SEBI suggests SIM-linked authentication

Sarvam AI to Develop Sovereign AI Solutions

INDIA'S FRONTLINE IT MAGAZINE

VARINDIA

THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

VOLUME XXVI ISSUE 06 FEBRUARY 2025 PRICE RS. 50

TECH, SECURITY & GOVERNANCE:

BUILDING A RESILIENT DIGITAL INDIA

brother
at your side

TONER BOX LASER PRINTER

DCP-B7620DWB

Print Scan Copy

34 Pages Per Minute	Auto Duplex Printing	Ethernet	Wi-Fi	2600 Pages Inbox Toner*

Faster the Speed. Smarter the Features.

NEW LAUNCH

With ORIGINAL TONER COST 33 Paise* Per Page

MRP ₹ 26,990/-*
(Incl. of all taxes)

SCAN TO KNOW MORE

FOR SALES ENQUIRIES : Mumbai : Ritesh Talewar - 9325003130 I **Pune, Chattisgarh, Goa, Rest of Maharashtra :** Shishir Singh - 9860728548 I **Gujrat, MP :** Pulin Shah - 9924253604 I **Bihar, Jharkhand, Orissa :** Deepak Singh - 9771403031 I **Telangana, Andhra Pradesh, Karnataka :** Naveen Choubey - 9849099159 I **Chennai & Kerala :** Govindrajan S - 9176681639 I **Delhi, Rajasthan, Haryana :** Ashish Kalra - 9899306959 I **Uttar Pradesh, Punjab, Jammu & Kashmir, Uttrakhand :** Ajay Saxena - 9919666636 I **Kolkata & Northeast :** Amitava Roy - 9830405757

☎ • 1-800-222-422 • 1-800-209-8904 (Toll Free) www.brother.in

* MRP mentioned above is for 1 unit and subject to change without prior notice | Yield in accordance with ISO/IEC 19752 | Original Toner cost per page is calculated on toner yield of 2600 pages (as per ISO/IEC 19752) at ₹ 846

CP PLUS Achieves BIS Certification for ER 01:2024 Compliance

Samsung seeks TN govt's support amid strike

INDIA'S FRONTLINE IT MAGAZINE

VARINDIA

THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

REIMAGINING JUSTICE:
HOW TECHNOLOGY CAN TRANSFORM INDIA'S COURTS

VOLUME XXVI ISSUE 06 FEBRUARY 2025 PRICE RS. 50 SUBSCRIPTION COPY NOT FOR SALE

VEEAM PROPARTNER SUMMIT 2025 EMPHASIZING ON AI POWERED DATA RESILIENCE

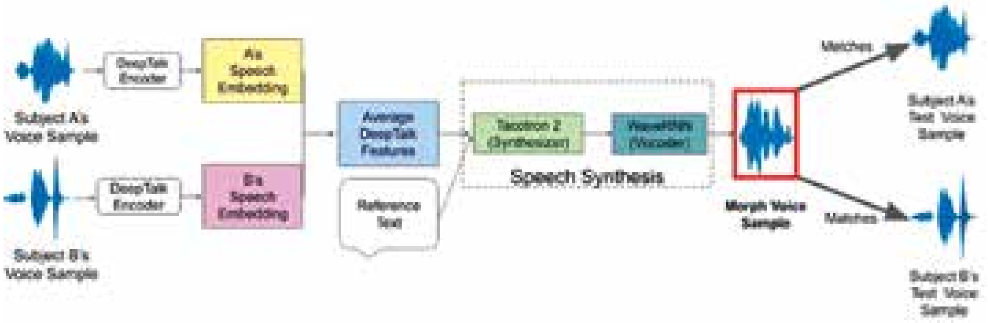
FOR MORE PAGE 30

Lenovo presents IdeaPad Slim 5

Lenovo has launched its IdeaPad Slim 5 (14", Gen 10) and (16", Gen 10)—the first laptops featuring the AMD Ryzen AI 300 Series 'Krackan Point' processor. These next-gen devices are designed to deliver AI-powered performance, enhanced multitasking, and smarter computing, making them ideal for professionals, creators, and students who need sleek, lightweight, and high-performance machines for their everyday tasks. Built on the latest 'Krackan Point' technology, they bring cutting-edge AI acceleration, efficient power consumption, and superior computing performance to ultra-portable form factors. The new Ryzen AI 300 Series integrate Zen 5 cores, AMD RDNA 3.5 graphics, and an enhanced XDNA 2 NPU, delivering up to 55 TOPS of AI processing power—enabling intelligent workload management, real-time enhancements, and future-ready AI capabilities.

Microsoft unveils AI model

Microsoft Research, in collaboration with Xbox game studio Ninja Theory, has introduced a new artificial intelligence model called Muse, designed to generate gameplay visuals and predict controller inputs. This technology, which represents a major advancement in AI in gaming, is expected to have significant implications for video game development and preservation. Muse has been trained using over one billion images and controller actions from the 2020 game Bleeding Edge. This extensive training allows the model to demonstrate a deep understanding of 3D game worlds and physics, reacting to player interactions. Microsoft has dubbed Muse the first of a new category of AI, termed World and Human Action Models (WHAM). The innovation signals a new wave in the gaming industry with AI systems capable of understanding complex gameplay dynamics.



REGULATING DEEPSEEK: A STRATEGIC APPROACH FOR INDIA

The potential ban on DeepSeek, a Chinese AI model, has fueled intense debate in India, with comparisons drawn to previous restrictions on Chinese apps like TikTok. However, the nature of DeepSeek's operations is fundamentally different, as it serves businesses and researchers rather than mass consumers.

While concerns over data security, privacy, and foreign influence remain valid, India must take a balanced approach by implementing strong regulations instead of an outright ban. A well-structured regulatory framework will help mitigate risks while fostering innovation, ensuring that India continues to thrive in the AI revolution.

Unlike social media platforms, which collect extensive personal data from individual users, DeepSeek functions as a business-to-business (B2B) AI tool. Its AI models are primarily used in automation, research, and enterprise-level applications, making the risk profile different from consumer-driven platforms.

However, concerns remain about DeepSeek storing user inputs and metadata in China, raising fears of data leaks, unauthorized surveillance, and national security threats. These risks necessitate government intervention through strict regulations, ensuring that sensitive information is safeguarded.

Recognizing these issues, India's IT Minister, Ashwini Vaishnaw, has announced that DeepSeek will soon be hosted on Indian servers. This step will allow for greater oversight, improved cybersecurity compliance, and stricter enforcement of data protection laws.

Hosting DeepSeek within India ensures data residency, limiting the possibility of unauthorized cross-border data transfers. Additionally, the government can mandate security audits and compliance measures, reducing the risk of potential misuse or foreign interference.

In a move to reduce dependency on foreign AI models, India has launched the IndiaAI mission, allocating ₹10,300 crore to AI infrastructure, startup funding, and research. As part of this initiative, 18,693 GPUs have been empaneled to establish a national AI computing facility, ensuring that Indian researchers and businesses have access to advanced computational power. This initiative highlights India's commitment to becoming a global AI leader, accelerating domestic innovation while maintaining controlled collaborations with global firms.

Beyond concerns over data security, ethical challenges surrounding DeepSeek's AI development have also surfaced. OpenAI has accused DeepSeek of copying its technology, sparking discussions on intellectual property violations. To address these issues, India must enforce AI ethics regulations, security audits, and controlled API access, ensuring that foreign AI models comply with national standards.

Despite India's rapid AI expansion, private sector investment in AI research and development remains limited. While Mukesh Ambani has announced plans to build the world's largest data center, investing in Nvidia chips for AI model training, infrastructure alone is not sufficient. True advancements in natural language processing and AI model development require sustained funding and long-term commitment.

However, many Indian IT firms continue to focus on short-term shareholder gains, prioritizing dividends and buybacks over bold AI investments. This cautious approach could slow down India's AI growth, allowing global competitors to dominate.

Banning DeepSeek outright could also have geopolitical consequences. India and China already have strained trade relations, and further restrictions on Chinese technology could escalate economic tensions. Unlike previous bans on WeChat and UC Browser, DeepSeek operates in a different category, where complete elimination may not be necessary. A well-defined regulatory framework would allow India to control AI risks while maintaining technological access.

Additionally, India lacks homegrown AI models that can compete with DeepSeek, OpenAI, and Google DeepMind. Cutting off DeepSeek without a strong local alternative would make Indian businesses and researchers overly dependent on Western AI technologies, limiting India's strategic autonomy.

To mitigate these risks while ensuring security, India should implement targeted AI regulations rather than a blanket ban. This includes:

Data Localization – Ensuring that all AI-related data is stored and processed within India's jurisdiction.

Cybersecurity Audits – Conducting regular security assessments to detect vulnerabilities in foreign AI models.

Controlled AI Access – Restricting sensitive applications to Indian-developed AI models to enhance security.

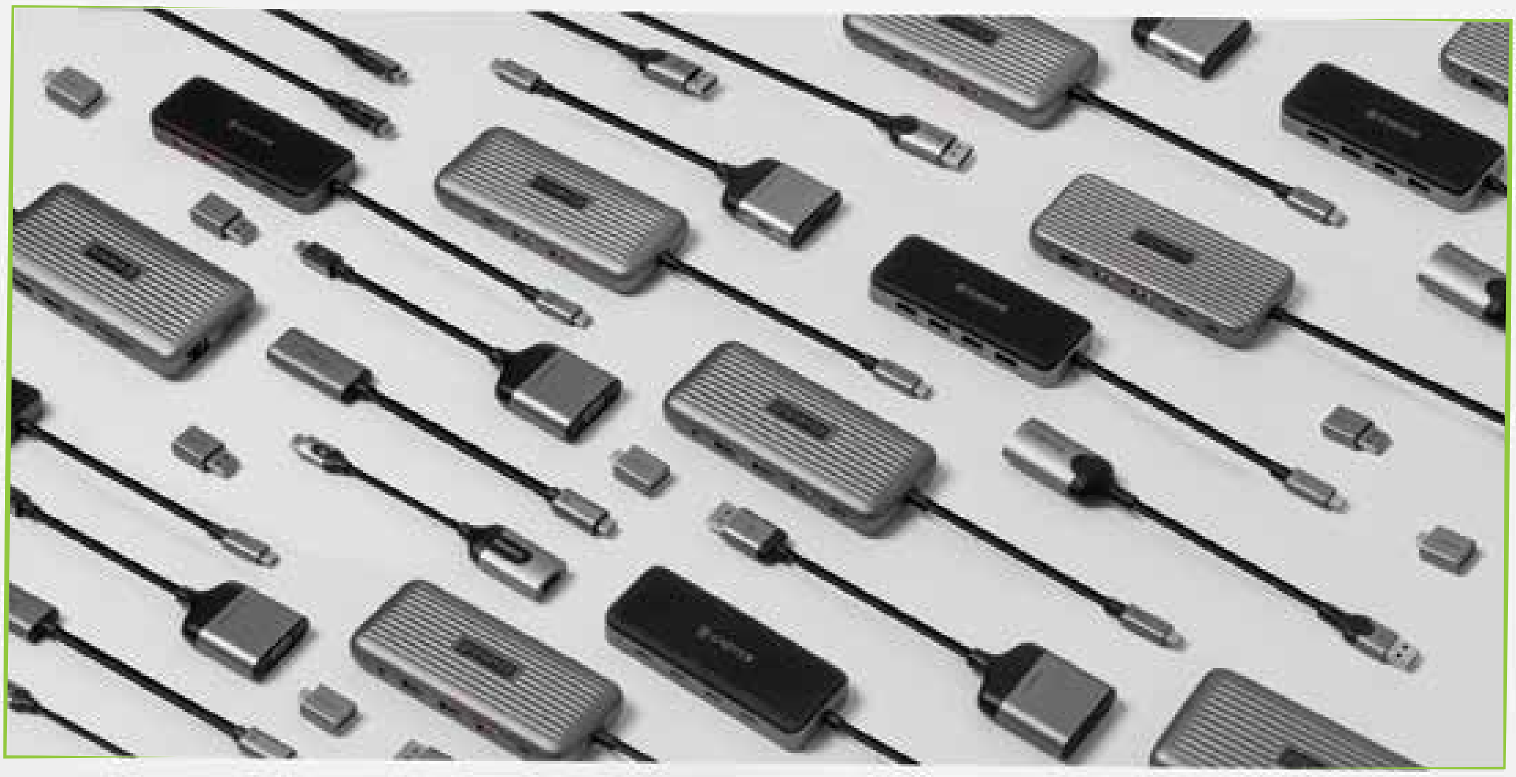
Ethical AI Guidelines – Enforcing compliance with AI transparency, accountability, and fairness standards.

India's approach to DeepSeek should be based on security assessments rather than reactionary bans. By enforcing strong AI regulations, cybersecurity audits, and controlled data-sharing protocols, the government can protect national interests while allowing businesses to leverage global AI advancements. The establishment of India's AI Safety Institution, expansion of AI infrastructure, and increased private investment in AI research will play a crucial role in shaping India's future as a global AI leader.

Moving forward, by striking a balance between innovation, security, and regulatory oversight, India can position itself at the forefront of AI development while safeguarding its digital ecosystem.

Mohini

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



INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

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
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
Megatherm Electronics Pvt. Ltd.
6th Floor, Megatherm Tower, Electronics Complex,
Plot L1, Sector -5, 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

CONTENTS

COVER STORY / 32pg

CYBER & DATA SECURITY SUMMIT 2025 STRENGTHENING DIGITAL RESILIENCE

REGULARS

CHANNEL BUZZ

COVER STORY

INDUSTRY EVENT

LEAD STORY

DELL Technologies

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 AIOps
- All-inclusive software

IRIS GLOBAL

Please Contact
shivani.saini@irisglobal.in

Iris Global Services Pvt Ltd
1Bypass Road, Mahipalpur, New Delhi,110037

A bold 'Make in India' product takes on Tech Giants!

Digital transformation shouldn't be complicated. Yet, outdated systems and fragmented data hold businesses back. GainHub.Ai simplifies the process with an all-in-one platform integrating sales, marketing, operations, and finance. With seamless automation and real-time insights, businesses can streamline workflows, boost sales, and stay ahead. **LV Sastry, Board Advisor & CXO mentor,** highlights how this Made-in-India solution drives innovation and makes transformation effortless. GainHub.Ai ensures businesses don't just adapt but lead in today's fast-paced digital world.

Today's SaaS, CRM, and digital transformation platforms promise to revolutionize the way businesses operate, but let's be honest—they still have plenty of gaps and shortcomings. Many platforms are rigid and difficult to customize, forcing companies to adjust their processes to fit the software instead of the other way around. Automation is an area where these platforms often fall short. Many claim to streamline workflows, yet businesses still find themselves bogged down with manual tasks because the automation tools lack flexibility or require too much technical know-how to configure properly. And let's not forget about integrations—how often have companies invested in a "seamless" tech stack, only to end up with a patchwork of disconnected apps that don't talk to each other?

