterprises are not aspirational—they’re operational, today.”

From Buzzword to Backbone: Acronis' Cyber Protection Vision for the MSP Era

RAJESH CHHABRA
GM (INDIA & SOUTH ASIA)- ACRONIS

“Let me introduce you to Acronis—a global leader redefining how we protect the digital world. Born in Singapore in 2003, later established in Switzerland, we now span 45 countries with 2,000 professionals, speaking 26 languages, and powering over 750,000 customers through 20,000 trusted service providers.

But we don't just talk about security—we pioneered CyberProtection. Years ago, we saw the future: businesses needed more than just cybersecurity or backup. They needed a unified approach. That's why we built Acronis CyberProtect Cloud—a single platform where data protection, cybersecurity, and remote monitoring work seamlessly together, not as separate tools but as one intelligent system. Imagine backing up anything—your on-prem systems, your cloud workloads, your Microsoft 365 mailboxes, or even critical databases like Oracle and SAP—and at the same time, safeguarding them with AI-driven defenses like EDR, XDR, MDR, and DLP. Picture this: during recovery, your data is automatically patched and secured, so you're up and running—safe and compliant—in moments.

And we're not just fighting threats; we're simplifying everything. With near-zero RPO through continuous protection, integrated SaaS and email security, and real-time threat intelligence, we take the complexity out of cybersecurity so businesses can focus on growth, not gaps.

Acronis isn't just a vendor. We're your partner in resilience—empowering organizations to thrive in an unpredictable, hyper-connected world.”



'Listening Customer First Approach' helps SonicWall Redefine Product Innovation

SANJEEV KUMAR
REGIONAL SALES DIRECTOR, INDIA & SAARC- SONICWALL

“SonicWall's evolution is much beyond than a firewall company. While many associate us with firewalls, we have grown into a comprehensive cybersecurity provider with a presence across government, corporate, mid-enterprise, and enterprise sectors. With 33 years of expertise, SonicWall has transitioned from focusing primarily on SMBs to offering a full portfolio, including managed security services, MDR, EDR, and SASE solutions.

Originally acquired by Dell in 2011 and later becoming independent, SonicWall now operates globally with its headquarters in Milpitas, California, and its India operations based in Bangalore, where R&D and technical support serve several English-speaking countries. We hold nearly a third of the SMB firewall market and have strengthened our offerings through three recent acquisitions, expanding into advanced endpoint detection, MDR, and SASE capabilities. Our strategy focuses on customer and partner feedback, ensuring products meet real-world needs before launch. We emphasize customer retention, simplified licensing, flexible cloud-aligned subscriptions, and enhanced support, including comprehensive cyber warranties of up to \$1 million for eligible deployments.

SonicWall continues to innovate with Generation 8 firewalls, the MPSS license for proactive protection, and an integrated platform to simplify management and address alert fatigue. We serve diverse industries—healthcare, education, manufacturing, retail, and smart cities—through a 100% channel-driven model supported by strong partner networks.” I would like to reiterate that SonicWall remains committed to delivering robust, scalable, and innovative security solutions worldwide.”



"Upar Wala Sab Dekh Raha Hai": India's CCTV Revolution Built on Trust and Tech

M.A. JOHAR
PRESIDENT- CP PLUS

“We've spent the day immersed in cybersecurity—firewalls, data, threats. But let's shift gears. Let's talk about something just as vital: physical security. Because true protection doesn't stop at the cloud or the network—it extends to every space we walk through. And in today's world, “smart” isn't just a buzzword. Smart means technology that learns, adapts, and responds—whether online or on the ground. That's where CP PLUS, from Aditya Infotech, comes in. We didn't just bring CCTV to India—we brought it to everyone. From homes and corner shops to large enterprises, we made security accessible. You might even remember our now-iconic line, from BigBoss ‘Uparwala sab dekh raha hai.’ It became a household phrase—because we made surveillance a part of everyday life, not just a luxury.

From launching India's first domestic CCTV brand in 2005 to building the nation's first camera manufacturing facility in 2017, we've been pioneers. Today, we produce over 200,000 cameras a month—India's largest and the world's third-largest capacity.

But this isn't just about cameras—it's about intelligence. Security today means real-time analytics, detecting threats, recognizing faces, managing traffic, even automating decisions. Whether it's schools, smart cities, railways, or retail—our AI-driven systems are shaping safer environments everywhere. With STQC and BIS certifications, trusted-core technology, and 850+ models tailored for India, CP PLUS is redefining security—homegrown, intelligent, and built for the future. Because physical security isn't a luxury anymore—it's a lifeline. And we're here to protect not just spaces, but data, lives, and trust.”





GYANA RANJAN SWAIN
CONSULTING EDITOR, VARINDIA

“During our previous year event, VARINDIA had committed to coming out with an India-based research organization to conduct an impartial, in-depth demand-supply analysis of products. This initiative proudly complements the "Make in India" endeavour. We are now delighted to present the "Made in India Research Report," meticulously crafted from the core of our robust 30,000-partner business ecosystem across the country.

Talking about the Indian IT industry scenario at present, the market is poised for a huge growth. And what is driving that – the Make in India initiative launched by the government a few years back. Almost every manufacturing company or every hardware company that is present in the country today has started manufacturing, although all of them are at a different scale at present. Now that every global company has begun manufacturing in the country, we felt that India lacked a dedicated, unbiased IT service research unit in India to specifically cater to the Indian customers. There are big global research organization brands present in the country today, and they have been doing a fantastic job for the last many years. But the current research being done is global centric and overlooks India's unique opportunities. There are also local complexities like the MNCs getting overly prioritized at times without giving much priority to Indian organizations at the domestic level. Indian partners and the channel do need local insights and intelligence, and global agencies often miss these in their reports.

The Indian market presents some important and unique features like, it is a price sensitive market, almost every region has a different kind of purchasing power and the demands are usually festival driven. Another aspect is the Mobile first approach, where we see a lot of sales and purchasing happening on our mobile phones. So this is again very typical of our domestic market. So by coming together with the channel community of resellers, distributors and system integrators, we are bringing forward this dedicated India specific survey that we believe will help them immensely. We want to be the most trusted source of information for our Indian partners by equipping them with local insights and strategic intelligence. The areas that we will cover include cyber security, the electronics & telecom channel ecosystem, enterprise business, custom research and consulting, to mention a few. Our research methodology will be based on primary research by talking to customers, taking surveys, and interviews. We will also take help from secondary research like taking existing market data, vendor reports, and government inputs. Our research reports will also dive into vertical-wise industry best practices and annual market reviews. We will also ensure to conduct workshops and webinars, and provide consulting and advisory to our customers.”

OUR PARTNERS 2025

SUPPORTING PARTNER

PRINCIPAL PARTNER

PLATINUM PARTNER

POWERED BY

GOLD PARTNERS

NETWORKING PARTNERS

DATA PRIVACY PARTNER

CYBER SECURITY PARTNER

MEDIA PARTNERS





From L-R: Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA; Bharat B Anand, Group CIO & CTO, Contec Global; Vijay Sethi, Chairman, Mentorkart and Crafsol Technologies; Anil Nama, CIO, CtrlS Datacenters & Cloud4C; Ashis Rout, Sr. Vice President (IT), Ex-HDFC Bank; and Sandeep Sengupta, Founder & Director, ISOAH Data Securities

Panel Discussion I

AI and the Future of Work

The first panel discussion at the event, moderated by Dr. Deepak Kumar Sahu, Editor-in-Chief of VARINDIA, brought together eminent CIOs and CTOs to deliberate on the topic, “AI and the Future of Work.” The distinguished panellists included Ashis Rout, Sr. Vice President (IT), Ex-HDFC Bank; Vijay Sethi, Chairman, Mentorkart and Crafsol Technologies; Bharat B Anand, Group CIO & CTO, Contec Global; Anil Nama, CIO, CtrlS Datacenters & Cloud4C; and Sandeep Sengupta, Founder & Director, ISOAH Data Securities.

Opening the session, Dr. Sahu underlined how rapid advancements in AI and cloud technologies are redefining job roles, organizational structures, and business models. He urged industry leaders to share their perspectives on how these innovations are impacting the businesses, setting the stage for a compelling conversation on how enterprises must evolve to stay relevant in the future of work.

ANIL NAMA, CIO, CTRLS DATACENTERS & CLOUD4C

“Artificial intelligence is the next phase in the evolution of IT—from data entry and ERP systems to a world driven by insights and action. Business data, once passively stored, now fuels predictions, alerts, and even automated responses, reducing downtime and improving efficiency. The real shift, however, is cultural: moving from manual trust to machine trust. Many still hesitate to act on AI-generated data without verification, especially in traditionally mechanical or electrical roles. Bridging this belief gap is critical. Additionally, the old approach of dumping data for later processing must evolve—data today must be clean, real-time, and accessible to everyone, not just experts. AI demands not only new skills but a transformed mindset. As organizations adopt AI, the challenge isn’t just technology—it’s enabling people to believe in it, act on it, and let data drive decisions. AI brings benefits—when we’re ready.”