The result? Frustration, inefficiency, and a widening gap between what businesses expect and what these tools actually deliver. It's clear that the market needs smarter, more intuitive platforms that adapt to businesses—not the other way around. Take CRMs, for example—while they claim to offer a 360-degree view of the customer, most still struggle to integrate data smoothly across multiple touchpoints, leaving teams with fragmented insights.

OVERCOMING THE DATA DIVIDE IN MODERN ENTERPRISES

Businesses today are overwhelmed with data but struggle to extract real value from it. Disconnected tools and outdated systems create inefficiencies, leading to lost opportunities. GainHub.Ai eliminates these challenges with an all-in-one platform that seamlessly integrates sales, marketing, and operations, providing real-time insights and automation to drive efficiency and agility.

With its intuitive design, GainHub.Ai simplifies digital transformation, helping teams work smarter, close deals faster, and make data-driven decisions effortlessly. By leveraging AI-powered automation and seamless integration, businesses can focus on growth, innovation, and staying ahead of the competition—without the headaches of traditional software.

GainHub.Ai simplifies digital transformation by unifying systems, streamlining operations, and unlocking real-time insights. Its intelligent applications empower businesses to analyze processes, identify opportunities, and drive strategic growth effortlessly. With seamless integration and AI-powered automation, GainHub.Ai ensures enterprises stay agile, efficient, and ahead in today's fast-evolving digital landscape.

SIMPLIFYING DIGITAL TRANSFORMATION WITH GAINHUB.AI

Getting started with digital transformation can be daunting, but GainHub.Ai makes it effortless. With its sleek interface and robust features, the platform eliminates the hassle of outdated systems and scattered data. It acts as a central hub, seamlessly integrating sales, operations, and analytics into one cohesive ecosystem. No more inefficiencies—just a smarter, more connected way to run your business.

Many businesses struggle with fragmented systems and siloed data, slowing innovation and increasing costs. GainHub.Ai tackles these challenges head-on by unifying data across HRMS, CRM, marketing automation, and more. With 81% of IT leaders citing data silos as a major roadblock to transformation, this platform provides a game-changing solution. By breaking down barriers and streamlining workflows, GainHub.Ai empowers businesses to optimize operations, make real-time decisions, and scale with confidence—without the usual integration headaches.

KEY FEATURES OF GAINHUB.AI (GHP)

GainHub.Ai transforms business operations with a unified platform that integrates applications, tools, and legacy systems. Its AI-driven analytics offer deep insights for smarter decisions, while hierarchical segmentation ensures precise targeting and personalization. With real-time intelligence, businesses can continuously monitor and optimize performance, making operations more efficient and data-driven.

This unified approach offers a multitude of benefits for organizations looking to optimize both customer-facing and back-end operations.

MARKET CONSIDERATIONS

GainHub.Ai isn't just another digital tool—it's a game-changing investment for businesses seeking a high-performance, unified transformation platform. Designed for enterprise needs, it integrates AI, automation, and intelligent applications to streamline operations and enhance customer engagement. By breaking down silos and optimizing workflows, GainHub.Ai drives efficiency, productivity, and long-term growth, making digital transformation seamless and impactful.

WHY CHOOSE GAINHUB.AI?

GainHub.Ai isn't just another out-of-the-box solution. It is an enterprise-grade platform built to integrate deeply with ERP systems and other essential backend applications.

With integrated intelligent workflows, GainHub.Ai provides unparalleled optimization across key operational areas such as:

- Sales Management
- Order Management
- Invoicing & Billing
- Inventory & Supply Chain Tracking
- Project Management
- Service Management
- HR Management
- Operations Management
- Workflow Management

CHATGPT VS DEEPSEEK: RAGING DIGITAL WARFARE ENVELOPS WORLD

DR. ASOKE K. LAHA
Chairman-Emeritus and Founder
InterraIT

What are the things that are happening, and changing public discourse? A good number of people whom I talked to said that a hot topic people talk about is President Donald Trump's second term as the US President and how it will be unveiled in the coming days, months, and years. These are the people mostly businessmen linked with the US or parents whose children are living in the US on short-term visas, or people dabbling in the complex space of finance or the stock market, who want to know how much the rupee fell against the dollar and how much it will slide in the coming days.

Surprisingly, that was not the top subject gaining currency for a good number of people I spoke to. Most of the people, particularly the techie guys and students are involved in the debate of ChatGPT vs DeepSeek. People pursuing cerebral avocations want to know: first the difference between the two and, second which one is better. Interestingly, some people who must write a letter, representation to government agencies, or prepare a thesis or dissertation use ChatGPT to get an edge in their writing. They want to know which is better: ChatGPT or DeepSeek.

I have dealt with ChatGPT in this column a few times and do not intend to deal with it now. But, let me dwell on DeepSeek, which was launched recently. Though DeepSeek captured headlines, no one knows precisely what it is and how it is an improvisation over the ChatGPT, which has been on an innovation trail. Like me, most people may have only read about it in newspaper columns or videos that depict what it can.

But a few advantages of the free AI-powered chatbot DeepSeek, which looks, feels, and works very much like ChatGPT are in the public domain. People familiar with its operations say it can be used as ChatGPT. It is reportedly as powerful as OpenAI's o1 model - released end of last year and can undertake tasks including mathematics and coding.

Besides, people familiar with its work say it has more reasoning power and produces responses incrementally, simulating how humans reason through problems or ideas. The other claim is that it is available freely, and researchers behind it claim it cost US $6M to train, a fraction of the "over $100M" alluded to by OpenAI boss Sam Altman when discussing GPT-4. That is the reason why DeepSeek has outweighed all other platforms in downloading from Play store

Despite the geopolitical pulls and pressure with its advent, President Donald Trump welcomed the Chinese innovation calling it a great innovation and a game changer. But many interpret Trump's salutary words about DeepSeek a wake-up call for the American tech giants. Incidentally, major tech companies in the US shaved off their values in the stock market mayhem that happened with the Chinese announcement of DeepSeek.

There are other interpretations that the Chinese released this innovation to convey signals to Washington that it could strike back when the shoe pinches. China also wanted to amplify that it can minimize the impact of US restrictions on the most powerful chips reaching China. DeepSeek's founder reportedly built up a store of Nvidia A100 chips, which have been banned from export to China since September 2022. Some experts believe he paired these chips with cheaper, less sophisticated ones - ending up with a much more efficient process.

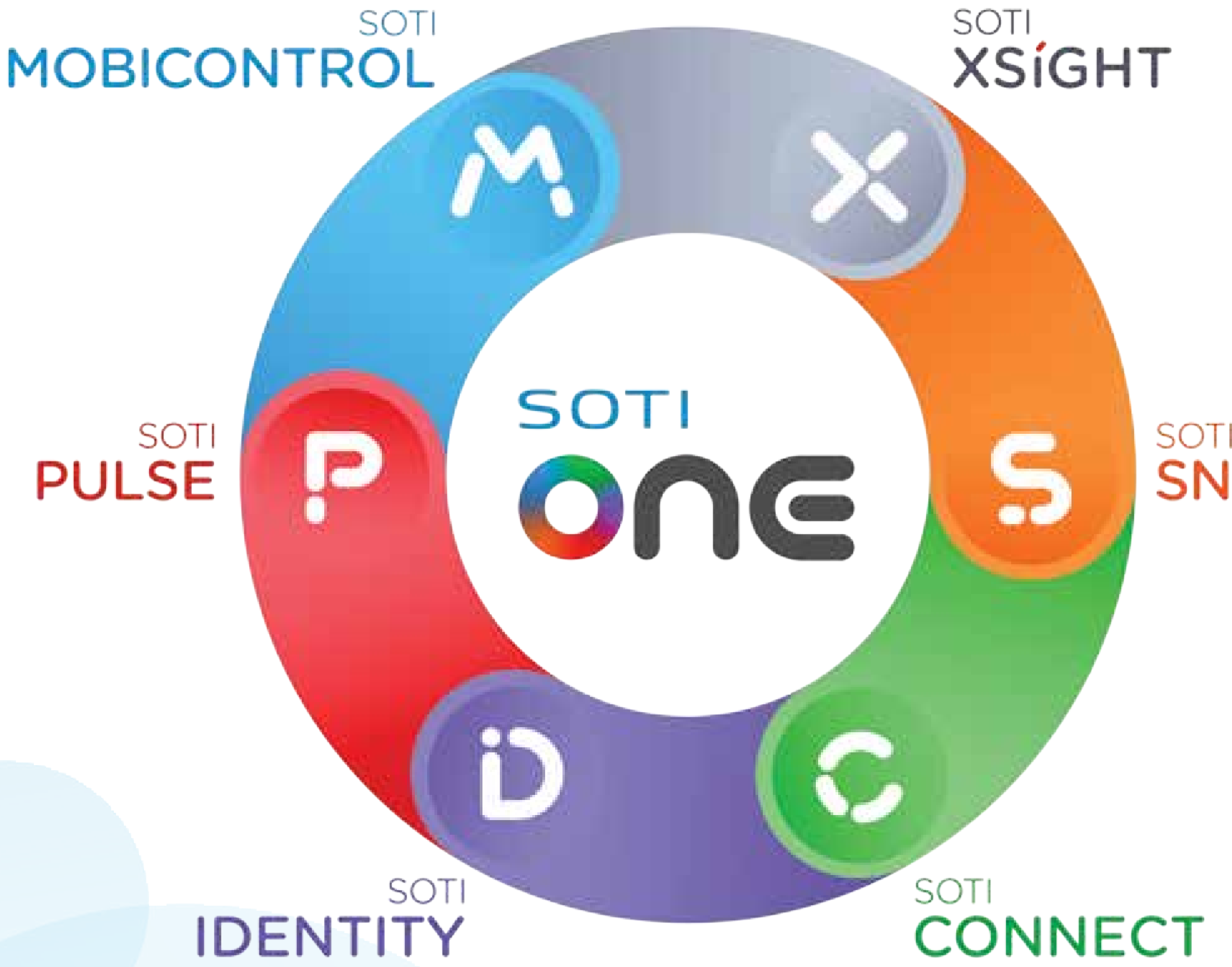
Like many other Chinese AI models - Baidu's Ernie or Doubao by ByteDance - DeepSeek is trained to avoid politically sensitive questions unlike Google, which can give all shades of opinions. It is reported that when someone asked a question about what happened in Tiananmen Square on 4 June 1989, DeepSeek did not give any details about the massacre, a taboo topic in China, which is subject to government censorship.

Let me now come to the point that I want to flag. I find a lot of literature that is coming out these days is AI-driven. One can make out from the language used which is more synthetic and less natural. I do not know how much that will affect creativity when people seek the help of these tools, while doing simple changes in the narratives or solving mathematical puzzles or coding, the basic operation in software development.

That takes me to my younger days. In the primary classes, we have been asked to learn multiplication tables. The task was to learn it by heart. That would help us to use it anytime and anywhere. The advent of calculators reduced the relevance of learning multiplication tables by heart. Similarly, computers that have embedded software programs for spelling and grammar auto corrections have reduced the need for correct semantics and spellings impinging on the vocabulary.

How long this can take? Though there is a debate on chaining in AI-powered innovations that can impair creativity and replace the human workforce, such discourses remain wishful thinking. Everyone is glued to know what is the next breakthrough of AI and how long will it take to make a robot that can perform all pursuits a human being can do.

Of course, there are two issues to be reconciled to have a clear strategy to address this problem. One is the human quest to find excellence in technology, which is the sign of power and the best bargaining power in a highly competitive world. The other is global inclusive growth, which lays down normative principles of happiness, the welfare of all, and contentment. Civilizations over millennia chased a reconciliation of both issues. But could not come out with a solution or approximation of a solution. Yet, we have to strive for a solution however naïve or incomplete that may be.



SOTI
MOBICONTROL
SOTI
XSiGHT
SOTI
PULSE
SOTI
ONE
SOTI
SNAP
SOTI
IDENTITY
SOTI
CONNECT

SEBI suggests SIM-linked authentication

The Securities and Exchange Board of India (Sebi) has introduced a proposal to implement a SIM-based authentication system for trading and demat accounts. This system is designed to enhance security by ensuring that only authorized devices can access these accounts, using a method similar to the security protocols found in Unified Payments Interface (UPI) transactions. Under the new proposal, traders will need to log in to their trading accounts by linking their Unique Client Code (UCC) with the SIM and mobile device they use. This will ensure that only the registered device is able to access the account, providing a stronger layer of protection for trading account safety. This system will also enable investors to track and monitor any active sessions across different devices.

In addition to recognizing the UCC, SIM, and mobile device details, the system will require biometric authentication on the primary mobile device to further safeguard against unauthorized access. For logging into devices such as desktops or laptops, a QR code-based authentication system will be employed. This system will be time-sensitive and proximity-sensitive, mirroring features used by many social media platforms for multiple logins. Sebi's proposal also includes a fallback mechanism for instances where a user loses or changes their primary device, ensuring that they can still access their accounts securely. Moreover, one mobile device can be linked to multiple UCCs for family members using the same phone number, provided the proper authorizations are in place.

Google unveils 'Ananta,' its largest campus in India

Google has unveiled its largest campus in India—Ananta, which means "infinite" or "limitless" in Sanskrit. This happens to be one of Google's largest campuses in the world. Located in Mahadevapura, Bengaluru, Ananta has a seating capacity of over 5,000, and the campus has been designed with accessibility in mind, and the materials used for its construction are sourced almost entirely locally.

"Ananta will be known not just for the innovations that emerge from within its walls—powered by India but for the world—but also for its lasting impact. Six years ago, we made a pivotal shift, embracing an AI-first approach. We recognized India's potential not only as a deep talent pool but also as a place where AI can transform lives at scale. This new campus marks a milestone in the ongoing seismic shift in technology. It is a testament to our ambition to innovate and drive the next transformative leap in AI," said Preeti Lobana, Vice President and Country Manager, Google India.

Tesla sets sights on India with hiring push after PM Modi's US trip

Tesla is moving closer to its much-anticipated entry into the Indian market. The company has posted 13 job openings in India on its LinkedIn page, with roles ranging from customer-facing positions to back-end jobs. The positions are spread across key Indian cities like Mumbai and Delhi, and include positions such as service technician, customer engagement manager, and delivery operations specialist. These job listings are seen as a strong indicator of Tesla's intentions to establish a more robust presence in India.

This development comes shortly after Tesla CEO Elon Musk's meeting with Prime Minister Narendra Modi during his US trip. The two leaders discussed various topics, including technology and innovation, sparking new speculation about Tesla's plans for India. Historically, high import duties on cars have been a key obstacle for the company. However, Tesla's latest actions, including the job postings, suggest that the company is revisiting its India strategy with fresh optimism.

Sarvam AI to Develop Sovereign AI Solutions

Union Minister for Railways, Electronics and Information Technology, Ashwini Vaishnaw, recently shared significant developments in India's pursuit of technological self-reliance. He announced on the social media platform X (formerly Twitter) that discussions were held with Sarvam AI, a pioneering startup, to explore options for developing India's sovereign Large Language Model (LLM). Highlighting the immense potential of Indian language models, Vaishnaw emphasised their capability to address population-scale challenges effectively.

The sovereign AI model represents a strategic initiative to create AI solutions tailored to India's unique needs. Unlike generic AI systems developed by global tech giants, the India sovereign AI model is being designed to cater to the country's specific challenges, focusing on areas such as language processing for regional languages, healthcare innovation, agricultural advancements, and governance.

Sarvam AI's expertise in cutting-edge AI technologies and India's vast talent pool provide a powerful combination for fostering innovation. The partnership emphasizes building AI systems that align with national priorities, ensuring data privacy, security, and ethical AI use. The partnership between India and Sarvam AI highlights the country's commitment to embracing AI innovation while maintaining control over its technological future. The sovereign AI model represents a significant step forward in realizing the potential of AI development in India, paving the way for transformative advancements across industries.

Centre aims to empower 1 lakh young innovators through new AI programme

In a major push towards skill development in emerging technologies, the Ministry of Skill Development and Entrepreneurship (MSDE), National Skill Development Corporation (NSDC), and Intel India have launched the 'AI for Entrepreneurship' micro-learning module. The initiative is designed to simplify artificial intelligence (AI) concepts and encourage entrepreneurial thinking among young innovators across India. The programme aims to empower 1 lakh youth by 2025 and participants who complete the module will receive an industry-endorsed joint certification from MSDE, NSDC, Skill India, and Intel.

A key component of this initiative is the integration of AI education into STEM Education (Science, Technology, Engineering, and Mathematics). By incorporating AI concepts at an early stage, the programme aims to build a strong foundation for students, ensuring they develop computational thinking, data analysis, and machine learning skills. AI labs, hackathons, and mentorship programs will be introduced to provide hands-on learning experiences, preparing students for future AI-driven careers.

Multilingual AI hub launched as Centre revamps websites

In an endeavour to modernize its digital infrastructure and improve government communication, the Centre has rolled out a series of transformative initiatives, including the revamp of official websites and the creation of a multilingual AI hub. These efforts align with the country's vision of Digital India and Digital Bharat, aimed at making government schemes and initiatives more accessible and engaging to a diverse population.

On February 18, the Ministry of Electronics and Information Technology (MeitY) launched the Digital Brand Identity Manual, a comprehensive guide to standardizing the design of government websites. This initiative is part of a broader push to create a unified and accessible digital presence for the government. The Digital Brand Identity Manual seeks to provide a cohesive online experience, ensuring that government websites are not only user-friendly but also engaging. This initiative is a key part of India's ongoing commitment to a Digital Bharat, where digital platforms are seen as essential tools for governance, public engagement, and international interaction.

Hikvision Enhancing educational delivery through interactive displays

Yenepoya University, a leading higher education institution in Mangaluru, Karnataka, revolutionized its teaching methods by integrating Hikvision's Interactive Displays. The university installed 75-inch and 86-inch 4K Interactive Displays across classrooms and seminar halls to enhance student engagement and learning efficiency.

Previously, reliance on blackboards limited the interactive presentation of course materials, making it difficult for students, especially in large classrooms, to follow along. The 46 interactive panels now enable seamless content sharing via QR codes and allow lecturers to mirror content across multiple screens without lag.

Science subjects especially benefit from real-time annotations and visual demonstrations. Integrated with ClassIn software, the setup also facilitates remote learning, allowing students to participate virtually. This upgrade fosters inclusivity, transforming traditional classrooms into dynamic, technology-driven learning environments.

Sound Solutions makes 'Greh Pravesh' at new Chembur, Mumbai Office

Sound Solutions has achieved another significant milestone with the successful inauguration of its new office at The Epicenter, Chembur, Mumbai. This expansion marks a new chapter in the company's journey, reinforcing its commitment to excellence, innovation, and growth in the sound and audio solutions industry. The grand launch event witnessed an overwhelming response from industry leaders, partners, and well-wishers, making it a truly memorable occasion. Attendees from various sectors came together to celebrate this momentous achievement, sharing insights, experiences, and their support for Sound Solutions' continued success.

The event provided a valuable networking opportunity, strengthening relationships between the company and its esteemed stakeholders. Guests were welcomed into the state-of-the-art office space, reflecting Sound Solutions' dedication to creating a collaborative and inspiring work environment. Expressing gratitude to its channel partners and customers, Sound Solutions aims to expand its reach and offer seamless IT solutions. The company is all set to scale new heights, ensuring that its partners receive the best-in-class products and services.

Shaktikanta Das Appointed as Principal Secretary-2 to PM Modi

Former RBI Governor Shaktikanta Das has been appointed Principal Secretary-2 to Prime Minister Narendra Modi. His appointment, approved by the Appointments Committee of the Cabinet (ACC), will remain co-terminus with the tenure of the Prime Minister or until further orders. Das, a retired IAS officer of the 1980 batch, brings extensive experience in both fiscal and monetary policy, making him one of the most uniquely qualified officials to serve in this role. Before serving as the Governor of the RBI, he held key positions in the Ministry of Finance, including Revenue Secretary and Economic Affairs Secretary, where he played a crucial role in India's financial and economic policymaking. His appointment comes at a crucial time as India navigates global economic challenges, trade tensions, currency fluctuations, and efforts to sustain economic growth. Das's expertise in handling fiscal and monetary policy places him in a strategic position to help the government tackle these economic headwinds effectively. His leadership is expected to play a key role in ensuring economic stability, policy coherence, and strategic financial decision-making at the highest level of government. His deep insights into public finance, market regulation, and economic reforms will strengthen the PMO's economic policy framework, aligning with India's long-term growth and development objectives.

CP PLUS Achieves BIS Certification for ER 01:2024 Compliance

CP PLUS has reinforced its leadership in the security industry by earning the Bureau of Indian Standards (BIS) certification for compliance with ER 01:2024. This certification underscores the company's commitment to delivering high-quality, government-compliant surveillance solutions. ER 01:2024, introduced under the amended Electronics and Information Technology Goods Order, mandates CCTV compliance with IS 13252: Part 1: 2010 and additional security requirements.

CP PLUS

The BIS certification confirms that CP PLUS models meet these stringent standards as per the Ministry of Electronics and Information Technology (MeitY) notification dated April 9, 2024.

As a pioneer in surveillance technology, CP PLUS continues to lead with cutting-edge innovations. The BIS certification not only strengthens consumer trust but also aligns with the 'Make in Bharat' initiative, reinforcing India's self-reliance in security technology. With a focus on innovation and compliance, CP PLUS remains at the forefront of India's surveillance ecosystem, delivering future-ready and globally benchmarked security solutions.

Samsung seeks TN govt's support amid strike

Samsung India has urged the Tamil Nadu government to prioritize worker safety and business continuity as the labour strike at its Sriperumbudur manufacturing facility near Chennai continues. The strike, which began on February 5, follows the suspension of three office bearers from the Samsung India Workers' Union (SIWU), linked to the Centre of Indian Trade Unions (CITU). Despite several mediation efforts by state labour officials, the dispute remains unresolved.

Tensions flared on February 20 when a group of workers allegedly attempted to disrupt operations at the plant. Local police intervened at Vella Gate (White Gate) in Kanchipuram, dispersing the protesters and asking them to vacate the site. In response, Samsung India emphasized its commitment to maintaining a safe and stable workplace, stating, "A certain section of workers once again illegally tried to disrupt operations and industrial peace today. We have a zero-tolerance policy for any illegal activities that disturb industrial stability." While production at the facility remains unaffected, Samsung urged state authorities to ensure worker safety and maintain discipline. The company also warned that any violations of company policies would result in disciplinary action after due process. The Sriperumbudur plant, which employs around 1,800 workers, is crucial to Samsung's operations in India.

India introduces digital pilot licenses

Marking a major step toward digital transformation in India's aviation sector, Civil Aviation Minister K. Rammohan Naidu introduced the Electronic Personnel License (EPL) for pilots on February 20. With this initiative, India becomes the second country in the world, after China, to implement EPL for flight crews.

The EPL is expected to enhance the safety, security, and operational efficiency of Indian aviation. Minister Naidu highlighted that the initiative would bring increased convenience, transparency, and efficiency for pilots while ensuring that India remains at the forefront of technological advancements in the aviation industry. "The launch of EPL by the DGCA is not just a step forward for aviation but also for the future of digitalization across sectors," Naidu said.

Minister Naidu noted that with the rise in domestic air travel, India will require at least 20,000 more pilots in the coming years to meet the growing demand. India is among the fastest-growing aviation markets globally, and this increasing demand for pilots makes initiatives like the EPL essential for the sector's future.

ASUS unveils NUC 15 Pro for enhanced workflows

ASUS has introduced the NUC 15 Pro mini PC, a compact yet powerful machine designed to meet the diverse needs of developers, from AI model training to data visualization. Equipped with the latest Intel Core Ultra (Series 2) processors, DDR5 6400MHz memory, and the Intel Arc GPU, the NUC 15 Pro offers remarkable speed, efficiency, and AI performance, with up to 99 platform TOPS for demanding workloads.

The mini PC also features Intel WiFi 7, providing ultra-fast connectivity with support for up to 16 simultaneous devices and download speeds of up to 46Gbps, allowing for quick data transfers and seamless collaborations. Additionally, Bluetooth 5.4 and Intel WiFi Proximity Sensing enhance connectivity, security, and user experience. With a tool-free access design, the NUC 15 Pro allows easy upgrades for RAM and storage. It also supports multitasking across four 4K displays, making it ideal for SMBs and content creators. The Power Sync feature improves energy efficiency by managing power for connected monitors.

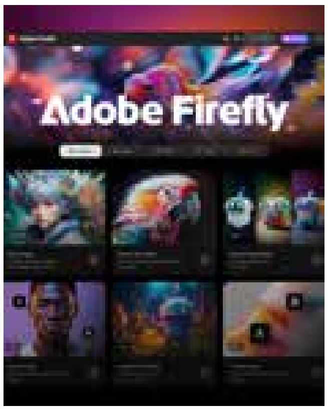
Axis unveils robust thermal cameras for enhanced security

Axis Communications has launched three advanced thermal cameras designed for reliable thermal imaging in any lighting or weather conditions, ensuring low false alarms while safeguarding privacy. The AXIS Q1972-E offers high-resolution thermal imaging in a compact bullet form factor, with four lens options (10 mm, 19 mm, 25 mm, and 35 mm) for versatile installation. Additionally, two box thermal cameras, AXIS Q2111-E and AXIS Q2112-E, provide long-range detection and high-resolution imaging.

The Q2111-E features a 60 mm lens for capturing events at great distances, while the Q2112-E offers multiple lens options for varying field-of-view needs, including long-range capabilities. Both box cameras can be mounted on a positioning unit for a 360° unobstructed field of view. These cameras include AXIS Motion Guard, Fence Guard, Loitering Guard, and AXIS Perimeter Defender with AI-based functionality for enhanced surveillance and security insights. Custom third-party analytics can also be added.

Adobe takes on OpenAI and Google with Firefly app

Adobe has launched the Firefly app, an all-in-one platform for generating images, vectors, and videos, now featuring the Firefly Video Model in public beta. Designed for professionals, Firefly enables seamless ideation and creation of high-quality production work with creative control and multi-modal workflows. The new Firefly Video Model powers both the Generate Video and Generative Extend features in Adobe Premiere Pro, delivering IP-friendly video content for use in production.



Adobe introduced Firefly Standard and Firefly Pro plans, offering premium video and audio features, with access to Firefly's imaging and vector capabilities. Firefly’s integration with Creative Cloud apps like Photoshop, Premiere Pro, and Adobe Express enhances creative projects, allowing users to generate, edit, and refine images and videos seamlessly. Firefly has already generated over 18 billion assets globally, empowering creative professionals to elevate their workflows with advanced AI-driven features.

Acer introduces FA200 PCIe 4.0 SSD for seamless gaming and professional use

Acer has unveiled its FA200 PCIe 4.0 SSD, setting a new standard for high-speed storage with impressive performance, durability, and versatility. Designed for gamers, content creators, and power users, it delivers seamless efficiency across desktops, laptops, and PlayStation 5 consoles. The SSD’s shock- and vibration-resistant design ensures reliable data security in demanding environments. Equipped with Graphene thermal pads, the FA200 maintains optimal cooling to prevent slowdowns, ensuring consistent performance during extended use.

Rajesh Khurana, Country Manager at BIWIN, highlighted the FA200’s speed and reliability, ideal for professionals and gamers. Its compact M.2 2280 form factor fits many devices, making upgrades effortless. Featuring an NVMe 2.0 interface, the FA200 is built for longevity. Acronis True Image software enables easy data migration and backup. Available through Fortune Marketing in India, the FA200 comes with a five-year warranty, transforming data-heavy tasks for professionals and gamers.

Cisco AI Assistant for Webex Contact Center goes live

Cisco has announced the general availability of its AI Assistant on Webex Contact Center, offering support to contact center agents and supervisors. The AI tool is designed to enhance customer service operations by automating routine tasks and providing real-time insights. Jay Patel, SVP & GM of Cisco Webex, highlighted that the AI Assistant helps optimize customer interactions by providing agents with automated guidance, context, insights, and summaries.

Key features include Transfer Context Summaries, Dropped Call Summaries, and Agent Wellbeing. Transfer Context Summaries ensure smooth escalations by providing live agents with conversation summaries. Dropped Call Summaries record interaction details to assist agents if a customer disconnects. Agent Wellbeing detects burnout indicators in real-time, triggering actions like schedule adjustments or breaks. These features collectively improve efficiency and enhance customer service quality.

Fortinet launches its latest G series NGFWs

Fortinet has come up with the latest G series next-generation firewalls (NGFWs): FortiGate 70G, FortiGate 50G, and FortiGate 30G, designed for the modern needs of distributed enterprises. These firewalls are powered by Fortinet’s proprietary ASIC technology and the unified FortiOS, offering exceptional security performance. Featuring advanced networking support and FortiGuard AI-Powered Security Services, they reduce cyberattack risks, future-proof IT infrastructure, and minimize operational costs and environmental impact.

Nirav Shah, Senior Vice President at Fortinet, highlighted the importance of combining cutting-edge technology with sustainability. The FortiGate G series provides unmatched power efficiency, with the 70G offering up to 11x higher IPsec VPN and 7x higher firewall throughput than the industry average, while consuming significantly less energy.

FortiAI, Fortinet’s generative AI assistant, enhances threat detection and incident analysis, automating security tasks. Integrated into the Fortinet Security Fabric, these solutions offer unified management and improved cybersecurity posture, ensuring greater protection across enterprises.

HPE debuts ProLiant servers with AI and advanced security

Hewlett Packard Enterprise has unveiled eight new high-performance servers in its HPE ProLiant Gen12 series, designed to enhance enterprise performance, security, and management with advanced technologies. These servers, powered by Intel Xeon processors, cater to the demanding needs of data centers and edge environments in industries like finance, healthcare, and more. A key feature of the Gen12 servers is the HPE Integrated Lights Out (iLO) 7, which includes a secure enclave providing quantum computing-resistant protection against evolving cybersecurity threats.