VIJAY SETHI CHAIRMAN, MENTORKART AND CRAFTSOL TECHNOLOGIES

“AI is not a fad—it’s here to stay. It has moved beyond pilots and is now embedded in production systems, reshaping job roles across all levels. From automating data entry and quality checks using AI, RPA, and optical vision, to enabling predictive maintenance and supporting senior-level decision-making, AI is everywhere. It’s driving a cultural shift toward data-driven decision-making. New roles are emerging rapidly—prompt engineers, AI ethicists, model governance

experts, and cloud-AI architects. To successfully scale AI, start small, ensure your data is clean and reliable, and most importantly, focus on reskilling and building trust in data throughout the organization. Companies that fail to adapt risk being left behind in this ongoing transformation.”

BHARAT B ANAND, GROUP CIO & CTO, CONTEC GLOBAL

“AI began as flawed and merely imitative but has evolved into augmented and artificial intelligence, becoming a true disruptor. While reports predict 44% of jobs impacted over 3 decades, this disruption also creates opportunities—97 million new jobs are expected. The real focus must be on how we handle this change through upskilling and reskilling ourselves to stay relevant. Engaging with newer generations who inherently understand this tech is essential. Security remains critical; AI adoption requires defense-in-depth strategies with ongoing awareness since threats grow with new touchpoints. Data privacy is paramount and will drive new roles and regulations. For AI integration, start with high-impact, low-risk initiatives, then monitor, measure, and adjust continuously. Ultimately, AI is an opportunity, not a threat—it’s about how we embrace and adapt to it.”

ASHIS ROUT, SR. VICE PRESIDENT (IT), EX-HDFC BANK

“AI, like in my school days’ stories, often starts off unrelated or flawed but gradually gains precision. Human intelligence remains

superior since we created AI, but AI excels in scale, volume, and centralized tasks—especially critical in BFSI, where data is public money. AI plays a vital role in cybersecurity today, enabling predictive threat analysis and faster responses. With emerging regulations like DPDP, data privacy and zero-trust access are becoming mandatory, impacting how data is handled across organizations. Many projects fail due to low accuracy, so focusing on usable results is key. Compliance must extend beyond internal teams to vendors processing data. The future of work with AI demands continuous upskilling and learning to stay relevant in a rapidly evolving landscape.”

SANDEEP SENGUPTA, FOUNDER & DIRECTOR, ISOAH DATA SECURITIES

“Most companies are unprepared for the true risks of AI-driven automation. While people focus on tools like ChatGPT or Copilot, dangerous variants like WormGPT and FraudGPT operate in the shadows. Security shouldn’t stop at infrastructure—humans, especially top executives, are often the weakest links, traveling with unprotected devices. Many organizations are simply playing with AI, not using it meaningfully. Prompt engineering should be part of school education, but AI must not become our teacher—it often gives confidently wrong answers. Worse, if AI starts learning human traits like greed or violence, it could become a serious threat. To manage this risk, AI must be explainable, auditable, and traceable. Adopting standards like ISO 42001 and ensuring third-party compliance is essential. AI won’t replace humans—but it will replace lazy ones who fail to adapt.”



From L-R: Ms. S. Mohini Ratna, Editor of VARINDIA, Mr. Venkat Patnaik, CEO, Bonsai Enterprises, Mr. Dhananjay Rokde, CISO & Director- iManEdge Services, Dr. Harold D'Costa, President- Cyber Security Corporation, Mr. Deepak Kumar, Global Head - Cyber Defense, Infogain India, Mr. Nabendu Misra, Sr. AI Architect- EY and Mr. Jaspreet Singh (Partner), Clients & Markets Leader - Advisory Services, Grant Thornton Bharat LLP

Panel Discussion II

Navigating the Tech Trinity: Accelerating the Future with 5G, AI & IoT Advancements

We're at the cusp of a tech revolution where 5G, AI, and IoT are converging to transform how we live and work. To delve deeper into this transformative journey in the second panel discussion, **Ms. S. Mohini Ratna, Editor of VARINDIA**, highlighted how 5G's ultra-low latency, AI's analytical power, and IoT's smart device ecosystem are creating a hyper-connected, intelligent world. This synergy is driving innovation, reshaping industries, and enabling personalized, contextual digital experiences—redefining business models and enhancing everyday life for individuals and societies alike. While the scope of 5G, AI, and IoT is vast, the panelists certainly managed to touch on some of its most exciting and impactful dimensions.

DR. HAROLD D'COSTA PRESIDENT- CYBER SECURITY CORPORATION

He explained how AI is becoming central to both personal and professional decision-making. However, its effectiveness hinges on the quality and authenticity of data—be it supervised, unsupervised, or empirical. The integration of AI with 5G enhances speed, efficiency, and simplifies strategic processes. Yet, challenges remain, particularly from a legal and cybersecurity standpoint. Harold D'Costa emphasizes the need for a robust legal framework to manage risks associated with AI and IoT. He highlights the reluctance of CISOs and CIOs to allow third-party audits due to fear of exposing vulnerabilities. The legal system often lacks clarity on accountability when AI fails, making it crucial to redefine legal responsibilities and ensure a holistic risk mitigation approach.

DHANANJAY ROKDE CISO & DIRECTOR- IMANEDGE SERVICES

He highlighted how hyperconnected future is driven by 5G, AI, and IoT brings both innovation and unseen risks. These technologies enable real-time microtransactions, automation, and smart infrastructure, enhancing productivity. However, AI's reliance on the OODA loop—observe, orient, decide, and act—makes it vulnerable to bias, hallucinations, and unpredictability. In high-stakes environments like defense or smart factories, such flaws can result in critical failures. Rokde stressed that zero trust frameworks must be complemented by strong human oversight. While the combined power of 5G, AI, and IoT holds immense promise, we are not yet ready to entrust AI with executive decisions. Responsible, cautious adoption and governance are vital to ensure safe deployment.

JASPREET SINGH (PARTNER) CLIENTS & MARKETS LEADER - ADVISORY SERVICES, GRANT THORNTON BHARAT LLP

He shared that AI's growing presence in cybersecurity brings both promise and peril. While AI can enhance threat detection, attackers are often quicker in leveraging it. Organizations now spend more on combating AI-driven attacks than adopting AI itself. Yet, most CISOs lack visibility into how many AI engines operate within their systems. Misuse and overhype of AI have become common, with vague use cases clouding judgment. Investments are shifting from detection to protection and now to response. Weak legal frameworks and the rising risk of deepfakes—like the false Pentagon attack photo—expose glaring vulnerabilities. Without clear regulation, defined AI use cases, and responsible deployment, organizations risk being blindsided in an increasingly AI-driven, hyperconnected world.

VENKAT PATNAIK, CEO, BONSAI ENTERPRISES

With the rapid rise of 5G, AI, and IoT technologies he raised an important question: are we genuinely ready? While these innovations promise speed, automation, and intelligence, many sectors—especially healthcare, defense, and MSMEs—are yet to see meaningful adoption. AI, in particular, is often used as a buzzword rather than for impactful, decision-making applications. With 5G amplifying speed and connectivity, the potential for security threats also multiplies, especially in the loosely controlled IoT space. The integration of these technologies demands a deeper understanding and strategic deployment, not just excitement. Without it, we risk creating more chaos than progress in critical industries.

MR. NABENDU MISRA, SR. AI ARCHITECH- EY

He emphasized the need for a tailored tech strategy to unlock the full potential of 5G, AI, and IoT in India. While countries like Singapore and the Philippines are advancing with AI-powered innovations like autonomous vehicles and smart logistics, India lags in realizing its smart city ambitions. Key challenges include inadequate infrastructure, absence of localized use cases, and weak cybersecurity frameworks. Critical threats such as IoT vulnerabilities, poor encryption standards, and fragile IT-OT integration increase risks like espionage, grid outages, and data breaches. To harness next-gen technologies effectively, India must focus on region-specific deployments, strengthen IoT security, and develop adaptive, scalable smart city frameworks that align with local needs and risks.