HPE's holistic security approach ensures protection from the chip to the cloud, creating an unbreakable chain of trust to prevent firmware attacks. Additionally, the Gen12 servers offer up to 65% better power savings annually compared to legacy systems, with a 41% improvement in performance per watt, supporting energy-efficient operations. These servers also feature AI-driven management, enabling more streamlined, automated processes for modern workloads without sacrificing performance.

Micron powers Samsung Galaxy S25's next-level AI

Micron Technology announced that its cutting-edge low-power LPDDR5X memory and UFS 4.0 storage are now featured in select Samsung Galaxy S25 series devices, which introduce advanced multimodal AI agents for intuitive, context-aware mobile experiences. Additionally, Micron is shipping its most power-efficient LPDDR5X memory, offering over a 10% improvement in power efficiency.

With the One UI 7 update, the Galaxy S25 series delivers personalized, AI-driven experiences that seamlessly integrate text, speech, images, and videos. Power efficiency is also critical, with over 70% of smartphone users stating that battery life is the most important feature they consider when purchasing a phone.

This announcement follows Micron's LPDDR5X and UFS 4.0 validation last fall for the Snapdragon 8 Elite Mobile Platform, a chipset designed to accelerate AI-capable smartphones, in addition to complementing these solutions' inclusion last year in Samsung's AI-centric Galaxy S24 series. Together, these announcements illustrate Micron's close collaboration across the mobile ecosystem, from chipset vendors to smartphone manufacturers, to enable a new generation of flagship smartphones delivering on-device AI.

HID launches FARGO HDP5000e ID printer in India

HID has unveiled the next-generation FARGO HDP5000e, designed to produce vibrant, high-definition photo IDs and credentials. Vishal R Soni, Sales Director of FARGO, Secure Issuance, South Asia, emphasized that the HDP5000e demonstrates HID's commitment to delivering innovative, secure, and reliable identity solutions. Featuring advanced retransfer technology, the printer ensures superior image quality for high-security cards.

Built on the legacy of the renowned HDP5000 series and 25 years of proven retransfer technology, the HDP5000e sets a new benchmark in reliability and usability. Ideal for universities, businesses, healthcare, and government agencies, the HDP5000e is perfect for personalizing contactless cards or upgrading from direct-to-card printers. The versatile and feature-rich printer meets the evolving needs of organizations looking for enhanced image quality and security in card issuance. With robust channel partnerships, HID continues to lead in providing secure identity solutions across India.

Hikvision VDP Multi-Apartment Solution

The Hikvision Video Door Phone Multi-Apartment Solution is redefining residential security by integrating advanced AI, automation, and cloud-based technologies. Tailored for multi-tenant properties, it offers seamless communication, centralized management, and enhanced access control, making it a vital component for modern residential complexes.

The system comprises several key components. The DS-KH9510 Video Intercom Indoor Station features a 10.1-inch IPS touchscreen with real-time video and intuitive controls. It serves as a smart home control hub, integrates emergency alerts via a panic button, and allows remote access through the Hik-Connect app. It also enables flat-to-flat communication and integrates seamlessly with surveillance cameras, offering residents complete situational awareness.

The DS-KD9403-E6 Modular Video Door Station is designed for advanced visitor management, equipped with a high-definition camera, night vision, and a 146-degree wide-angle lens for clear visitor identification. AI-enabled facial recognition and QR code scanning simplify access control. Supporting up to 500 units, it is ideal for large residential buildings. Its robust design, with IP65 and IK07 ratings, ensures reliability in any environment.

Instagram introduces DM scheduling feature for up to 29 days

Instagram has rolled out a new feature allowing users to schedule direct messages (DMs) for later delivery, enhancing the messaging experience with greater flexibility. This feature enables users to choose the exact date and time for their text-based messages, addressing a long-standing request from creators and frequent users. To schedule a message, users can long-press the 'send' button, select a date and time, and a notification will appear in the chat showing pending scheduled messages.

Users can edit, delete, or send scheduled messages immediately by tapping the notification. The feature supports scheduling up to 29 days in advance, though it currently only applies to text-based messages. Photos, videos, GIFs, and voice notes must still be sent in real time. This update is part of Instagram's broader strategy to enhance messaging tools and cater to content creators, businesses, and regular users, offering more control over communication workflows.

WhatsApp rolls out custom chat themes, bubbles, and more

WhatsApp has introduced new features that offer users enhanced personalization and control over their messaging experience. The latest update brings chat themes and an expanded wallpaper selection, available for both individual and group chats on Android and iOS. Users can now personalize chat bubbles and backgrounds, with WhatsApp offering multiple pre-set themes that adjust both elements simultaneously. For even more customization, users can create their own unique themes by mixing and matching different colors.

While the new themes will only be visible to the user who sets them, it provides a more personalized feel compared to shared themes on platforms like Instagram. Additionally, WhatsApp has added 30 new wallpapers to its library, and users can still upload their own images as custom backgrounds. This update allows WhatsApp users to tailor their conversations to their preferences, making each chat more visually appealing and providing a more customized messaging experience.

Sundyne Technologies

A CyberCorp Ltd Company

CYBERCORP

Firewall to a secure world

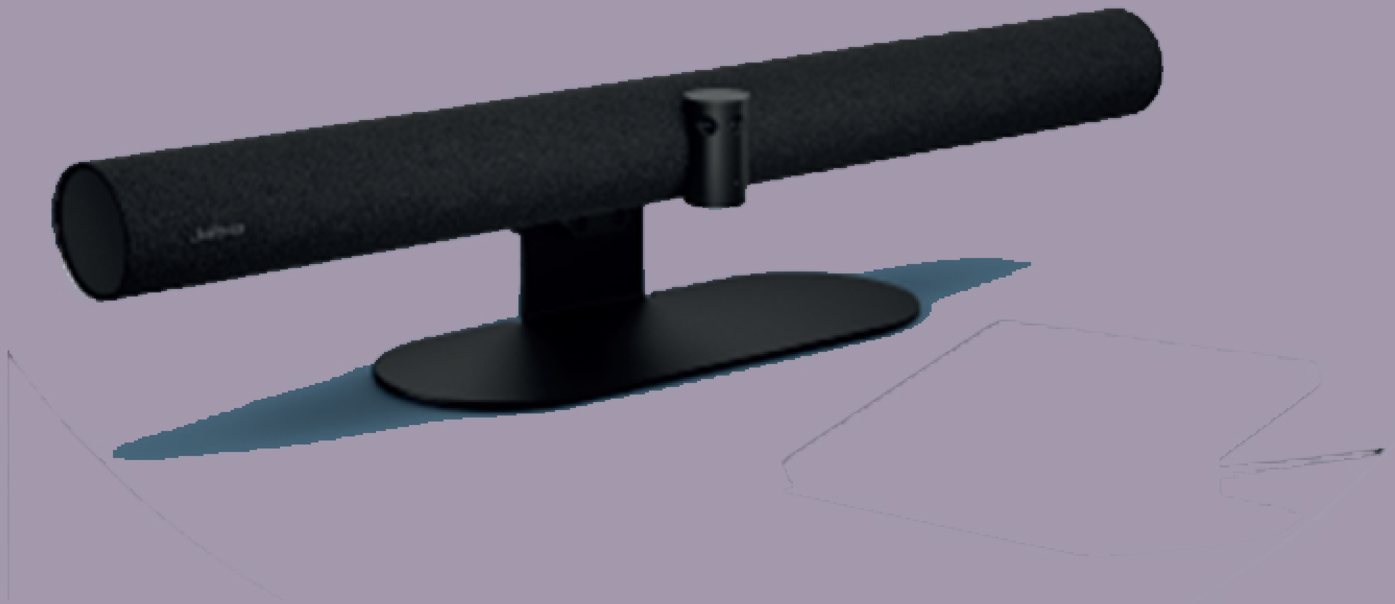
Conquer the Virtual World: Unleash the Power of Virtualization!

Similar to a master magician juggling crystal balls, your business needs seamless control over multiple virtualization software. Our cutting-edge virtualization solutions for Digital Workspaces, Virtual Desktop Infrastructure (VDI) and UCI (Ultra Converged Infrastructure) empower you to secure, manage, and scale effortlessly—without dropping the ball.

Scan the QR code to experience the magic with Sundyne.

For sales and channel partner enquiries, please call us at

☎ + 91 226920 4130 | ✉ info@sundynetech.com | ✉ www.sundynetech.com | www.cyber-corp.com



Jabra

JioHotstar streaming platform is launched

The much-anticipated JioHotstar streaming platform has officially been launched, marking a significant milestone in India's digital entertainment landscape. This new service aims to revolutionize online content consumption by offering a diverse range of movies, TV shows, live sports, and exclusive originals. The Jio Hotstar streaming platform combines the technological prowess of Jio with the vast content library of Disney+ Hotstar. The platform also includes exclusive access to blockbuster movies, premium web series, and live sporting events, making it a comprehensive destination for entertainment lovers.

With the JioHotstar subscription, users can choose from a variety of plans that cater to different audience segments. The platform offers flexible pricing models, ranging from free ad-supported streaming to premium paid subscriptions. JioHotstar subscription plans are designed to be affordable and competitive, ensuring that users get maximum value for their money. In addition, Jio subscribers may receive exclusive benefits, including discounted subscription rates and bundled offers with Jio mobile and broadband services.

Airtel teams up with Nokia to expand 5G FWA nationwide

Bharti Airtel has partnered with Nokia and Qualcomm to expand 5G Fixed Wireless Access (FWA) and Wi-Fi solutions, aiming to provide high-speed internet to millions in India. As part of the arrangement, Nokia will supply Airtel with its 5G Fixed Wireless Access (FWA) outdoor gateway receiver and Wi-Fi 6 Access Point, utilizing Qualcomm Modem-RF and Wi-Fi 6 chipsets. This initiative will enable Airtel to provide superior broadband services in areas where fiber connectivity is either scarce or challenging to implement.

The deployment of fixed wireless broadband access via 5G networks stands out as a significant application of 5G technology, especially in India, which faces low fiber penetration and a high demand for digital services. Airtel will leverage Nokia's FastMile 5G outdoor receivers, which are tailored for multi-dwelling units and capable of serving two households concurrently, thus facilitating a reduction in connection expenses. Airtel will implement Nokia's Wi-Fi 6 access point within residences to enhance the in-home experience.

Altair and LTTS announce 5G-6G Wireless CoE

Leader in computational intelligence, Altair and L&T Technology Services have announced the launch of a groundbreaking 5G-6G Wireless CoE. This will harness the potential of 5G and 6G networks to address prevailing industry challenges like connectivity breakdowns, high operational costs, and slower innovation cycles for applications in segments like Mobility and Tech.

By combining Altair's best-in-class simulation and design tools with LTTS' domain expertise in end- to-end product development and technology services, the CoE will incubate offerings and applications that cut across telecommunications, automotive, manufacturing, healthcare, and beyond. 5G and 6G networks deliver lightning-fast speeds, low latency, and unmatched scalability, while Digital Twins provide real-time, virtual models to predict issues, optimize performance and drive proactive decisions. Together, they empower businesses to boost connectivity reliability, enhance decision-making and improve operational efficiencies.

TRAI bans 10-digit numbers for telemarketing

The Telecom Regulatory Authority of India (TRAI) has come up with a series of new regulations aimed at addressing the issue of spam calls and unsolicited commercial communications (UCC). Effective from February 12, this year, the amendments include TRAI's new telemarketing rule, which prohibits the use of 10-digit numbers for telemarketing. This step is designed to strengthen consumer protection and ensure more transparent marketing practices in the telecom industry.

TRAI's new rules enforce stricter penalties, including a 15-day suspension for first-time violators, blacklisting for repeat offenders, and fines ranging from Rs 2 lakh to Rs 10 lakh for telecom operators failing to comply. The goal is to improve transparency and reduce the occurrence of telemarketing scams and fraudulent calls.

TRAI has also introduced several consumer-friendly initiatives to strengthen telemarketing scam prevention. One key change is the simplified spam reporting process, which now allows consumers to report unwanted calls and messages without pre-registering their preferences.

BharatNet Connects 2.12 Lakh Gram Panchayats

Union Minister Jyotiraditya Scindia announced a major milestone for India's rural connectivity: 2.12 lakh gram panchayats now have access to broadband internet through the BharatNet initiative. This achievement significantly boosts rural digital infrastructure and marks substantial progress towards bridging the urban-rural digital divide.

Scindia emphasized the Modi government's commitment to infrastructure development, noting a five-fold increase in investment compared to the previous UPA government. "Over the past year, we have allocated ▯11 lakh crore to strengthen our infrastructure, compared to ▯2 lakh crore under the UPA," he stated. This investment is fueling growth across multiple sectors, including railways, highways, and telecommunications. Implemented by Bharat Broadband Network Limited (BBNL), the initiative aims to connect 2.5 lakh gram panchayats with high-speed fiber-optic networks. This connectivity is crucial for delivering essential services like education, healthcare, banking, and e-governance to remote villages. The combined impact of BharatNet and the government's substantial infrastructure investments is driving digital inclusion and fostering economic progress across rural India.

TP-Link presents cutting-edge Software-Defined Networking at Tech Sabha 2025

TP-Link India made a notable impact at Tech Sabha 2025 in Hyderabad, a leading e-governance conference, by presenting its advanced Software-Defined Networking (SDN) solution, Omada. Sumith Satheesan, Head of Enterprise Solution Consulting India, discussed how SDN is transforming digital infrastructure, particularly in government initiatives.

Satheesan highlighted how Omada simplifies network management, boosting performance, scalability, and security. The solution supports seamless connectivity for smart cities, digital classrooms, and e-governance platforms, aligning with India's Digital Transformation goals. Omada also empowers CIOs by enabling centralized management of infrastructure, enhancing team efficiency.

TP-Link's cutting-edge features like centralized cloud management and AI-driven network optimization received positive feedback from industry leaders and government officials. The company's participation reinforced its commitment to providing the public sector with reliable, future-ready networking solutions that support India's digital growth and e-governance initiatives. "Tech Sabha showcases TP-Link's Omada platform for resource optimization and seamless operational scaling," said Satheesan.

HERITAGE CYBERWORLD LLP

drona
Detection Response Organization
Network Analysis

We are ISO Certified: #startupindia

India's First AI-Driven Integrated Cyber Security Command and Control Center

OUR SERVICES

SOC
24×7 monitoring detects threats in real time for proactive defense.

DFIR
Expert-led incident response investigates, contains, and mitigates cyber threats swiftly.

NOC
24×7 monitoring optimizes performance, resolves issues, and ensures uptime.

RED TEAMING
Simulated attacks identify vulnerabilities, enhancing security and resilience.

VAJRA EQUIPMENT OF DIGITAL FORENSICS

- **AI DFIR** Laptop and Tablet
- Pre-installed **DFIR Tools,** Datasheet & SOP
- **99.99%** Data Breach Proof
- Get **24* 7 Real Time monitoring** using laptop/tablet

Made In India

www.heritagecyberworld.com
+91 90545 04805
contact@heritagecyberworld.com

Ingram Micro & Udemy Partner to Boost Workforce Upskilling in India

Ingram Micro has announced a strategic partnership with Udemy, a premier online learning platform, to enhance workforce upskilling and improve customer experience across India. This collaboration will leverage Udemy Business' vast content library and Ingram Micro's extensive distribution network to make high-quality learning solutions more accessible. Udemy Business offers nearly 30,000 courses covering technical, business, and power skills, aligning with both companies' missions to drive digital transformation. The partnership aims to equip organizations with the necessary skills and tools to remain competitive in the evolving digital landscape.

NS Bindra, EVP & CCE, Ingram Micro India, emphasized that this partnership marks a significant milestone in delivering value-added services that empower businesses and professionals in the digital era.

Vinay Pradhan, Country Manager & Senior Director, India & South Asia at Udemy highlighted that Ingram Micro's wide distribution reach will enable businesses and educational institutions across India to access Udemy's learning solutions, helping them stay agile and future-ready. This partnership positions Ingram Micro at the forefront of innovation and workforce enablement, integrating Udemy's interactive learning solutions to transform the way businesses approach employee development.

Oracle Strengthens Partner Strategy at CloudWorld Tour Mumbai

At an exclusive partner briefing in Mumbai, held alongside the Oracle CloudWorld Tour Mumbai, Oracle reaffirmed its commitment to driving innovation and business growth through strategic collaborations. The event brought together Oracle PartnerNetwork (OPN) members, including Accenture and Deloitte, to discuss market dynamics and collaborative opportunities.

Lalit Malik, Group Vice President, Alliances & Channels, Oracle Asia Pacific, led the discussion alongside Yatin Patil, Partner & Head of Enterprise Technology & Performance at Deloitte India, and Ankur Aggarwal, MD & Lead - Growth & Strategic Client Relationships at Accenture India. The session underscored the importance of co-creating innovative, next-generation solutions that enhance customer success and business transformation.

Oracle's PartnerNetwork strategy was a key focus, offering a flexible engagement framework for partners to integrate their expertise with Oracle Cloud Infrastructure (OCI), applications, and managed services. Partners can host applications, integrate solutions, or provide consulting and implementation services, ensuring business agility and customer trust. To enhance collaboration, Oracle enables partners to attain Oracle Expertise by meeting key qualifiers such as certifications, customer success stories, and demonstrated commitment to Oracle's ecosystem. By strengthening these partnerships, Oracle continues to empower businesses with cutting-edge cloud and technology solutions.

RAH Infotech Partners with Commvault for India & SAARC Enterprises

RAH Infotech has announced a strategic collaboration with Commvault. This partnership is poised to redefine data resilience and cybersecurity in the Indian enterprise market, delivering robust solutions to tackle the complexities of modern digital ecosystems. This alliance combines Commvault's innovative solutions, including its industry-leading Commvault Cloud Platform powered by Metallic AI, with RAH Infotech's extensive distribution network and customer-centric approach.

Ashok Kumar, Founder and Managing Director of RAH Infotech, emphasized the importance of this partnership, "In today's hyper-connected world, data is not just an asset - it's the foundation of innovation and competitive advantage. Collaborating with Commvault aligns perfectly with our vision to provide best-in-class technology solutions to our clients. Together, we are bringing unmatched expertise and advanced tools to Indian enterprises, enabling them to protect, manage, and extract value from their data in ways that were previously unimaginable."

Commenting on the partnership, Balaji Rao, Area Vice President – India & SAARC, Commvault said, "Our strategy moves resilience from a reactive measure to a proactive safeguard - ensuring continuous security, rapid recovery, and uninterrupted operations. The partnership with RAH Infotech reinforces this vision, combining our cutting-edge innovations with deep market expertise, empowering organizations across India and the SAARC region to mitigate evolving threats and drive sustainable growth."

The partnership aims to address these issues with Commvault's state-of-the-art solutions - including its newly launched cloud - first offerings, Cleanroom Recovery, Cloud Rewind, and Clumio Backtrack - designed to bolster customer resilience in the cloud. With features like early threat scanning, cloud-native data security, automated recovery processes, and rapidly restore cloud applications from outages and ransomware attacks, enterprises can significantly reduce downtime and secure their critical data assets.

Kaspersky expands its B2B footprint with Technobind

Kaspersky has appointed Technobind, a value-added technology distribution company, as its newest business-to-business (B2B) and Technology Alliance partner in India. Technobind can now provide to its customers and partners Kaspersky's complete business security suite as flexible, scalable, on-demand cybersecurity offering to Indian enterprises facing ever-evolving cyberthreats. This strategic partnership marks a significant step in further extending Kaspersky's reach and footprint within India's B2B sector.

Commenting on the partnership, Ernest Chai, Head of Channel for Asia Pacific at Kaspersky said, "India is a key market for Kaspersky, and our collaboration with TechnoBind is another significant step towards expanding our reach in the local cybersecurity market. TechnoBind's expertise in value-added distribution and its strong foothold in the Indian IT landscape make them an ideal partner to deliver our solutions to more enterprises and SMBs alike."

"We are thrilled to partner with Kaspersky and expand our cybersecurity portfolio with their globally trusted security solutions. This partnership aligns with our mission to bring sophisticated cybersecurity technologies to enterprises, ensuring they are well-equipped to combat modern cyber threats. With our strong partner ecosystem, we aim to accelerate the adoption of Kaspersky's solutions across businesses in India," said Prashanth GJ, CEO, TechnoBind.

Through this alliance, TechnoBind will leverage its deep channel expertise and robust partner network to drive the adoption of Kaspersky's industry-leading endpoint security, threat intelligence, and cyber defense solutions across various industry verticals.

FRUX

Frux Technologies Pvt. Ltd.

A technology distributor committed to restoring the lost "value" in value-added distribution, driving demand, and boosting revenue.

Our Alliances

Data Resolve	UBA Based DLP | Insider Threat Management | Employee Productivity & Monitoring | Print and Email DLP
InstaSafe Cloud. Secure. Instant.	ZTNA | ZTAA | Secure Remote Access | Multi Factor Authentication | Identity & Access Management
DocQ	Document Management System | Process Automation | Learning Management Solution | IPASS
haltdos	Anti-DDoS, Server Load Balancer, Link Load Balancer, WAF, ADC, GSLB
ACCELPRO	ZTNA | Multifactor Authentication
SecneurX	Threat Intel, Breach Attack Simulation, Malware Analysis(SandBoxing), Email Security, CDR
CYBERSRC SECURITY RISK COMPLIANCE Simplifying Cyber Risk Management..	External Threat Intelligence, Surface Attack Monitoring, Dark Web, Deep Web Monitoring, Brand Protection
mobisec Cybersecurity Enablers	Mobile Device Management, Mobile Threat Detection & Mitigation
xcitium	EDR , XDR ,MDM , Endpoint Protection
NEXAPP	4G LTE Router | Access Points | SD-WAN
SONICWALL	NGFW | Email Security | ZTNA | Acceess Point | Switches | End Point Security | Cloud Security
Prophaze The New Phase of Security	API SECURITY , WAF , BOT Protection , DDoS Protection , CDN
tapplent	Global HR Suite | Talent & Rewars Suite | Recruiting Suite | Learning Suite

Email: sales@fruxtech.com | Ph: +919999055082

DATA CENTERS
Get Smart With AI

With increasing digital transformation and cloud adoption, AI is enhancing efficiency, security, and automation in Indian data centers. AI-driven predictive maintenance, energy optimization, and real-time threat detection are revolutionizing operations, reducing downtime, and cutting costs. As we enter 2025, VARINDIA attempts to examine how Indian enterprises leverage AI to streamline workload management and improve scalability. Exploring the evolving role of AI in data centers across India, analyzing current trends, challenges, and future potential, we spoke with various industry players to understand the AI's transformative impact on India's data center landscape.

The rapid digital transformation across industries has significantly increased the demand for data centers. In this evolving landscape, Artificial Intelligence (AI) is playing a crucial role in optimizing operations, enhancing efficiency, and ensuring the security of data centers. In India, where digital adoption is growing exponentially, AI-driven data centers are becoming essential for meeting the rising computational and storage demands.

AI-DRIVEN EFFICIENCY IN DATA CENTERS

One of the primary roles of AI in data centers is improving efficiency. AI-powered automation helps manage workloads dynamically, optimize server utilization, and reduce energy consumption. By leveraging machine learning algorithms, data centers can predict demand patterns and allocate resources accordingly, leading to better cost management and reduced wastage. This is particularly beneficial in India, where power costs and availability remain a challenge.

Market Potential for Data centers

- Cloud Computing & IT Services
- Banking, Financial Services & Insurance (BFSI)
- E-Commerce & Retail
- Healthcare & Life Sciences
- Telecommunications & 5G Networks
- Media & Entertainment
- Government & Smart Cities
- Manufacturing & Industry 4.0
- Education & EdTech

Google's DeepMind AI, for example, has helped reduce cooling costs in data centers by up to 40%. Similar AI-powered cooling techniques are being explored in India, where rising temperatures and power constraints make energy efficiency a priority. AI can monitor and adjust cooling systems in real-time, ensuring optimal performance while minimizing costs.

PREDICTIVE MAINTENANCE AND DOWNTIME REDUCTION

AI-driven predictive maintenance is another critical advantage for data centers. Traditional maintenance methods often rely on scheduled servicing, which can lead to inefficiencies and unexpected failures. AI-based monitoring systems analyze vast amounts of sensor data to detect anomalies and predict hardware failures before they occur. This proactive approach minimizes downtime and ensures uninterrupted service.

In India, where industries like banking, e-commerce, and telecommunications rely heavily on data centers, minimizing downtime is crucial for business continuity. AI-powered monitoring tools help companies maintain operational efficiency, reduce repair costs, and extend the lifespan of hardware components.

AI FOR CYBERSECURITY IN DATA CENTERS

With increasing cyber threats, AI is playing a pivotal role in strengthening data center security. AI-driven security systems analyze network traffic, detect unusual patterns, and identify potential security breaches in real-time. By leveraging machine learning, these systems can adapt to new threats, making them more effective than traditional rule-based security measures.

India's data security landscape is evolving rapidly, with increasing concerns over data breaches and cyberattacks. AI-powered security solutions help protect critical infrastructure by identifying vulnerabilities, automating threat response, and mitigating risks before they escalate.

AI'S ROLE IN SUPPORTING INDIA'S DIGITAL EXPANSION

The Indian government's Digital India initiative and the rise of 5G connectivity are accelerating the need for robust data center infrastructure. AI is playing a significant role in enabling this transformation by optimizing data storage, managing network traffic, and improving overall performance.

Furthermore, AI is helping data centers manage the increasing workload from cloud computing, IoT, and AI-based applications. As India moves towards becoming a global digital hub, AI-driven data centers will be instrumental in ensuring seamless operations and scalability.

FINALLY…

AI is revolutionizing data centers worldwide, and India is no exception. By enhancing efficiency, reducing downtime, bolstering security, and supporting digital expansion, AI is transforming data center management in India. To conclude we can say that as industries embrace digital transformation, data centers are becoming the backbone of business operations, ensuring scalability, security, and efficiency. And, as technology continues to evolve, AI will remain at the forefront of innovation, driving sustainable and intelligent data center operations in the country.

Equinix's Three-Dimensional Approach to AI-Ready Infrastructure

MANOJ PAUL

Managing Director- India, Equinix

At Equinix, we're analyzing heterogeneous, unstructured data sets to extract and export information about the equipment and parts inventory in our Equinix IBX data centers. We're running Coral TPUs on IoT devices to bring local AI capabilities into our Equinix IBX sites. We're also performing a proof of concept for using AI-enabled IoT devices to predict failures of chiller pumps and UPS (uninterruptible power supply systems). This could ultimately lead to more resilient data centers for our customers.

LEVERAGING AI: AUTOMATION, OPERATIONAL EFFICIENCY AND COOLING SOLUTIONS

Equinix is transforming its infrastructure to meet growing AI demands through a three-pronged strategy. First, we're deploying advanced cooling solutions like direct-to-chip liquid cooling, boosting energy efficiency by up to 40%. Second, we're investing in sustainability with microgrids, renewable energy integration, and next-gen battery technologies. Third, we're driving collaboration between chip developers, infrastructure providers, and utilities to build efficient, future-ready data centers.

With AI advancements like Blackwell chips and new algorithms, our infrastructure supports both current and future AI processing, particularly AI inferencing. Equinix's vendor-neutral approach ensures seamless deployment of preferred hardware with optimized performance.

AI ENHANCED CYBERSECURITY MEASURES

We are implementing AI-driven security capabilities to protect our customers' systems and hosted data from evolving threats. AI models rely on high-quality data, and cybersecurity is no exception—we need diverse threat intelligence sources to identify and mitigate risks effectively.

To achieve this, we have established threat intelligence exchanges, enabling collaboration with industry and government partners.

These exchanges enhance visibility into threat indicators, allowing for proactive defense. By working within a robust ecosystem, we strengthen our ability to detect, analyze, and respond to cyber threats, ensuring a secure environment for our customers and their critical data.

EQUINIX'S DATA CENTER- COMPETITIVE EDGE

Equinix sets itself apart with a comprehensive AI infrastructure strategy. Through Private AI, we ensure data privacy and control while offering multicloud capabilities across 260+ data centers in 70+ metros. Our high-performance network connects 10,000 enterprises, 2,000 networks, and 3,000+ service providers, optimizing AI workload traffic. Unlike traditional colocation providers, we deliver advanced interconnection services, enabling seamless connectivity with Cloud Service Providers, Carriers, and Enterprises. Strategic partnerships with NVIDIA and HPE provide customers with flexibility and choice. Our ecosystem democratizes AI access, balancing high performance with cost efficiency to support evolving AI inferencing needs.

ESDS: Advancing AI-Powered Cybersecurity and Sustainable Data Centers

JITENDRA PATHAK
COO - ESDS

We leverage AI to automate operations, including cloud orchestration, predictive maintenance, and real-time monitoring. Our in-house AI-driven solution optimizes workloads, enhances server performance, and reduces downtime through proactive maintenance. With 20 years in the industry, we utilize vast datasets (securely and ethically) to refine pattern forecasting and failure prediction. AI-driven analytics boost efficiency while improving customer experience with scalable self-service solutions. By integrating AI across operations, we enhance reliability, minimize disruptions, and ensure seamless cloud management, delivering a smarter, more responsive, and efficient infrastructure for our users.

LEVERAGING AI: AUTOMATION, OPERATIONAL EFFICIENCY AND COOLING SOLUTIONS

ESDS is continuously enhancing its data center capabilities to meet the rising demands of AI workloads. We are investing in efficient AI models that require fewer resources while maintaining high performance. Our scalable cloud architecture enables enterprises to expand compute capacity dynamically without infrastructure bottlenecks. AI-driven resource allocation optimizes workload distribution, reducing latency and enhancing efficiency. Our R&D focuses on sustainable AI computing, aligning growth with energy-efficient practices. AI-powered cooling systems leverage real-time sensor data to optimize airflow, improving Power Usage Effectiveness (PUE) by dynamically adjusting cooling mechanisms based on heat distribution patterns for maximum efficiency.