DEEPAK KUMAR, GLOBAL HEAD - CYBER DEFENSE AT INFOGAIN INDIA,

He described AI in cybersecurity as a double-edged sword—strengthening both defense and attack capabilities. AI-generated phishing emails now mimic human language with alarming accuracy, making detection difficult and increasing credential theft. Even novice users can create malware using AI tools. On the flip side, AI enhances security operations by enabling proactive threat detection, minimizing false alerts, and supporting faster decisions. To build resilient infrastructure, organizations are adopting high-availability systems, geo-segmentation, zero trust models, and micro-segmentation. Regular cyber drills, business continuity testing, and engaging all stakeholders, including third-party vendors, are vital. Cybersecurity today demands a holistic approach—where people, technology, and processes align to defend against evolving threats.



From L-R: Gyana Ranjan Swain, Consulting Editor, VARINDIA; Arvind Saxena, CMO- NEC India; Ritesh Dhawan, Marketing Head (India)- Redington Ltd.; Sanjay Chaudhary, Head of Enterprise Marketing- SAP; and Vinny Sharma, Marketing Director for APJ & MEA – Securonix

Panel Discussion III

Safeguarding Brand Trust in the Deepfake Era

The third panel discussion titled - Safeguarding Brand Trust in the Deepfake Era was moderated by Gyana Ranjan Swain, Consulting Editor, VARINDIA. He set the stage ready by discussing how deepfakes and data privacy threats erode trust and democratic processes. “This issue has been plaguing us since the entry of AI and other innovative technologies. Malicious use of personal data is fueling realistic misinformation, and manipulating public perception towards a particular person, entity or an issue. This challenges digital integrity and informed discourse and demands urgent solutions.

The panellists who joined the discussion included Arvind Saxena, CMO- NEC India; Ritesh Dhawan, Marketing Head (India)- Redington Ltd.; Sanjay Chaudhary, Head of Enterprise Marketing- SAP; and Vinny Sharma, Marketing Director for APJ & MEA – Securonix.

VINNY SHARMA
MARKETING DIRECTOR FOR
APJ & MEA – SECURONIX

On recounting her first instance with deepfake, Vinny explained how a WhatsApp message from her company CEO, Nayaki Nayyar got her thinking if it was a real or a fake one. “On seeing the CEO’s WhatsApp profile picture, I opened the message where she was asking for some information. She was not supposed to touch base with me directly as there was no ongoing project. Had there been any project, she would definitely reach out to me. It was not late before realizing that somebody was impersonating her in the pretext of extracting some information, and this started happening with multiple colleagues of mine. So when such instances happen, is a normal consumer aware about it or do they know how to react to it, that is a big question that comes up.”

RITESH DHAWAN
MARKETING HEAD (INDIA)-
REDINGTON LTD

Ritesh cited an instance of deepfake of his own. “A couple of months back, there was a rock concert happening in Mumbai. The place was packed with more than 1500 people with very high security and we were allowed to carry along very few things inside. So in the outer periphery of this stadium, there were some food and refreshment stalls

put up. Out of the seven or eight different stalls, there was one particular stall which was selling coffee and it had a very relatable, circular green logo with the mermaid in the center. The logo drew a very major reference to a certain big global coffee brand and we instantly knew it was not genuine. Five out of 10 people walking into that stall were ready to buy a coffee or a beverage over somebody which is not impersonating any brand. And I think that speaks volumes about consumer behavior and how this whole deepfake industry is feeding over global brands creating over millions of dollars and resources.”

SANJAY CHAUDHARY,
HEAD OF ENTERPRISE
MARKETING- SAP

On the growing cases of deepfake Sanjay said, I feel that as a marketer, you have three ‘Rs’ to manage – the third R, which we sometimes keep as number one, is Revenue, but that’s a byproduct. The other two ‘Rs’ are Relationship and Reputation. Reputation plays a very, very important role and if that trust or relationship is compromised, then you will have a difficult time to rebuild that. So there is a huge implication of any form of reputation damage that can impact the brand in the long run. So it is very critical to make sure that you protect your brand reputation above everything else. Deepfake was so common in the political scenarios,

among celebrities, but this has now started to happen in the B2B space as well. Imagine the implications a fake earning call or a fake interview of an analyst will have on a company. There is no denying that you cannot control this but you can keep smarter and smarter to prevent this. There will come a point of time when humans will not be able to match the machines but we have to use these machine to counter these threats.”

ARVIND SAXENA
CMO- NEC INDIA

In this digital age, with the threat always looming over one’s head to manage brand validation and customer trust, Arvind said that NEC has always been innovating, and the company’s values and culture has always stood the test of time. “For us, security, specifically cyber security has been placed across all possible channels of communication as risk number one and we have stitched together the required SOP or a guidebook to guide us along. Marketing or branding, communication, content creation till yesterday used to be limited to just a bunch of a few. Today we understand that everyone who owns a smartphone is a pseudo marketer and they have the same set of tools, which can be played around. Sensing this as a risk, we therefore believe that in order to stay ahead of threats like deepfake, we can simulate some of these scenarios in our own environment.”



EMINENT CIOs OF INDIA 2025

102 Eminent CIOs 2025-26 Honored at Infotech Forum 2025

Digital transformation today is far more than a technological upgrade—it is a strategic journey reshaping business models, operational culture, and customer engagement across industries. It demands vision, agility, and the courage to embrace emerging technologies while navigating unprecedented disruption. In an era defined by cybersecurity challenges, AI-led innovation, rapid cloud adoption, and surging customer expectations, India’s technology leaders are at the forefront, ensuring that organizations remain resilient, competitive, and future-ready. They are not only managing IT but also orchestrating growth, innovation, and enterprise-wide transformation. VARINDIA is proud to celebrate these leaders—the CIOs, CTOs, CXOs, and CISOs—who have risen to these challenges with foresight and determination. Their contributions span architecting robust digital strategies, fortifying cyber resilience, and fostering innovation ecosystems that empower their enterprises to thrive in a hyperconnected world. The “Eminent CIOs of India 2025” recognition honours this select group of professionals who have redefined the role of technology leadership. They have turned disruption into opportunity, driven sustainable growth, and ensured operational continuity, even amid a volatile global landscape.

These individuals are more than IT leaders—they are strategists, change agents, and visionaries shaping the future of Indian business and technology. It is our privilege to showcase their achievements and acknowledge the vital role they play in advancing India’s digital economy. The winners, this year are...



ADV (DR.) PRASHANT MALI, PRACTICING LAWYER, BOMBAY HIGH COURT



DR. ARINDAM SARKAR, RAMAKRISHNA MISSION VIDYAMANDIRA, BELUR MATH



DR. BALVINDER SINGH BANGA, V-TRANS INDIA LTD.



DR. HAROLD D’COSTA, CYBER SECURITY CORPORATION



DR. PAVAN DUGGAL, INTERNATIONAL COMMISSION ON CYBER SECURITY LAW



DR. RAVI MUNDRA, TECHNOCRACY PVT. LTD.



DR. SUSHIL MEHER, AIIMS



AJAY YADAV, SBL HOMEOPATHY



AMIT ARORA, SHR LIFESTYLES (P) LTD.



ARVIND SINGH PURAVANKARA LIMITED



ASHIS ROUT
HDFC BANK



ASHISH GUPTA, NEC
CORPORATION INDIA PVT. LTD.



ANAND RUHELA,
SGT UNIVERSITY



ANIL NAMA,
CTRLS DATACENTERS



ARVIND KUMAR, PATHKIND
DIAGNOSTICS PVT. LTD.



BALWANT SINGH, DHARAMPAL
SATYAPAL LIMITED (DS GROUP)



BHARAT B ANAND, CONTEC GLOBAL



BHAVESH KUMAR, SK FINANCE



DEEPAK KUMAR, INFOGAIN



DEEPAK KUMAR PANDA, NATIONAL
HIGHWAY INFRA TRUST



DHANANJAY CHANDRASHEKHAR
ROKDE, IMANEDGE SERVICES



DINESH KAUSHIK, SHARDA
MOTOR INDUSTRIES LTD.



FARMAN KHALID, EMAAR INDIA



GANESH VISWANATHAN, ASSISTO
TECHNOLOGIES PVT. LTD.



GAURAV VIJ, HOOLIV.COM



GAURAV VYAS, STOVEK INDUSTRIES LTD. (SPG PRINTS)



GOLOK KUMAR SIMLI, PASSPORT SEVA PROGRAMME, GOVT. OF INDIA



J. P. DWIVEDI, RAJIV GANDHI CANCER INSTITUTE & RESEARCH CENTRE, ROHINI



KRIPADYUTI SARKAR, AMBUJANEOTIA GROUP



KUMAR PRASOON, TWYN



KUSHAL KUMAR VARSHNEY, ACME



MAJOR GENERAL DR. DILAWAR SINGH, GLOBAL ECONOMIST FORUM



MOHAN SHAH, CLAIMPRO ASSIST PVT. LTD.



MRINMOY MUKHERJEE, PATTON INTERNATIONAL LTD.



NITIN DHINGRA, INDIRA IVF HOSPITAL LTD.



PANKAJ MITTAL, DIGIZEN CONSULTING



PRADIPTA PATRO, KEC INTERNATIONAL LTD. (RPG GROUP CO.)



PRASENJIT MUKHERJEE, JWIL INFRASTRUCTURE LTD.



DR. PRINCE JOSEPH, NEST GROUP AND SFO TECHNOLOGIES



RAMKUMAR MOHAN, AIR WORKS INDIA ENGINEERING PVT. LTD.



RAVI RAZDAN, JYOTHY LABS



ROHIT KACHROO, OMNI CYBERX PVT. LTD.



SANDEEP SENGUPTA, ISOAH DATA SECURITIES PVT. LTD.



SANJAY KUMAR DAS, DEPT. OF IT & ELECTRONICS, GOVT. OF WEST BENGAL



SANJEEV SAXENA, IFB INDUSTRIES LTD.



SHIBU V KURIAN, 7 SAGES SOLUTIONS



SIVAKUMAR NANDIPATI, FEDBANK FINANCIAL SERVICES



SUBROTO KUMAR PANDA, ANAND AND ANAND



SUJOY BRAHMACHARI, ROSMERTA TECHNOLOGIES LTD.



SUNIL GUBRANI, FRATELLI WINES



TAPAS SAHA, VEEDOL CORPORATION LTD.



VIJAY SETHI, MENTORKART AND CRAFTSOL TECHNOLOGIES



VINOD KUMAR GUPTA, PAYTM MONEY



VIVEKANANDA NASKAR, PROTEGRITY INDIA



RECEIVING ON BEHALF OF JASPREET SINGH (PARTNER), GRANT THORNTON BHARAT LLP

ADV (DR.) PRASHANT MALI	PRESIDENT	CYBER LAW CONSULTING (ADVOCATES & ATTORNEYS)
DR. ARINDAM SARKAR	HOD & ASSISTANT PROFESSOR,	RAMAKRISHNA MISSION VIDYAMANDIRA, BELUR MATH
DR. BALVINDER SINGH BANGA	GROUP CTO,	V-TRANS INDIA LTD.
DR. CHITRANJAN KESARI	HEAD OF IT,	N R AGARWAL INDUSTRIES LTD.
DR. HAROLD D’COSTA	PRESIDENT,	CYBER SECURITY CORPORATION
DR. JAGANNATH SAHOO	CISO	INOX WIND LTD.
DR. MAKARAND SAWANT	DIRECTOR & CTO,	SEAFB
DR. PANKAJ DIKSHIT	CTO	GEM, GOVT. OF INDIA
DR. PAVAN DUGGAL	CHAIRMAN,	INTERNATIONAL COMMISSION ON CYBER SECURITY LAW
DR. RAKSHIT TANDON		CYBER SECURITY EVANGELIST
DR. RAVI MUNDRA	VICE PRESIDENT & CO-OWNER FOR PRODUCT DEVELOPMENT (CYBER),	TECHNOCRACY PVT. LTD.
DR. SANDIP PRADHAN	CIO	CENTURY PLYBOARDS (INDIA) LTD.
DR. SUSHIL MEHER	HEAD – IT,	AIIMS
DR. VINEET BANSAL	CIO,	SURYA ROSHNI LTD.
DR. YUSUF HASHMI	GROUP CHIEF INFORMATION SECURITY OFFICER,	JUBILANT BHARTIA GROUP
AJAY KUMAR AJMERA	CIO	ROCKMAN INDUSTRIES LTD.
AJAY YADAV	HEAD –IT, SECURITY & E-COMMERCE,	SBL HOMEOPATHY
AMIT ARORA	CIO	SHR LIFESTYLES (P) LTD.
AMIT KAPOOR	GROUP HEAD IT/APPLICATION,	PRISTINE GROUP
ANAND KUMAR SINHA	CIO & GLOBAL HEAD IT,	BIRLASOFT (C K A BIRLA GROUP)
ANAND RUHELA	HEAD – IT,	SGT UNIVERSITY
ANIL NAMA	CIO	CTRLS DATACENTERS
ANIL SHARMA	SENIOR DIRECTOR S&T (AMESA),	PEPSICO INC.
ARCHIE JACKSON	VP - CIO & CISO,	INCEDO INC.
ARVIND KUMAR	AVP-IT,	PATHKIND DIAGNOSTICS PVT. LTD.
ARVIND SINGH	CHIEF TECHNOLOGY & PRODUCT OFFICER,	PURAVANKARA LIMITED
ASHIS ROUT	SR. VICE PRESIDENT - IT,	HDFC BANK
ASHISH GUPTA	CIO & CISO,	NEC CORPORATION INDIA PVT. LTD.
ASHOK RAMCHANDRA JADE	GLOBAL CIO (CIC),	KIRLOSKAR BROTHERS LTD.
BALWANT SINGH	GROUP CISO & DPO,	DHARAMPAL SATYAPAL LIMITED (DS GROUP)
BHARAT B ANAND	GROUP CIO AND CTO,	CONTEC GLOBAL
BHASKAR RAO	CISO	BHARAT CO-OPERATIVE BANK (MUMBAI) LTD.
BHAVESH KUMAR	CISO & DPO,	SK FINANCE
BHOOPENDRA SOLANKI	CHIEF INFORMATION OFFICER,	SAKRA WORLD HOSPITAL
BIBHAS SEN CHOUDHURI	DGM – IT,	AMBUJA NEOTIA HEALTHCARE VENTURE LTD.
BIPRADAS BANDYOPADHYAY	HEAD OF IT,	ZUARI INFRAWORLD INDIA LTD.
BRIJESH SINGH	ADGP & PRINCIPAL SECRETARY TO CHIEF MINISTER,	GOVT. OF MAHARASHTRA
DEBOJYOTI MITRA	HEAD – IT,	POLAR ELEKTRIC LTD.
DEEPAK KUMAR	HEAD – CYBER DEFENSE,	INFOGAIN
DEEPAK KUMAR PANDA	GM - IT	NATIONAL HIGHWAY INFRA TRUST
DHANANJAY CHANDRASHEKHAR ROKDE	DIRECTOR & CTSO,	IMANEDGE SERVICES
DINESH KAUSHIK	CIO	SHARDA MOTOR INDUSTRIES LTD.
DOMINIC VIJAY KUMAR	PRESIDENT & HEAD OF TECHNOLOGY,	NAMDEV FINVEST PVT. LTD.
FARMAN KHALID	HEAD IT / CHIEF DIGITAL OFFICER,	EMAAR INDIA
GANESH VISWANATHAN	PRESIDENT,	ASSISTO TECHNOLOGIES PVT. LTD.
GAURAV VIJ	CIO	HOOLIV.COM
GAURAV VYAS	HEAD IT,	STOVEK INDUSTRIES LTD. (SPG PRINTS)
GOLOK KUMAR SIMLI	CTO	PASSPORT SEVA PROGRAMME, GOVT. OF INDIA