AI ENHANCED CYBERSECURITY MEASURES

Cybersecurity is an utmost priority for ESDS, and AI plays a vital role in building the security framework. Security monitoring of network traffic, coupled with logs and events generated by various IT systems, ensures the tracking of activities for anomalies and potential threats in real time. We, in conjunction with our partners, leverage machine learning models to examine patterns in a bid to detect and neutralize sophisticated cyber threats and zero-day attacks. These systems analyze patterns, detect anomalies, and proactively respond to threats to provide robust protection for our data center infrastructure and customer environments, including data.

ESDS' DATA CENTER- COMPETITIVE EDGE

ESDS stands out in AI-powered data centers with a focus on innovation, sustainability, and customer-centric solutions. Our trademarked eNlight Cloud technology leverages AI for auto-scaling, optimizing resource utilization. We prioritize green computing, integrating AI-driven power and cooling management for energy efficiency. Our Government Community Cloud, backed by MeitY empanelment, ensures secure, compliant AI-driven infrastructure. ESDS leads with future-ready data centers, combining industry expertise, automation, and sustainability. With well-defined processes, a dedicated team, and in-house monitoring systems, we proactively detect and resolve irregularities, ensuring seamless operations and a robust, intelligent data center ecosystem.

AI-Powered Data Centers: Enhancing Threat Detection and Operational Efficiency

RAGHUVEER SUBODHA
Executive Director - Cloud Platform Architecture and Engineering
EY Global Delivery Services

AI is transforming cybersecurity by enabling rapid threat detection and proactive responses in data centers. Using machine learning, Large Language Models (LLMs), and distilled models, AI analyzes behavior patterns in real time, improving detection of suspicious activity. Continuous training enhances its ability to identify threats before escalation, minimizing breaches. By monitoring logs and network traffic, AI anticipates emerging threats and adapts defenses efficiently. Automated responses also reduce mitigation time, lowering risk exposure and strengthening overall security while optimizing resource allocation for a more resilient cybersecurity framework.

LEVERAGING AI: AUTOMATION, OPERATIONAL EFFICIENCY AND COOLING SOLUTIONS

AI-driven models, including Large Language Models and distilled variants, are transforming data center operations by enabling proactive server utilization, cooling, and power optimization. These systems analyze vast datasets and undergo fine-tuning for specific parameters, extending equipment lifespan and reducing manual workload. AI detects potential failures before they occur, minimizing downtime and costly outages. Automated resource allocation enhances capacity planning, scaling operations dynamically based on real-time demand. Additionally, AI-driven insights provide faster, precise recommendations, streamlining complex decision-making and significantly improving operational efficiency while ensuring data centers run more sustainably and cost-effectively.

EY GDS'S DATA CENTER- COMPETITIVE EDGE

The need for preparing data centers of the future is of paramount importance now, given the increasing computational demands for AI workloads. Investments in high-performance s Graphics Processing Units (GPUs), Tensor Processing Units (TPUs) and flexible storage systems are coupled with cloud-native technologies like containerization and microservices for seamless scalability. Moving to cloud-smart approach that enables iterative architectures, placing of workloads in an optimized manner, and so on enables data centers to not only manage workloads but be ready for informed and optimised scaling. AI-driven resource management optimizes power usage, cooling and workload distribution both on-premises and in the cloud. Hybrid and multi-cloud strategies provide agility, enabling data centers to scale on demand while maintaining cost efficiency. Advanced automation, predictive maintenance, and real-time AI-powered analytics enable dynamic resource allocation and prevents downtime. Sustainable data centers are the need of the hour, and that is driving data centers to implement energy-efficient cooling and renewable energy sources.

Sify's AI- Ready Data Centers: Scalable, Smarter, Greener, and More Resilient

ROOPESH KUMAR

Head- Data Center Projects, Sify Technologies Ltd

At Sify's data centers, we look at AI from two perspectives. Firstly, to enable enterprises to host dense AI workloads which needs scalable, purpose-built infrastructure, robust power supply tolerant to dynamic load variations, modern cooling methodologies like liquid immersion and high capacity low latency network connectivity. Secondly, how can we incorporate AI in our Data Center Operations for enhanced automation, efficiency, and sustainability to eventually serve our customer better.

Beyond the obvious, AI optimizes energy use, dynamically adjusts cooling, and distributes workloads to reduce costs and extend infrastructure lifespan. AI-driven predictive maintenance prevents downtime, while digital twin technology enables informed decision-making. These innovations ensure a scalable, smarter, greener, and more resilient data center ecosystem.

LEVERAGING AI: AUTOMATION, OPERATIONAL EFFICIENCY AND COOLING SOLUTIONS

Managing the heat output efficiently is critical in the DC. Besides direct-to-chip, liquid immersion cooling technologies, we have implemented enhanced thermal management and lower energy costs. Edge & Distributed AI Computing minimizes latency by processing data closer to the source and optimizing performance. Sustainability initiatives include energy partnerships and AI-driven workload scheduling. Scalable & Modular Infrastructure enables seamless expansion using a POD-based model, ensuring adaptability to growing demands. Our AI-powered cooling solutions enhance efficiency and performance. AI-Driven Dynamic Cooling adjusts systems in real time using sensor data, optimizing energy use. Liquid Cooling with AI Optimization regulates coolant flow for high-density workloads, ensuring efficient heat dissipation and proactive failure prevention. Smart Airflow modifies fan speeds and optimizes airflow using Computational Fluid Dynamics (CFD). These innovations enable a more energy-efficient, resilient, and cost-effective DC environment.

AI ENHANCED CYBERSECURITY MEASURES

Our DCs leverage AI-driven security for enhanced threat detection, response, and risk mitigation, analysing network traffic in real time, detecting anomalies and zero-day vulnerabilities. Automated incident response isolates threats instantly, predictive intelligence pre-empts cyberattacks, and behavioral analytics detect insider threats.

SIFY DATA CENTERS- COMPETITIVE EDGE

Sify is making bold moves in AI-driven infrastructure with a $5 billion commit. Scaling its data center footprint, integrating AIOps, and acquiring GPUs, Sify's AI-workload ready hyperscale data center campuses are spread across Noida, Mumbai, and Chennai. As an NVIDIA colocation partner, it has secured liquid cooling certification for GPUs up to 130kW per rack. Expanding beyond metros, Sify is launching AI inferencing facilities in Tier-II cities starting with Lucknow. On its commitment to sustainability, Sify has already contracted for 231 MW renewable energy, reinforcing its leadership to sustainable AI-driven infrastructure.

AI-Driven Efficiency & Sustainability in Yotta's Hyperscale Data Centers

ROHAN SHETH

Head – Colocation, Data Center Build and Global Expansion, Yotta Data Services

At Yotta, we are harnessing AI to optimize our data center operations across multiple dimensions. In physical security, AI-powered surveillance systems continuously monitor and analyze activities in real time to enhance response measures. However, the most transformative impact has been in AI-driven energy management, where energy constitutes a significant portion of both capital and operational expenditures costs. By leveraging AI to dynamically adjust GPU and server states based on real-time workload demand, we are achieving substantial energy savings while maintaining peak performance.

LEVERAGING AI: AUTOMATION, OPERATIONAL EFFICIENCY AND COOLING SOLUTIONS

AI is transforming data center operations with predictive analytics and automated monitoring, identifying and addressing issues before escalation. As AI adoption grows, high-uptime, scalable infrastructure is essential. Yotta is expanding its hyperscale data centers with Nvidia H100 GPUs to support AI model training and inferencing at scale. Shakti Cloud, India's first AI-centric GPU cloud, features 16,384 Nvidia GPUs for seamless AI scaling. Yotta integrates advanced cooling solutions—air-cooled chillers, RDHx, and liquid immersion cooling—to enhance efficiency and sustainability. By evolving beyond traditional storage, Yotta ensures AI workloads operate efficiently, making AI-driven data centers the future of intelligent computing.

AI ENHANCED CYBERSECURITY MEASURES

Yotta's in-house cybersecurity suite, Suraksha, leverages AI and machine learning to proactively monitor, detect, neutralize threats in real time, enabling rapid incident response. Its smart CSOC security framework provides comprehensive prevention, detection, and threat hunting, backed by a dedicated team of security experts. Suraksha offers a 360-degree view of security incidents and seamlessly integrates with existing security stacks, allowing for quick and efficient deployment. Additionally, Gen AI is revolutionizing cybersecurity training, enabling realistic, AI- driven simulations of cyber-attack scenarios that help cybersecurity professionals refine decision-making and baseline threat detection capabilities.

YOTTA'S DATA CENTER- COMPETITIVE EDGE

AI-optimized infrastructure is crucial for managing complex AI workloads. Data centers must invest in HPC, specialized GPU clusters, and intelligent cooling to support large-scale AI training and inferencing. India's AI growth relies on robust, scalable, low-latency data centers for mission-critical applications. Yotta leads this shift with H100 GPUs and hyperscale infrastructure expansion. Prioritizing sustainability, Yotta optimizes energy use, sourcing renewable energy. NM1 in Navi Mumbai operates on 80% green energy, while Yotta D1 in NCR-Delhi runs entirely on 100% green energy, ensuring efficiency and eco-friendly AI operations.

REIMAGINING JUSTICE:

HOW TECHNOLOGY CAN TRANSFORM INDIA'S COURTS

NEW TECHNOLOGICAL SOLUTIONS ADDRESS KEY CHALLENGES IN THE INDIAN JUDICIAL SYSTEM, OFFERING HOPE FOR FASTER, MORE ACCESSIBLE JUSTICE

In a candid address that cut through typical bureaucratic rhetoric, Honourable Justice Girish Kathpalia of the Delhi High Court recently outlined a vision for technological transformation that could reshape India's judicial landscape. His speech highlighted a critical truth: India's courts are not just venues for legal proceedings—they are information processing hubs handling millions of documents, testimonies, and decisions daily.

As India's judiciary grapples with a backlog of over 40 million cases, Justice Kathpalia's practical assessment provides a roadmap for how strategic technology deployment could address the system's most pressing challenges. His vision goes beyond digitization to reimagine the very processes that have defined Indian courts for generations.

BREAKING DOWN SILOS: THE PROMISE OF INTEROPERABLE SYSTEMS

Perhaps the most immediate challenge identified by Justice Kathpalia is the fragmentation of India's criminal justice system. Currently, different departments—from police stations to prisons to courtrooms—operate on disparate, often incompatible technological platforms. This creates what technologists call "information silos," preventing the seamless flow of critical data.

The consequences can be profound and deeply human. Justice Kathpalia cited cases where bail orders took a month to reach prisoners, meaning individuals legally granted freedom remained incarcerated due to communication failures. Such delays not only violate rights but erode public trust in the judicial system.

The Interoperable Criminal Justice System (ICJS) represents India's attempt to address this challenge. This ambitious initiative aims to connect police stations, courts, prisons, forensic laboratories, and prosecution agencies through a common digital backbone. However, its success depends on overcoming significant hurdles.

The first challenge is technical compatibility. Legacy systems built on different technological foundations must somehow communicate effectively. This requires not just software solutions but standardized protocols for data sharing. The second challenge is institutional: agencies accustomed to operating independently must embrace collaborative approaches and information sharing. Early ICJS implementation has shown promising results in pilot districts. When fully realized, the system could dramatically reduce case processing times. A bail order could reach jail authorities within minutes rather than weeks, and police verification reports could be instantly accessible to judges making remand decisions. For ordinary citizens, this means justice delivered more swiftly and reliably.

SECURING JUSTICE: DATA PROTECTION AND CYBERSECURITY

As courts digitize their operations, they become repositories of sensitive information. Justice Kathpalia highlighted the vulnerability of this transition period, noting that while judicial records are increasingly stored on servers, India lacks a comprehensive legal framework governing this digital ecosystem.

The Delhi High Court's initiative to maintain a duplicate server in Madurai represents a pragmatic approach to disaster recovery, but it addresses only one dimension of a multifaceted challenge. A truly robust data protection strategy requires clear protocols for data classification, access controls, encryption standards, and regular security audits.

Recent incidents have underscored the urgency of addressing these vulnerabilities. Justice Kathpalia referenced a court hacking incident that exposed weaknesses in existing security infrastructure. As courts digitize more of their operations, they become increasingly attractive targets for cybercriminals and other malicious actors.

The emergence of deepfake technology creates additional concerns. Justice Kathpalia warned that manipulated evidence—from doctored documents to fabricated testimony—could undermine the very foundation of fact-finding in courts. Addressing this threat requires both technological countermeasures and procedural safeguards.

Effective solutions will likely combine multiple approaches. AI-driven security protocols can identify unusual patterns that might indicate intrusion attempts. Blockchain technology could provide tamper-proof records of document authenticity. Most importantly, a culture of security awareness must permeate all levels of the judicial system, from judges to clerical staff.

AUGMENTING JUDICIAL INTELLIGENCE: THE ROLE OF AI

Justice Kathpalia's vision extends beyond security to the very cognitive processes of judges themselves. With hundreds of cases on daily dockets, judges must absorb and analyze vast amounts of information. AI-powered tools offer the potential to augment judicial intelligence without replacing critical human judgment.

Automated transcription represents low-hanging fruit in this domain. Currently, court reporters manually transcribe proceedings, creating bottlenecks and potential for error. Voice recognition technology, customized for legal terminology and Indian accents, could produce real-time transcripts with increasing accuracy.

More ambitious is AI-driven document summarization. Justice Kathpalia suggested that such tools could help judges quickly extract the essence from lengthy submissions. Advanced natural language processing algorithms can already identify key arguments, relevant precedents, and statutory references in legal documents. When deployed thoughtfully, these tools could allow judges to focus their intellectual energy on the most complex aspects of cases.

The justice was careful to acknowledge the limitations of these technologies. Legal reasoning involves nuance, context, and ethical considerations that current AI systems cannot fully grasp. The goal is augmentation rather than automation—providing decision support while preserving the irreplaceable human elements of judgment.

Implementation challenges include ensuring accuracy, addressing bias in algorithms, and maintaining transparency in how AI tools influence judicial work. A phased approach, beginning with straightforward applications like document classification before moving to more complex analytical tasks, offers the most promising path forward.

BRIDGING LANGUAGE BARRIERS: VERNACULAR TECHNOLOGIES

In a country with 22 official languages and hundreds of dialects, language poses a unique challenge for India's courts. Justice Kathpalia highlighted the need for real-time vernacular-to-English text conversion technologies to help judges work across linguistic boundaries.

The technical challenges are substantial. Indian languages feature complex scripts, context-dependent meanings, and idiomatic expressions that resist literal translation. Local expressions—what linguists call "regionalisms"—pose particular difficulties for machine translation systems.

Yet recent advances in neural machine translation offer hope. Systems trained on legal corpora in multiple Indian languages are showing increasing accuracy in specialized judicial contexts. These technologies could significantly reduce delays caused by translation requirements and enable faster case processing.