HARIHARAN SUBRAMANIAN	VICE PRESIDENT - INFORMATION TECHNOLOGY,	SHRIRAM PROPERTIES
HARMIT SINGH MALHOTRA	CTO	NDTV- PROFIT
HARSH KUMAR ARORA	GROUP HEAD IT,	HINDUSTAN POWER PROJECTS
J. P. DWIVEDI	CIO	RAJIV GANDHI CANCER INSTITUTE & RESEARCH CENTRE, ROHINI
JASPREET SINGH (PARTNER)	CLIENTS & MARKETS LEADER - ADVISORY SERVICES,	GRANT THORNTON BHARAT LLP
KHUSHBU JAIN	PARTNER	ARK LEGAL
KRIPADYUTI SARKAR	CIO	AMBUJANEOTIA GROUP
KUMAR PRASOON	GROUP CIO,	TWYN
KUSHAL KUMAR VARSHNEY	AVP & HEAD IT,	ACME
LAKSHMANA VADAGA	CIO	MIND NERVES TECHNOLOGY PVT. LTD.
LALIT TRIVEDI	HEAD INFORMATION SECURITY,	FLEXM
LEE NOCON	CO-FOUNDER AND CTO,	DATA SAFEGUARD INDIA
MAJOR GENERAL DR. DILAWAR SINGH	SR. VICE PRESIDENT	GLOBAL ECONOMIST FORUM
MOHAN SHAH	CTO	CLAIMPRO ASSIST PVT. LTD.
MRINMOY MUKHERJEE	CIO (AVP-IT),	PATTON INTERNATIONAL LTD.
NARAYAN BASAK	CISO & HEAD IT OPERATIONS,	TCG DIGITAL SOLUTIONS PVT. LTD.
NIKHIL KUMAR NIGAM	DIRECTOR TECHNOLOGY - GLOBAL OPERATIONS,	MSM UNIFY
NITIN DHINGRA	CHIEF TECHNOLOGY OFFICER,	INDIRA IVF HOSPITAL LTD.
PANKAJ MITTAL	FOUNDER & CEO,	DIGIZEN CONSULTING
PARTHA PROTIM MONDAL	CIO	BERGER PAINTS INDIA LTD.
PARVEEN KUMAR SHARMA	VICE PRESIDENT – IT,	MIGSUN GROUP
PRADIPTA PATRO	HEAD - CYBER SECURITY & IT PLATFORM,	KEC INTERNATIONAL LTD. (RPG GROUP CO.)
PRADNYA UMAJI MANWAR	SR. DIRECTOR, INFORMATION SECURITY AND CYBERSECURITY,	SUTHERLAND
PRAGNESH MISTRY	HEAD OF IT AND CYBER SECURITY,	RPG ENTERPRISES LTD. (RPG GROUP)
PRAMOD KUMAR MOHAPATRA	GM - IT & CISO,	NATIONAL HIGHWAYS AUTHORITY OF INDIA
PRASENJIT MUKHERJEE	CIO & CDO,	JWIL INFRASTRUCTURE LTD.
PRINCE JOSEPH	GROUP CIO,	NEST GROUP AND SFO TECHNOLOGIES
PROF. TRIVENI SINGH	CHAIRPERSON & CHIEF MENTOR,	FUTURE CRIME RESEARCH FOUNDATION
PUNEESH LAMBA	CIO	CMR GREEN TECHNOLOGIES LTD.
RAMKUMAR MOHAN	SR. VP & CIO,	AIR WORKS INDIA ENGINEERING PVT. LTD.
RAVI RAZDAN	DIRECTOR – IT & HR,	JYOTHY LABS
RITESH BHATIA	INCIDENT RESPONSE SPECIALIST & FOUNDER,	V4WEB CYBERSECURITY
ROHIT KACHROO	CO-FOUNDER AND CTO,	OMNI CYBERX PVT. LTD.
SANDEEP SENGUPTA	MANAGING DIRECTOR,	ISOAH DATA SECURITIES PVT. LTD.
SANDIIP KOTHAARI	CTO,	SPECIALITY GROUP
SANJAY KUMAR DAS	STATE INFORMATION SECURITY OFFICER,	DEPT. OF IT & ELECTRONICS, GOVT. OF WEST BENGAL
SANJEEV SAXENA	GM – IT,	IFB INDUSTRIES LTD.
SANJEEV SINHA	PRESIDENT – IT & DIGITALIZATION,	INDIA POWER
SAURABH GUGNANI	GLOBAL HEAD OF CYBERSECURITY ENGINEERING, PROJECTS AND ARCHITECTURE,	TMF GROUP
SAURABH GUPTA	GROUP CHIEF DIGITAL AND INFORMATION OFFICER,	GUJARAT FLUOROCHEMICALS LTD.
SHIBU V KURIAN	CHIEF INFORMATION & TECHNOLOGY OFFICER,	7 SAGES SOLUTIONS
SIVAKUMAR NANDIPATI	CDO	FEDBANK FINANCIAL SERVICES
SOURAV DAS	GROUP CHIEF OF DIGITAL & IT,	RUPA AND COMPANY LTD.
SUBROTO KUMAR PANDA	CIO & CTO,	ANAND AND ANAND
SUJOY BRAHMACHARI	CIO & CISO - SMART CARD BUSINESS,	ROSMERTA TECHNOLOGIES LTD.

SUNIL GUBRANI	HEAD IT SECURITY & INFRA,	FRATELLI WINES
TAPAS SAHA	HEAD IT,	VEEDOL CORPORATION LTD.
TEJAS SHAH	HEAD IT INFRA,	PRINCE PIPES AND FITTINGS LTD.
V RANGANATHAN IYER	CIO & EVP-IT,	JBM GROUP
VIJAY SETHI	CHAIRMAN	MENTORKART AND CRAFTSOL TECHNOLOGIES
VIKAS SHARMA	HEAD - IT,	TCI EXPRESS LTD.
VINOD KUMAR GUPTA	CISO AND DPO,	PAYTM MONEY
VIVEKANANDA NASKAR	DIRECTOR - IT,	PROTEGRITY INDIA
YOGENDRA SINGH	HEAD - IT & SAP,	BARISTA

DELEGATES IN THE EVENT



SOLUTION DISPLAY KIOSKS



IRIS | DELL



SONICWALL



POSTGRESPRO



FACEOFF TECHNOLOGIES PVT. LTD.



ALLIED TELESYS INDIA PVT. LTD.



ACRONIS



PURESTORAGE | CISCO



REDINGTON



CONTEXT



CP PLUS

MOST TRUSTED COMPANIES

Top 25 Trusted Tech Brands 2025-26 Honored at Infotech Forum 2025

In an era where competition is intense, trust has emerged as a core driver of brand credibility and long-term success. Companies that consistently deliver value, uphold their commitments, and enhance customer experiences stand out in the marketplace.

The “Most Trusted Companies in India 2025” initiative, led by VARINDIA and the Brand Book editorial team, acknowledges technology brands that have earned the confidence of consumers while contributing meaningfully to India’s digital growth.

Featured in the 14th edition of the Brand Book, the 25 selected companies were identified through an extensive survey and in-depth evaluation across several key performance indicators. This recognition highlights the leading tech brands steering India’s digital transformation journey.



CISCO SYSTEMS INDIA PVT. LTD.



DELL TECHNOLOGIES PVT. LTD.



GOOGLE INDIA PVT. LTD.



HEWLETT PACKARD ENTERPRISES INDIA PVT. LTD.



INGRAM MICRO INDIA PVT. LTD.



IBM INDIA PVT. LTD



ORACLE INDIA PVT. LTD.



REDINGTON LTD.



SAMSUNG INDIA ELECTRONICS PVT. LTD.



TATA CONSULTANCY SERVICES LIMITED



WIPRO LTD.

ADOBE SYSTEMS INDIA PVT. LTD.
APPLE INDIA PVT.LTD.
AWS INDIA

BHARTI AIRTEL LIMITED
BROADCOM INDIA PVT. LTD.
CISCO SYSTEMS INDIA PVT. LTD.

DELL TECHNOLOGIES PVT. LTD.
GOOGLE INDIA PVT. LTD.
HCL TECHNOLOGIES LIMITED
HEWLETT PACKARD ENTERPRISES INDIA PVT. LTD.
IBM INDIA PVT. LTD.
INFOSYS LIMITED
INGRAM MICRO INDIA PVT. LTD.
INTEL TECHNOLOGY PVT. LTD.
MICROSOFT CORPORATION (I) PVT.LTD.
NVIDIA GRAPHICS INDIA PVT. LTD.

ORACLE INDIA PVT. LTD.
QUALCOMM INDIA PVT. LTD.
REDINGTON LTD.
RELIANCE JIO INFOCOMM LIMITED
SALESFORCE INDIA PVT. LTD.
SAMSUNG INDIA ELECTRONICS PVT. LTD.
TATA CONSULTANCY SERVICES LIMITED
TECH MAHINDRA LTD.
WIPRO LTD.

MOST ADMIRIED BRANDS

50 Admired Tech Brands 2025-26 Recognized for Innovation & Excellence

In a competitive business landscape, trust, innovation, and customer satisfaction set leading brands apart. The “Most Admired Brands in India 2025” initiative by VARINDIA and the Brand Book editorial team recognizes technology brands that have earned consumer loyalty and advanced India’s IT journey.

The selection of 50 standout brands is based on a transparent process involving nationwide consumer surveys, expert evaluations, and analysis of brand purpose, innovation, and market impact.

Now featured in the 14th edition of the Brand Book, these brands are honored for their consistent quality, engagement, and technological leadership—solidifying their status as the most admired names shaping India’s digital future.



ACER INDIA PVT. LTD.



ALCATEL- LUCENT ENTERPRISE



ALLIED TELESYS INDIA PVT. LTD.



AMD INDIA PVT. LTD.



KSG TECHNOLOGIES PVT. LTD. (CADYCE)



COMMSCOPE NETWORKS INDIA PVT LTD.



CONTENTVERSE BY COMPUTHINK



CP PLUS INDIA PVT. LTD.



CYBLE INFOSEC INDIA PVT. LTD.



D-LINK INDIA LTD.