The benefits would extend beyond judges to litigants themselves. Many Indians who appear in court struggle to understand proceedings conducted in unfamiliar languages. Real-time translation could make justice more accessible to ordinary citizens, regardless of their linguistic background.

TRUTH ASSESSMENT: FROM HUMAN PERCEPTION TO TECHNOLOGICAL ASSISTANCE

Perhaps the most intriguing application mentioned by Justice Kathpalia involves technologies for credibility assessment. Judges have traditionally relied on their perception of witness demeanor to evaluate truthfulness—a notoriously subjective process.

While acknowledging that judges are human and subject to the same cognitive biases as others, Justice Kathpalia suggested that facial recognition technologies could potentially assist in truthfulness assessment. Such systems analyze microexpressions and physiological indicators that might escape human notice.

However, he was careful to note the limitations of such approaches. Current technologies cannot provide certainty about deception, and there are significant ethical questions about their use in judicial settings. Cultural differences in emotional expression further complicate their application in India's diverse society.

A balanced approach might involve using such technologies as one input among many in credibility assessment, rather than as definitive truth detectors. Proper training would be essential to ensure judges understand both the capabilities and limitations of these tools.

ADMINISTRATIVE EFFICIENCY: LAND RECORDS, VOTER VERIFICATION, AND DOCKET MANAGEMENT

The final use cases mentioned by Justice Kathpalia focus on administrative functions that, while less visible than courtroom proceedings, are vital to justice delivery. Technological solutions can bring transparency and efficiency to land record management, voter verification, and docket management.

Digital land records, when properly implemented, can reduce property disputes that currently flood India's courts. Blockchain-based systems offer particular promise, creating immutable records of ownership and transactions. Several Indian states have already begun implementing such systems, though challenges remain in digitizing historical records and addressing boundary disputes.

Voter verification technologies can strengthen democratic processes while reducing election-related litigation. Biometric identification systems, when coupled with proper privacy safeguards, can help prevent electoral fraud while streamlining the voting process.

Intelligent docket management systems represent perhaps the most direct way technology can address court backlogs. By analyzing case characteristics, such systems can optimize scheduling, balance judicial workloads, and identify opportunities for consolidation of similar cases. Some Indian courts have already seen significant efficiency gains from initial implementations of such systems.

THE PATH FORWARD: LEADERSHIP AND INTEGRATION

Throughout his address, Justice Kathpalia emphasized a critical enabler for all these technological advances: sustained leadership in IT departments. Without dedicated experts possessing what he called "missionary zeal," technological initiatives tend to falter. High turnover in government IT departments has historically undermined continuity in digital transformation efforts.

The solution lies in creating specialized career tracks for judicial technology experts who can bridge the worlds of law and technology. These professionals need competitive compensation, opportunities for advancement, and institutional support to drive long-term innovation.

Equally important is a comprehensive approach to technology implementation. Rather than isolated solutions addressing individual pain points, the judiciary needs an integrated digital ecosystem where different applications work in harmony. This requires careful architectural planning and governance structures that span traditional departmental boundaries. Justice Kathpalia's insights offer a blueprint for a technology-enabled judiciary that could transform how justice is delivered in India. The technologies he describes are not futuristic fantasies but practical solutions, many already deployed in other sectors or jurisdictions.

By focusing on interoperability, security, judicial augmentation, language technologies, truth assessment, and administrative efficiency, India's courts can address their most pressing challenges. The result would be not just a more efficient system but a more trustworthy one—a judiciary where justice is not only done but is seen to be done, swiftly and accessibly, for all citizens.

CYBER & DATA SECURITY SUMMIT 2025
STRENGTHENING DIGITAL RESILIENCE

Girish Kathpalia

DIGNITARIES AT THE INAUGURATION OF CDS 2025

Tarun Pratap Singh

Dr. Pavan Duggal

Prof. Amlan Chakrabarti

Anuj Aggarwal

Dr. Harold D'costa

Tarun Pratap Singh

Ram Vaidyanathan

Nakul Khandelwal

Rajaram Venkatesan

PANEL DISCUSSION I: DATA PRIVACY: A TICKING TIME BOMB FOR THE INDUSTRY

Panel Discussion II: Mitigating Secu

ATTENDEES
300+

POWER-PACKED PANEL DISCUSSIONS
3

SPEAKERS
20+

e-BOOK LAUNCH

Dr. Pankaj Dixit

B. Shanker Jaiswal

Prof. Kamaljeet Sandhu

Brijesh Singh, IPS

Ms. Deepa Ojha

Dr. Rakshit Tandon

Aman Thareja

Lee Nocon

Akshay Garg

Tarun Pratap Singh

CDS - Winners

rity Risks in Emerging Technologies

Panel Discussion Session III : From Risk to Resilience

Cyber & Data Security Summit 2025 Strengthening Digital Resilience

Cybersecurity is a shared responsibility, and through collaboration, businesses, corporations, CIOs, CTOs, and CISOs can foster a safer and more resilient digital world. With this fundamental principle in mind, the 9th edition of the Cyber & Data Security Summit 2025 was held in New Delhi. The event's theme, 'Recognizing Excellence in Digital Innovation', emphasized the need to build a secure, digital-first future where innovation and security are seamlessly integrated.

The summit focused on addressing the ever-evolving challenges posed by cyber threats and data security. It provided a platform for insightful discussions, keynote addresses, expert presentations, corporate insights, and valuable networking opportunities with cybersecurity and data privacy experts.

The event was graced by eminent dignitaries, including names like Shri B. Shanker Jaiswal, IPS, Joint CP (Operations & Licensing), Delhi Police, Brijesh Singh, IPS, ADGP Police & Principal Secretary to the Chief Minister, Government of Maharashtra, Justice Girish Kathpalia, Judge, Delhi High Court, Dr. Pavan Duggal, Advocate, Supreme Court of India, Lee Nocon, Co-Founder & CTO, Data Safeguard India, Prof. Kamaljeet Sandhu, University of New England, Australia, Prof. Amlan Chakrabarti, Director, A.K. Choudhury School of IT, University of Calcutta and Dr. Harold D'Costa, President, Cyber Security Corporation.

The event commenced with a welcome address by Dr. Deepak Kumar Sahu, Editor-in-Chief of VARINDIA. He spoke about the emerging trends in cybersecurity and artificial intelligence, highlighting India's significant strides in AI development. He mentioned the government's announcement of an indigenous Large Language Model (LLM) expected to be completed within ten months while also pointing out the rising cybersecurity threats. India ranks second globally in cyberattacks, with 95 organizations suffering data breaches in 2024, underscoring the need for enhanced security measures.

Dr. Pavan Duggal, Advocate, Supreme Court of India, delivered the inaugural address, engaging the audience with his insights into current cybersecurity trends and practices.

Followed by Shri B. Shanker Jaiswal, IPS, Joint CP (Operations & Licensing), Delhi Police, who provided an overview of cybercrime and digital security, discussing the future landscape of cybersecurity challenges and solutions.

Dr. Rakshit Tandon, Cybersecurity Evangelist & Risk Advisory Expert, spoke about AI's role in cybersecurity and how it could drive the next generation of cyberattacks.

Guest of Honour Brijesh Singh, IPS, ADGP & Principal Secretary to the Chief Minister of Maharashtra, delivered an inspiring address on cybersecurity and digital transformation, reinforcing the importance of proactive security measures.

While, Deepa Ojha, Manager, Privacy & Policy, DSCI, addressed data protection for a Digital India, then Dr. Pankaj Dikshit, CTO – GeM, Government of India, shared insights on securing IT systems against AI-generated threats. Given the event's focus on the current DPDPA, Anuj Aggarwal, Chairman of the Centre for Research on Cyber Crime & Cyber Law, leveraged the platform to provide insights into the challenges associated with DPDP implementation.

Prof. Kamaljeet Sandhu, University of New England, spoke on the challenges and opportunities AI presents for global cybersecurity leaders. Dr. Harold D'Costa, President of Cyber Security Corporation, provided the audience with an in-depth techno-legal perspective on mitigating cyber-attacks. He elaborated on the evolving nature of cyber threats, the legal challenges in prosecuting cybercriminals, and the need for stronger regulatory frameworks to enhance cybersecurity resilience.

Building on this, Hon'ble Justice Girish Kathpalia of the Delhi High Court delivered a compelling keynote address, taking the discussion to the next level. He outlined six critical use cases from the Indian judiciary where technology, particularly artificial intelligence (AI), could drive significant transformation. Justice Kathpalia emphasized that when applied responsibly, AI has the potential to revolutionize legal proceedings, streamline case management, and enhance judicial efficiency.

CDS 2025 had three interesting information loaded panel discussions. The first panel discussion, themed 'Data Privacy – A Ticking Time Bomb for the Industry', was moderated by Dr. Deepak Kumar Sahu and featured esteemed experts, including Sameer Mathur, Founder & CEO of S M Consulting; Sushant Mohapatra, Senior Lawyer at the Supreme Court of India; Shantanu Sahay, Partner at Anand and Anand; Major Subhendu Mahunta, Director of Financial Crime Prevention at FPL Technologies; Anil Kaushik, Founder & Vice Chairman of Cybercorp Ltd; and Mahi Gupta, Director of Privacy Strategy at Data Safeguard. The panel delved into pressing data privacy concerns, evolving legal frameworks, and effective strategies to mitigate associated risks.

The second panel discussion, on 'Mitigating Security Risks in Emerging Technologies', was moderated by Deepak Maheshwari, Senior Consultant at the Centre of Social & Economic Progress. It featured prominent industry leaders, including Pawan Chawla, CISO & DPPO of TATA AIA Life Insurance; Mayank Mehta, CISO of Bajaj Allianz Life Insurance; Kapil Madan, CISO & DPO of Max Healthcare; Amit Dhawan, CEO of Network Intelligence; Sujoy Brahmachari, CIO & CISO of Rosmerta Technologies Ltd.; and Manoj Srivastava, CIO of EaseMyTrip. The session explored the rising threats of cyber intrusions, emphasizing the critical need for advanced security frameworks to protect sensitive and business-critical information.

The third panel discussion, From Risk to Resilience, was moderated by Gyana Swain, Consulting Editor at VARINDIA, and brought together distinguished experts to discuss strategies for safeguarding critical assets while enabling innovation in an increasingly interconnected world. The panel featured Vijay Sethi, Chief Mentor & Digital Transformation Evangelist; Bharat B Anand, Group CIO & CTO of Connect Global; Bhaskar Rao, CISO of The Bharat Cooperative Bank Mumbai Ltd.; Khushbu Jain, Advocate at the Supreme Court of India & Founder of Ark Legal; Ritesh Kumar, Assistant Vice President at EXL; and Dr. Yusuf Hashmi, Group CISO at Jubilant Bhartia Group.

The event also had interesting Corporate Presentations from industry experts who provided valuable insights into various facets of cybersecurity and data protection initiatives.

Akshay Garg, Senior Presales & Business Manager at Varonis Systems, shared his expertise on data security and risk management, emphasizing the need for proactive threat mitigation strategies. Ram Vaidyanathan, Cybersecurity Evangelist at ManageEngine, explored the expanding role of artificial intelligence in cybersecurity beyond 2025, highlighting AI's potential in threat detection and response.

Nakul Khandelwal, Director of Product Management at Qualys, presented Risk Harmonics, offering a comprehensive analysis of enterprise cyber risk data and how organizations can leverage it for better risk management.

Rajaram Venkatesan, Geo Lead – India-South & Sri Lanka at SOTI, discussed next-generation mobile workforce management, focusing on security challenges and solutions for enterprises. Tarun Pratap Singh, Associate Vice President – Cyber Security Practice at Hitachi Systems India, outlined best practices in cybersecurity, stressing the importance of a multi-layered security approach.

Aman Thareja, Managing Director of Forcepoint India & South Asia, examined the latest security trends shaping the industry, providing a forward-looking perspective on emerging threats and defenses.

Lee Nocon, Co-Founder & CTO of Data Safeguard India, shared his expertise on data privacy, emphasizing the role of trusted partnerships in navigating the complexities of DPDPA compliance. He highlighted how businesses can effectively align with regulatory frameworks while ensuring robust data protection.

In the Tech Talk session, Prof. Amlan Chakrabarti, Professor and Director, A.K. Choudhury School of IT, University of Calcutta spoke on how to decode malicious cyrillic URLs, the threats that are powered by Deep Neural Networks. He went on to enlighten the audience on how cybercriminals use cyrillic-based URLs for phishing attacks.

The summit also featured the launch of the Technology Trends Handbook, an e-magazine compiling expert insights on top technology trends and forecasts. Next the event also witnessed the much-anticipated awards ceremony which recognized top security OEMs and vendors based on user feedback collected via the VARINDIA platform. Additionally, CDS 2025 celebrated the outstanding contributions of India's Top 10 Partners & VARs across various categories.

The Cyber & Data Security Summit 2025 successfully provided a vital platform for industry leaders, government officials, and cybersecurity experts to share insights and collaborate on strengthening digital resilience. The discussions underscored the importance of proactive security strategies, compliance, and innovation in navigating the complexities of today's digital landscape.

E-magazine : Technology Trends 2025 Handbook Unveiled

The Make in India initiative is accelerating India's ascent as a global manufacturing hub, strengthening IT hardware, semiconductors, and Fab industries. With the IT sector projected to reach US$ 350 billion by 2026, contributing 10% to GDP, India is solidifying its position as a global technology leader.

In line with this vision, VARINDIA has launched India's first Technology Trends Handbook e-Magazine, curated by Dr. Deepak Kumar Sahu, and his team to showcase emerging innovations and strategic insights. This compendium fosters industry collaboration and provides valuable intelligence to drive Make in India and Made for India enterprises. By bridging technological foresight with industrial growth, this initiative reinforces India's trajectory as a global powerhouse in technology and digital innovation.

The Role of Technology in Judiciary: Enhancing Efficiency and Trust

HON'BLE JUSTICE GIRISH KATHPALIA

DELHI HIGH COURT

"As a consumer of judicial technology, I want to share insights on what citizens expect from a modern justice system. One of the biggest challenges is the lack of continuity in leadership within IT departments of government institutions. Without dedicated experts who possess a missionary zeal for technological progress, innovation stagnates.

6 USE CASES OF INDIAN JUDICIARY SYSTEM

- A critical issue is the lack of synchronization between different departments. Many operate on incompatible systems, limiting the efficiency of technological solutions. The Interoperable Criminal Justice System (ICJS) is an attempt to bridge this gap, ensuring seamless communication between courts, police, and correctional facilities. Delays, such as bail orders taking a month to reach prisoners, create discontent. ICJS aims to prevent such issues, but its success hinges on system compatibility across institutions.
- Data protection is another pressing concern. Judicial records are stored on servers, yet we lack a legal framework to govern a secure, centralized repository. Delhi's initiative to maintain a duplicate server in Madurai is a step forward, but a more comprehensive strategy is needed.
- Cybersecurity threats are also growing. A recent court hacking incident underscored the urgent need for stronger firewalls and AI-driven security protocols. The rise of deepfake technology poses additional risks, as manipulated evidence could threaten judicial integrity.
- AI-powered tools can streamline court proceedings. Automated transcription can save time, and AI-driven document summarization could help judges handling hundreds of cases daily. However, concerns about accuracy, ethical implications, and the irreplaceable role of human judgment must be considered.
- I believe that the market should start working on real-time vernacular-to-English text conversion for judges. However, local expressions pose challenges. Demeanor analysis is subjective, as judges are human. Still, Facial recognition could help assess truthfulness, though not with absolute certainty.
- Tech improves land records, voter verification, and docket management by ensuring transparency, reducing fraud, and improving efficiency.