ESET ASIA PTE. LTD



FORTINET TECHNOLOGIES INDIA PVT. LTD.



HP INC.



INFLOW TECHNOLOGIES PVT. LTD.



IVALUE INFOSOLUTIONS PVT. LTD.



JABRA CONNECT INDIA PVT. LTD.



JUNIPER NETWORKS SOLUTION INDIA PVT LTD.



KYNDRYL INDIA



LENOVO INDIA PVT. LTD.



MICRON SEMICONDUCTOR TECHNOLOGY INDIA PRIVATE LIMITED



NEC CORPORATION INDIA PVT. LTD



NETAPP INDIA PVT. LTD.



PALO ALTO NETWORKS (INDIA) PVT. LTD.



POSTGRESSPRO



PRAMA INDIA PVT. LTD.



**QUALYS SECURITY
TECHSERVICES PVT. LTD.**



REDHAT INDIA PVT. LTD.



RUBRIK INDIA PVT. LTD.



SAVEX TECHNOLOGIES PVT. LTD.



**SEAGATE TECHNOLOGY
HDD INDIA PVT. LTD.**



SECURONIX INDIA PVT. LTD.



SIFY TECHNOLOGIES LTD.



**SONICWALL TECHNOLOGY
SYSTEMS INDIA PVT. LTD.**



**SOPHOS TECHNOLOGIES
PRIVATE LIMITED**



SUPERTRON ELECTRONICS PVT. LTD.



**TECH DATA ADVANCED
SOLUTIONS INDIA PVT. LTD.**



**TENABLE NETWORK SECURITY
INDIA PVT. LTD.**



TRELLIX INC.



VEEAM SOFTWARE PVT. LTD.



VERSA NETWORKS INDIA PVT. LTD.



VIEWSONIC TECHNOLOGIES INDIA PVT LTD



PURE STORAGE INDIA PVT. LTD.



HARITASHA ELECTRONICS



TP-LINK INDIA PVT. LTD.

MOST ADMIRIED BRANDS

ACER INDIA PVT. LTD.
ALCATEL- LUCENT ENTEREPRISE
ALLIED TELESYS INDIA PVT. LTD.
AMD INDIA PVT. LTD.
KSG TECHNOLOGIES PVT. LTD. (CADYCE)
CANON INDIA PVT. LTD.
COMMSCOPE NETWORKS INDIA PVT LTD.
CONTENTVERSE BY COMPUTHINK
CP PLUS INDIA PVT. LTD.
CROWDSTRIKE INDIA PVT. LTD.
CYBLE INFOSEC INDIA PVT. LTD.
D-LINK INDIA LTD.
ESET ASIA PTE. LTD
FORTINET TECHNOLOGIES INDIA PVT. LTD.
HARITASHA ELECTRONICS
HITACHI VANTARA INDIA PVT. LTD.
HP INC.
INFLOW TECHNOLOGIES PVT. LTD.
IVALUE INFOSOLUTIONS PVT. LTD.
JABRA CONNECT INDIA PVT. LTD.
JUNIPER NETWORKS SOLUTION INDIA PVT LTD.
KASPERSKY INDIA
KYNDRYL INDIA
LENOVO INDIA PVT. LTD.
MICRON SEMICONDUCTOR TECHNOLOGY INDIA PRIVATE LIMITED

NEC CORPORATION INDIA PVT. LTD
NETAPP INDIA PVT. LTD.
NUTANIX TECHNOLOGIES INDIA PVT. LTD.
PALO ALTO NETWORKS (INDIA) PVT. LTD.
PICUS SECURITY PVT. LTD.
POSTGRESSPRO
PRAMA INDIA PVT. LTD.
PURESTORAGE INDIA PVT. LTD.
QUALYS SECURITY TECHSERVICES PVT. LTD.
REDHAT INDIA PVT. LTD.
RUBRIK INDIA PVT. LTD.
SAVEX TECHNOLOGIES PVT. LTD.
SEAGATE TECHNOLOGY HDD INDIA PVT. LTD.
SECURONIX INDIA PVT. LTD.
SIFY TECHNOLOGIES LTD.
SONICWALL TECHNOLOGY SYSTEMS INDIA PVT. LTD.
SOPHOS TECHNOLOGIES PRIVATE LIMITED
SUPERTRON ELECTRONICS PVT. LTD.
TECH DATA ADVANCED SOLUTIONS INDIA PVT. LTD.
TENABLE NETWORK SECURITY INDIA PVT. LTD.
TP-LINK INDIA PVT. LTD.
TRELLIX INC.
VEEAM SOFTWARE PVT. LTD.
VERSA NETWORKS INDIA PVT. LTD.
VIEWSONIC TECHNOLOGIES INDIA PVT. LTD.
ZSCALER SOFTECH INDIA PVT. LTD.

MOST INFLUENTIAL CMOs IN INDIA

India’s Top 11 CMOs 2025 Honored for Business Impact

Digital technology has transformed the role of the CMO, elevating it from brand stewardship to a key driver of enterprise strategy. Modern CMOs now lead business growth by harnessing data, technology, and customer insights to boost revenue and profitability across functions.

They play a critical role in digital transformation—adopting advanced analytics and tools to stay ahead of market shifts, improve marketing efficiency, and enhance customer engagement.

The 2025 edition of the Brand Book proudly features India’s 50 Most Influential CMOs from the technology sector, recognizing their visionary leadership and strategic impact. Among them, 11 CMOs have been specially honored as India’s Most Influential CMOs for 2025-26, reflecting their exceptional contributions to the evolving business landscape.



MR. DEEPAK MATHUR, HEAD
MARKETING (INDIA & SAARC)
PALO ALTO NETWORKS



MR. PUNEET CHADHA,
CHIEF MARKETING OFFICER
REDINGTON INDIA LTD.



MR. KUSHAGRA SHARMA ,
HEAD OF MARKETING (INDIA &
SAARC), VEEAM SOFTWARE



MR. ARVIND SAXENA
CMO
NEC INDIA



RECEIVING ON BEHALF OF
MR. RAHUL SINGH, VP & HEAD OF
MARKETING, SAP INDIA PVT. LTD.



RECEIVING ON BEHALF OF
MR. DEBUR S BALAMURLI, V.P.-
MARKETING & CUSTOMER
EXPERIENCE, KYNDRYL INDIA



MS. VINNY SHARMA, SR.
MARKETING DIRECTOR- APJ,
EUROPE & EMEA, SECURONIX



RECEIVING ON BEHALF OF
MR. ANUPAM SAH, G.M- MARKETING
ADITYA INFOTECH PVT. LTD.



RECEIVING ON BEHALF OF
MS. RIMI DAS, HEAD OF MARKETING
PURE STORAGE INDIA PVT. LTD.

ARVIND SAXENA	NEC CORPORATION INDIA PVT. LTD.
DEEPAK MATHUR	PALO ALTO NETWORKS
KUSHAGRA SHARMA	VEEAM SOFTWARE
MAYURI SAIKIA	DELL TECHNOLOGIES
KARTHIK SATHURAGIRI	MARKETING DIRECTOR
PUNEET CHADHA	REDINGTON INDIA LTD.
RAHUL SINGH	VP & HEAD OF MARKETING
RIMI DAS	PURE STORAGE INDIA PVT. LTD.
VINNY SHARMA	SECURONIX
DEBUR S BALAMURLI	KYNDRYL INDIA
ANUPAM SAH	ADITYA INFOTECH PVT. LTD.



MOST PROMISING PARTNERS

26 Most Promising Partners 2025-26 Recognized at Infotech Forum 2025

In today’s rapidly evolving technology ecosystem, Value-Added Resellers (VARs) and Channel Partners are not just intermediaries—they are the driving force behind business transformation. By combining deep industry expertise with robust alliances with global vendors, they deliver tailored, future-ready solutions that help enterprises navigate digital disruption, achieve operational efficiency, and stay competitive in a demanding market.

These partners act as trusted advisors, enabling organizations to embrace emerging technologies such as cloud, cybersecurity, AI, and next-generation infrastructure. Their ability to integrate, customize, and support solutions ensures that businesses can scale faster while reducing complexity and risk. By bridging the gap between innovation and execution, VARs and Channel Partners have become critical enablers of India’s digital growth story.

To celebrate their contributions, VARINDIA proudly presents the “Most Promising Partners of 2025” awards, recognizing 25 outstanding VARs and partners across five categories. These winners have demonstrated remarkable differentiation through innovation, customer-centricity, and measurable impact—extending the reach of technology vendors and empowering enterprises with transformative capabilities.

These awards not only acknowledge excellence but also underscore the pivotal role of the partner ecosystem in shaping India’s technology future. By driving adoption of cutting-edge solutions and delivering exceptional customer experiences, these partners continue to redefine how technology fuels growth and resilience in the digital era.

As VARINDIA honors these achievers, we celebrate their dedication, leadership, and their invaluable role in powering India’s journey toward a digitally empowered economy. The winners, this year are...



ACMA COMPUTERS LTD.



BM INFOTRADE PVT. LTD.



DIAMOND INFOTECH PVT. LTD.



ENSONIC COMPUTECH PVT. LTD.



E-SOFT ONLINE



FORTUNE MARKETING PVT. LTD.



FRUX TECHNOLOGIES PVT. LTD



IRIS GLOBAL SERVICES PVT. LTD.



IVALUE INFOSOLUTIONS



LDS INFOTECH PVT. LTD.



**NETPOLEON SOLUTIONS
INDIA PVT. LTD.**



**NIVESHAN TECHNOLOGIES
INDIA PVT. LTD.**



**PENTAGON SYSTEM AND
SERVICES PVT. LTD.**



RAH INFOTECH PVT. LTD.



RASHI PERIPHERALS LIMITED



REDINGTON LIMITED



SANGHVI INFOTECH PVT. LTD.



SHIVAAMI CLOUD SERVICES PVT. LTD.



SUPERTRON ELECTRONICS (SEPL)



TDM GROUP



**TECH DATA ADVANCED
SOLUTIONS INDIA PVT. LTD.**

Most Promising Partners

BIREN SELARKA	ACMA COMPUTERS LTD.
VK MALHOTRA	AGMATEL INDIA PVT. LTD.
DR. MUKUL GUPTA	BM INFOTRADE PVT. LTD.
MANOJ RATHI	DIAMOND INFOTECH PVT. LTD.
DHIRENDRA KHANDELWAL	E SQUARE SYSTEM & TECHNOLOGIES PVT LTD.
MINAL BHAGAT	ENSONIC COMPUTECH PVT. LTD.
RAJNIKANT DAS	E-SOFT ONLINE
MANOJ GUPTA	FORTUNE MARKETING PVT. LTD.
DALIP ARORA	FRUX TECHNOLOGIES PVT. LTD.
SANTOSH SANKUNNY/RAJESH KUMAR	INFLOW TECHNOLOGIES PVT. LTD.
NAVNEET SINGH BINDRA	INGRAM MICRO INDIA
SANJIV KRISHEN	IRIS GLOBAL SERVICES PVT. LTD.
SUNIL PILLAI	IVALUE INFOSOLUTIONS
AMARNATH SHETTY	LDS INFOTECH PVT. LTD.
MOHAN KUMAR TL	NETPOLEON INDIA
KUMAR BACHCHAN	NIVESHAN TECHNOLOGIES INDIA PVT. LTD.
SAIRAMAN MUDALIAR	PENTAGON SYSTEM & SERVICES
ASHOK KUMAR	RAH INFOTECH PVT. LTD.
RAJESH GOENKA	RASHI PERIPHERALS LIMITED
RAJAT VOHRA	REDINGTON LIMITED
JIGAR SANGHVI	SANGHVI INFOTECH PVT. LTD.
MAHENDRA WAHILE	SAVEX TECHNOLOGIES PVT LTD.
PRIYANKA KHANNA	SHIVAAMI CLOUD SERVICES PVT. LTD.
DEBRAJ DAM	SUPERTRON ELECTRONICS (SEPL)
NARINDER SINGH MANRAL	TDM GROUP
SUNDARESAN K	TECH DATA TECHNOLOGY SOLUTIONS

Palo Alto Eyes AI Security with CyberArk Deal

In a landmark cybersecurity deal, Palo Alto Networks announced the acquisition of CyberArk for approximately \$25 billion, marking its official entry into the Identity Security market. CyberArk shareholders will receive \$45 in cash and 2.2005 shares of Palo Alto Networks common stock for each share, representing a 26% premium over CyberArk’s recent 10-day average.



Nikesh Arora, CEO of Palo Alto Networks, said, "The acquisition aligns with their strategy to enter markets at their inflection point—now evident in identity security. Udi Mokady, Executive Chairman of CyberArk, called the deal a natural next step in their mission to protect critical assets through innovation and trust."

This strategic move aims to create an end-to-end security platform tailored for the AI era, establishing Identity Security as a core pillar of Palo Alto Networks’ multi-platform approach. The integration of CyberArk’s PAM and identity security capabilities with Palo Alto’s AI-powered platforms like Strata and Cortex will secure human, machine, and Agentic AI identities—a new class of privileged users. The deal expected to close in H2 2026 will create an integrated cybersecurity portfolio.

Microsoft Surpasses \$4 Trillion in Market Value

Microsoft has officially crossed a \$4 trillion market cap, becoming only the second company after Nvidia to reach this milestone. The surge came after a strong fourth-quarter earnings report, with revenue of \$76.4 billion and earnings of \$3.65 per share, beating Bloomberg estimates of \$73.89 billion and \$3.37 per share. Shares rose over 9% in after-hours trading, driven by robust growth in Microsoft’s cloud and AI segments.



CEO Satya Nadella highlighted Azure’s impressive \$75 billion revenue, up 34%, calling cloud and AI the key drivers of transformation across industries. For the first time, Microsoft disclosed Azure’s revenue separately, showcasing transparency amid its aggressive AI push.

The company also announced \$30 billion in capital expenditures for the next quarter to expand data center capacity, reflecting high demand. As rivals like Google increase capex, Microsoft’s bold investments signal its intent to dominate AI and cloud computing. With record growth and ambitious plans, Microsoft is solidifying its position in the AI-driven digital economy.

CADYCE Celebrates Unity and Innovation with a Vibrant Team Photo-Shoot

On a bright Thursday morning, July 3, 2025, the Pune headquarters of CADYCE buzzed with an extra dose of energy. The tech brand, known for its pioneering work in connectivity and digital solutions, turned the spotlight inward with a vibrant team photo-shoot—an event that was more than just a set of pictures. It was a celebration of the people behind the innovation, and a powerful visual representation of unity, collaboration, and CADYCE’s forward-thinking ethos.



Dressed in a coordinated official dress code, the entire CADYCE team gathered to showcase their collective identity—an ensemble of individuals driven by purpose, bound by trust, and united in their vision of delivering cutting-edge technology to the world. The photo-shoot, held within the premises of CADYCE’s headquarters, wasn’t just about aesthetics; it was about culture, creativity, and capturing the heartbeat of a company that thrives on synergy and shared goals.

The images, full of enthusiasm and team spirit, are set to be featured in select technology and corporate lifestyle magazines, offering a rare behind-the-scenes glimpse into the minds driving CADYCE’s relentless pursuit of excellence. The photo session also symbolized a pivotal moment in CADYCE’s growth story—reaffirming its commitment to empowering modern digital lifestyles through high-quality, user-centric products.

As CADYCE continues to lead with innovation in the connectivity space, this initiative beautifully underscored the core values that fuel its journey: people, purpose, and progress. In a world increasingly defined by technology, CADYCE reminded us that at the center of every innovation lies a team of passionate individuals working together to make a difference.

VAR SECURITY

Hikvision Powers Smarter, Sustainable Schools with Paperless Classrooms and Advanced Security Solutions

Schools and institutions worldwide are embracing technology-driven transformation, combining sustainability with security to enhance learning and operational efficiency. Traditional classrooms, burdened by paper dependency, costly consumables, and power-intensive projectors, pose significant financial and environmental challenges. In the US, schools use 32 billion sheets of paper annually, while UK schools average one million sheets each year, driving deforestation, waste, and unnecessary costs.



Interactive displays, such as Hikvision’s WonderHub, are reshaping education by eliminating paper, enabling digital collaboration, and improving energy efficiency. Features like intelligent brightness control, energy-saving modes, and extended lifespans reduce landfill waste while boosting student engagement. Spring Dale Senior School in Punjab demonstrates this transformation, deploying WonderHub displays across 80 classrooms to cut costs, reduce environmental impact, and create dynamic, tech-enabled learning spaces.

Beyond classrooms, Hikvision’s Speed Gate and Turnstile solutions deliver robust, customizable entrance control for schools, universities, corporate campuses, hospitals, and transport hubs. Built with durable SUS304 stainless steel, these systems integrate face recognition, biometric and card authentication, AI-driven video analytics, and real-time monitoring for heightened security. Safety is paramount with anti-collision, anti-pinch, and anti-trailing functions, while integration with fire alarm systems enables seamless emergency evacuation.

Offering a wide range of products—including tripod turnstiles, flap and swing barriers, bollards, and tyre killers—Hikvision ensures flexibility for diverse needs. Supporting lane widths from 650 mm to 1100 mm and designed for durability with up to 30 million mean cycles between failure (MCBF), these solutions minimize downtime while ensuring smooth, secure operations.

By merging sustainable, paperless education with cutting-edge security infrastructure, Hikvision is helping institutions worldwide reduce costs, enhance efficiency, and build smarter, greener, and safer environments for the future.



KPMG announces new Partner & Technology Consulting Leader

KPMG in India has announced the appointment of Gautam Bhattacharya as Partner and Technology Consulting Leader. Gautam will play a key role in strengthening the firm's digital transformation and analytics offerings, helping clients harness the power of data, AI, and emerging technologies to drive scalable, sustainable growth.

Gautam brings over two decades of global experience in analytics, enterprise transformation, and decision intelligence. He has successfully led large teams and high-impact programs across industries including consumer markets, manufacturing, and supply chain.

This appointment reinforces KPMG in India's commitment to delivering end-to-end technology consulting services that enable future-ready enterprises. The firm continues to invest in expanding its technology offerings.



PhonePe names Shivnath Thukral as VP for Public Policy and Government Affairs

PhonePe has appointed Shivnath Thukral as Vice President for Public Policy and Government Affairs. In this role, Shivnath will be responsible for leading PhonePe's external engagement and discussions with policy makers and regulators to ensure the company continues to innovate and create a positive impact in the Indian economy,

while also building on its thought leadership in the industry. He will be part of the leadership team at PhonePe and work closely with founders Sameer Nigam and Rahul Chari and other leaders.

Shivnath Thukral joins PhonePe after an impactful stint at Meta as its Vice President of Public Policy to where he led the organisation as a strategic thinker, business leader and an effective advocate on regulatory issues related to technology and financial inclusion. Shivnath in recent years has emerged as a leading policy professional occupying important positions in various industry associations such as BIF, USISPF, PAFI etc.



Kamolika Gupta Peres appointed as VP for Autodesk India & SAARC

Autodesk has announced the appointment of Kamolika Gupta Peres as vice president, Autodesk India and SAARC business, effective June 2025. In her new role, she will lead Autodesk's growth and scaling efforts in India and SAARC, strengthen the company's customer and partner ecosystem, and further deepen

Autodesk's position as a trusted transformation partner in the region. Her appointment marks a significant step in Autodesk's continued investment in India.

Known for her agile, empathetic leadership and passion for bold, future-focused transformation, Kamolika brings a people-first approach that inspires clarity, ownership, and high performance across teams. As the leader of India and SAARC, Kamolika will play a pivotal role in expanding Autodesk's market presence and building a strong ecosystem to support the next wave of growth across the India and SAARC region. She will work closely with key stakeholders to drive strong execution and help expand Autodesk's footprint by tapping into India's dynamic business opportunities and growing its investments in public infrastructure.

Commvault announces new appointments

Commvault has announced Alan Atkinson has become the company's first Chief Business Development Officer. In this new role, he will build strategic next-gen technology and security partnerships, drive co-development initiatives, and create new go-to-market opportunities for Commvault and its partners, all within the Business Development organization led by Chief Trust Officer Danielle Sheer.

With this transition, Commvault has recruited a new dynamic partner leader, Michelle Graff, as Senior Vice President of Global Partners and Channel. In her role, Graff will lead Commvault's global partner strategy and ecosystem, overseeing partner sales, resellers and alliances, and the vision and execution of the company's partner programs. She will focus on advancing growth and co-innovation with partners and delivering differentiated cloud and AI-forward solutions to customers.



NetApp ropes in Kiran Sukhtankar for Systems Engineering India and SAARC

NetApp has appointed Kiran Sukhtankar as Director of Systems Engineering for India and SAARC. In this role, Kiran will lead NetApp's systems engineering strategy across the region, driving technical engagement and innovation with customers and partners. This strategic appointment reflects NetApp's continued commitment to empowering customers with innovative, data-driven solutions and world-class technical expertise.

A seasoned technology leader, Kiran brings over 30 years of rich experience in the IT and software industry, with a strong track record in pre-sales leadership across India, APAC, and EU markets. He has held key roles at global technology leaders such as IBM, Veritas, Symantec, Hitachi, and Oracle. Most recently, he led presales for Veritas/Cohesity, where he was instrumental in solving complex Data Management and Security challenges for enterprise clients.



Altimetrik ropes in Sreenivas V as its CFO

AI-First, data and digital engineering solutions company, Altimetrik has appointed Sreenivas V as its new Chief Financial Officer (CFO). Reporting directly to CEO Raj Sundaresan, Sreenivas will strategically transform and spearhead the company's global finance function as Altimetrik accelerates into its next growth phase, fuelled by AI innovation.

Embracing an AI-First approach across its internal operations and client engagements, Altimetrik has embarked on a series of transformative initiatives aimed at unlocking the full potential of AI to deliver business value. As part of its strategic expansion, the company recently announced the signing of a definitive agreement to acquire SLK Software, strengthening its end-to-end enablement services, expanding its customer reach and global delivery capabilities.

Reinforcing its long-term vision, Altimetrik remains committed to pioneering industry-leading AI-led initiatives that accelerate enterprise AI adoption and deliver measurable, high-impact outcomes at scale.



The Smart Gatekeepers of Secure Networking

TP-Link's VPN Gateway Routers are purpose built to deliver secure, high-speed connectivity for every branch, every site, every user.



- Multi-WAN Load Balancing & Failover
- 4G+ Cat6 Support:
● Up to 300 Mbps with Nano SIM
- Wi-Fi 6 Support (ER706W)
- Up to 10G WAN Ports (ER8411)
- SPI Firewall and DoS Protection
- Ideal for Multi-Branch Businesses & Enterprises
- High-Security VPN – IPsec PPTP/L2TP/OpenVPN
- Centralized Management via Omada SDN

ER706W-4G

Omada 4G+ Cat6 AX3000 Gigabit VPN Router

ER7206

Gigabit VPN Router

ER8411

10G VPN Router with 8x RJ45 Ports + 2x SFP+

Call for Product Demo!

TP-Link India Contacts:

North Rajendra Mohanty M: +91 98711 51116 E: rajendra.mohanty@tp-link.com	South Sunil Nair M: +91 96111 13909 E: sunil.nair@tp-link.com	AP & Telangana Raminder Singh M: +91 97045 75432 E: raminder.singh@tp-link.com	East Satish Panda M: +91 91639 33951 E: satish.panda@tp-link.com	West Mohit Maheshpuria M: +91 98199 87178 E: mohit.m@tp-link.com	Nagpur Abhay Lanjewar M: +91 95796 46634 E: abhay.lanjewar@tp-link.com
North Bhushan KR Saxena M: +91 97174 74061 E: bhushan.kumar@tp-link.com	Banglore Srikanth S M: +91 99852 15156 E: srikanth.s@tp-link.com	Hyderabad Srikant R M: +91 94825 57627 E: srikanth.r@tp-link.com	East Abinash Roy M: +91 95236 53074 E: abinash.roy@tp-link.com	Mumbai Arvind Tripathi M: +91 98673 47909 E: arvind.tripathi@tp-link.com	Pune Sumeet Lambe M: +91 89995 64587 E: sumeet.lambe@tp-link.com

HIKVISION MONITOR
CLARITY BEYOND LIMITS

Experience ultra-clear visuals with Hikvision Monitors

DS-D5022QE-D 22" Value Series




-5° -15°
adjustable tilt angle
Protect your
cervical health


Low blue
light & flicker free
Anti glare screen,
filter blue light


Bracket with
own storage slot
Keep your desktop
organized

 /HikvisionIndiaOfficial

Prama Hikvision India Private Limited

 /HikvisionIndiaOfficial



Registered Office:
Office No.1-4, 2nd Floor, Siddhivinayak Arcade, Akurli Cross Road No.1,
Near Kandivali Station, Kandivali (E), Mumbai - 400 101, India.
CIN: U36100MH2009PTC190094
Corporate Office:
Oberoi Commerz II, International Business Park, 18th Floor, Near Oberoi Mall,
Off. W. E. Highway, Goregaon (East), Mumbai - 400063, India.
Board No.: +91-22-4041 9900, +91-22-6855 9900 | **Web:** www.hikvisionindia.com

 **Technical Support:** +91-22-6822 9999, +91-22-4068 9999
Email: support@pramahikvision.com
 **Sales:** +91-22-4041 9944, +91-22-6822 9944
Email: sales@pramahikvision.com
 **RMA Support:** +91-22-6822 9977, +91-22-4068 9977,
+91-250-663 6677 | **Email:** rma@pramahikvision.com
 **Toll No.:** 18602100108