Technology can also transform land record management, voter verification, and docket management by ensuring transparency, reducing fraud, and improving efficiency. While technology is a powerful enabler, it must be strategically implemented with strong safeguards. By addressing these challenges collaboratively, we can ensure that technological advancements strengthen the judiciary and uphold the cause of justice."

Harnessing AI: Balancing Innovation with Security

DR. PANKAJ DIXIT

CTO – GEM, GOVERNMENT OF INDIA

"The last two years have been transformative for AI, reshaping industries at an unprecedented pace. ChatGPT revolutionized the IT world, and now, with DeepSeek AI making waves, the evolution continues. AI agents are now streamlining business functions, from HR and document processing to financial analysis and security. Companies are actively seeking ways to maximize efficiency and ROI while navigating the inherent risks of AI adoption.

However, with great power comes great responsibility. AI's potential for efficiency is matched by its potential for misuse. The rise of generative AI means threat actors can now automate cyberattacks at an alarming scale. What once took weeks to develop can now be executed in seconds. Malicious actors are leveraging AI to create advanced attack vectors, injecting scripts, breaching security systems, and exploiting vulnerabilities faster than ever. This necessitates a proactive defense strategy, ensuring enterprise security systems are equipped to counter AI-powered threats.

At GeM, we are integrating AI cautiously, ensuring that our data exposure remains minimal and secure. We have implemented stringent safeguards—ring-fencing queries, curating knowledge bases, and restricting AI interactions to public datasets. By scanning inputs and outputs for potential threats, we prevent AI-driven exploits from infiltrating our systems. Our security measures extend to increasing SOC capabilities, enhancing EPS thresholds, and reinforcing our defenses in collaboration with cloud partners.

Looking ahead, we plan to integrate AI into post-login functionalities, allowing users to query deeper databases while ensuring strict access controls. This will require careful structuring of data lakes and warehouses to maintain security. Additionally, we are enhancing our customer service through AI-driven multilingual chatbots, ticket automation, and IVR-based interactions, with seamless human-agent handovers.

AI is revolutionizing how we work, but it also demands heightened vigilance. By adopting a structured, security-first approach, we can harness its immense potential while safeguarding against emerging threats. The journey continues—one step at a time, with caution and innovation in balance."

GULF (Greed, Urgency, Love/Lust, Fear) leads to Digital Arrest

B. SHANKER JAISWAL
JT. CP (OPERATIONS & LICENSING) – DELHI POLICE

"Digital Arrest has gained significant traction recently, particularly in India, where cybercriminals have become more sophisticated in exploiting technology for fraud. While the term might sound futuristic, it refers to a very real and alarming phenomenon that has been increasingly affecting people. As technology advances, so do the tactics used by criminals.

I come from a law enforcement background with extensive experience in cybercrime research. Over the years, I've observed how criminals are exploiting technology faster than we can keep up. The concept of a "digital arrest" isn't just a sci-fi idea—it's part of a real-world scam. In these scams, criminals impersonate law enforcement officials, telling victims they're under investigation for illegal activities. They then demand large sums of money, often in cryptocurrency, to avoid being arrested. These scams are getting more sophisticated, and their impact is growing.

EXPLOITING EMOTIONAL TRIGGERS

One case involved an IIT Delhi graduate who was tricked into paying four lakh rupees after being told he was involved in illegal activity. The scammer, posing as a police officer, used a fake arrest warrant and manipulated the victim into transferring money. This money was then converted to cryptocurrency and sent overseas. Another case involved a doctor who was convinced to pay 5.6 crore rupees after a fake customs officer fabricated a story about fake drugs and passports.

So, why are people falling for these scams? After years of research in the Cyber Crime Division, I've identified key emotional triggers criminals exploit: Greed, Urgency, Love/Lust, and Fear (GULF). These emotions push victims to act quickly, often without thinking, which is exactly what the scammers want. The best way to protect ourselves is by being aware and cautious. We need to practice S.E.A.C.—Slow down, Evaluate, Act with Caution, and be sceptical. If something feels off, it probably is.

STAY INFORMED, STAY SAFE

Furthermore, with the rise of generative AI, criminals can create highly convincing fake identities, making these scams harder to spot. We must also push for stronger data protection laws, like the Digital Personal Data Protection (DPDP) Act, to safeguard our personal information. Finally, as technology evolves, so do the tactics of cybercriminals. By staying informed, cautious, and spreading awareness, we can collectively reduce the impact of these digital threats."

Strategic leadership and investment are crucial for AI's future in India

PROF. KAMALJEET SANDHU
UNIVERSITY OF NEW ENGLAND, ARMIDALE, NSW, AUSTRALIA

"As Director of the Australian government's AI Hub, I'm passionate about fostering global collaborations, particularly between Australia and India, as we navigate the complex and exciting landscape of artificial intelligence and cybersecurity. We stand at a critical juncture. AI is rapidly transforming our world, presenting both incredible opportunities and significant challenges. How we respond will define the coming decades. And that response hinges on two crucial elements: strong leadership and strategic investment.

LEADERSHIP DRIVES INNOVATION

Leadership is paramount. Without visionaries at the helm, we risk drifting aimlessly in this sea of technological change. Cybersecurity, fundamentally, is a human problem. Technology is just a tool; it's leadership that guides its ethical and effective use. And investment? That's the fuel that powers innovation. History is clear: from the rise of the internet to the dominance of today's tech giants, strategic investment has been the catalyst for groundbreaking advancements.

AI holds immense promise. Imagine cures for Alzheimer's, Parkinson's, cancer. This is the transformative potential we must unlock. But we can't let fear paralyze us. We need open minds, encouraging exploration and responsible development. We must learn from the past. Microsoft's mobile market misstep teaches us about the critical importance of timing. AI is at a similar crossroads. India, with its vast talent pool, can be an AI leader, but we need decisive action.

SEIZE THE AI MOMENT RESPONSIBLY

Cyber warfare is a real and growing threat. It's a multi-billion dollar industry with the power to cripple nations. We need robust cybersecurity strategies, advanced technology, and the best minds working on solutions. Cyberattacks are often unseen, undetected for years. We must be proactive. Cybercrime is another major concern, impacting everyone. While we can't ignore it, we can't let it stifle progress. We need safeguards, smart regulations, and widespread cybersecurity awareness.

The internet's evolution offers a valuable lesson. It started without a clear plan, growing organically. We should let the AI world develop similarly, while always prioritizing security. Security and leadership are two sides of the same coin. This is a massive opportunity for India. I see the passion here. We are the leaders of this technological revolution. Let's seize this moment and shape AI's future responsibly."

AI security risks exposing vulnerabilities in system integrity

BRIJESH SINGH, IPS
ADGP POLICE & PRINCIPAL SECRETARY TO CHIEF MINISTER, GOVT. OF MAHARASHTRA

"AI is undeniably powerful. It can create music, generate images, write text, solve complex problems, and even perform tasks traditionally done by humans. But as we embrace AI's capabilities, one question looms large: Is AI secure enough to handle such responsibility?

AI already plays a significant role in our lives. Facial recognition systems, for example, are used in law enforcement to determine who goes to jail or not. Autonomous vehicles make life-and-death decisions about the safety of passengers and pedestrians. With such influence over our daily lives, can we trust AI to be secure?

VULNERABILITIES IN AI SYSTEMS

Unfortunately, AI security is a serious concern. AI systems are vulnerable to various attacks that can compromise their integrity. For instance, early versions of GPT models had vulnerabilities, such as the "DAN (Do Anything Now)" prompt attack, which allowed users to bypass safety measures and prompt the AI to give harmful responses. Despite efforts to patch these weaknesses, AI models are still susceptible to similar attacks.

Moreover, AI systems can be manipulated to make poor or harmful decisions. Efforts to align AI models with human values sometimes result in overly cautious or flawed responses, which opens the door to uncensored models capable of answering anything. These models, though powerful, pose significant security risks. For example, autonomous driving systems like Tesla's can be misled by simple changes to road signs, like placing stickers on a stop sign. Similarly, facial recognition systems can be tricked by altering a person's appearance.

PROTECTING AI FROM EXPLOITS

AI models are also at risk of being stolen or poisoned. A "model inversion attack" could expose sensitive information, such as health data. Additionally, malicious actors could compromise the infrastructure supporting AI systems, injecting vulnerabilities or backdoors.

As AI replaces human workers in various fields, such as coding, the need to protect these systems becomes more urgent. Cybersecurity must evolve to address AI-specific risks, such as backdoors or hidden vulnerabilities that could be exploited in critical applications like banking or law enforcement.

To conclude, securing AI is essential. It's not just about protecting technology—it's about ensuring privacy, fairness, and security for everyone. We must continue innovating while safeguarding the future."

AI and cybersecurity must work in harmony for a secure future

DR. PAVAN DUGGAL
ADVOCATE - SUPREME COURT OF INDIA

"Let me take you back to ancient India, during King Ashoka's reign. Like Alexander, Ashoka expanded his empire with immense power. Two crucial figures led his kingdom: the King and the Senapati, or Commander-in-Chief. When they worked together, the empire thrived; if not, it faced downfall. In today's world, our empire is artificial intelligence. Here, AI is the King, while cybersecurity is the Commander-in-Chief. For our future to be secure, AI and cybersecurity must function in harmony. However, if cybersecurity fails, AI's growth and stability will be at risk, leading to challenges and threats in our increasingly digital world.

AI ADVANCEMENTS AND RISKS

The world has already seen the impact of AI in recent advancements. Tools like DeepFake and Qwen2.5 have reshaped productivity, but with them come significant risks. In the US, legislation is already being discussed to curb AI misuse, such as the "No DeepSeek on Government Devices Act." But we also face the challenge of AI-driven cybercrime, where fraud GPT is enabling cybercriminals to breach security systems undetected.

As we continue to develop AI, we must recognize the growing risks it brings, especially regarding privacy. For example, AI platforms often collect data from users without clear disclosure, creating vulnerabilities. Despite the promise of AI, we must remain cautious. The Indian ecosystem, often trusting by nature, must recognize that AI technologies aren't guaranteed to protect their data.

PREPARE, REGULATE, AND SAFEGUARD

AI is also complicating traditional cybercrime, where cybercriminals are empowered by AI algorithms to execute crimes on a global scale. The criminal element is no longer bound by geographical or legal boundaries. The task of tracing and prosecuting such crimes has become increasingly difficult.

Governments, including China and the EU, have already established frameworks to address AI's risks. In India, however, we are still lagging behind. We lack an AI-specific cybersecurity law and are yet to take meaningful steps toward creating a robust legal framework. As AI continues to evolve, we must urgently develop policies to ensure privacy, security, and accountability.

This is the age of AI, and the challenges it presents will only grow. It's time to prepare, to regulate, and to safeguard this new digital era with proactive, well-designed legal and cybersecurity frameworks."

Advancing AI and Cybersecurity through Research: A Focus on URL Classification

PROF. AMLAN CHAKRABARTI

PROFESSOR & DIRECTOR, UNIVERSITY OF CALCUTTA

"Today I will highlight the importance of research within our AI Hub, a strategic India-Australia partnership led by Professor Kamaljit and myself, dedicated to AI and cybersecurity. Also, I will discuss key research areas that are shaping the future of AI applications.

AI-driven applications are transforming both hardware and software by how data is used and processed, and much of this progress relies on foundational research. A significant area we are investigating is edge computing, which reduces latency by processing data closer to its source. However, edge computing introduces new security challenges, particularly in securing AI inference models and the data they process.

Another critical area is neuromorphic and in-memory computing, which offer promising advancements beyond traditional computing. Our ongoing research in these areas is making important strides.

I would like to share one of the exciting projects my Ph.D. student is working on, in collaboration with Professor Kamaljit, that involves identifying vulnerabilities in URL masking using different encoding techniques. This research aims to address security risks like phishing attacks that occur when URLs appear safe but are malicious.

A crucial aspect of this work involves the manipulation of URLs through UTF encoding. By using non-Latin characters that resemble Latin characters, attackers can deceive users into visiting fraudulent websites. Phishing attacks exploiting these vulnerabilities are on the rise and are expected to reach nearly 340,000 incidents by the end of 2024.

The advent of internationalized domain names (IDNs), which allow non-English characters in URLs, has compounded this issue. While this innovation benefits non-English speakers, it also opens new security risks.

Our research on URL classification, using models like Bi-directional LSTM, is one way we are tackling these challenges. The model has shown promising results and will soon be published for broader use. I encourage more to connect with the AI Hub to help build a robust ecosystem that addresses the security challenges emerging in AI and cybersecurity."

Navigating the Digital Personal Data Protection Act (DPDPA)

ANUJ AGGARWAL

CHAIRMAN, CENTRE FOR RESEARCH ON CYBER CRIME & CYBER LAW

"Today, instead of a formal presentation, I want to engage in an interactive discussion about the Digital Personal Data Protection Act (DPDPA). The law is now in place, with the draft rules already approved by the Home Ministry.

Let’s start with a question: What does the DPDPA mean for Indian citizens? Many may think it applies only to Indian nationals, but that’s a misconception. Unlike the GDPR, which is residency-based, the DPDPA applies to any transaction involving personal data within India, regardless of citizenship. This includes transactions by foreign nationals or even those that are free of charge.

A key feature of the DPDPA is its provisions on data transfer. While businesses may store data anywhere, the law remains applicable if the transaction involves India. The primary method of data collection under the DPDPA is consent, and this consent must be clear and easy to understand—no more lengthy agreements that are impossible to decipher.

Consent forms must be provided in at least 22 languages, but businesses should accommodate additional languages if needed. For instance, if you're operating in a diverse area, you might need to offer consent forms in Japanese, German, or other languages.

While consent is the primary method, data can also be collected for legitimate purposes, such as employment. However, this must be done with the principle of minimal data collection. For example, businesses cannot demand Aadhaar numbers unless specifically authorized by law, and Aadhaar cannot be used as proof of address or age.

The DPDPA also has provisions for minors. Any business wanting to process a child's data must obtain consent from the guardian, not the child, and verify the guardian's identity. The law is designed to be simple and effective, but businesses must understand their responsibilities and ensure their practices align with it. The DPDPA is here to stay, and compliance is key."

Cybersecurity & Digital Forensics: Mitigating Cyber Threats Before They Strike

DR. HAROLD D'COSTA

PRESIDENT CYBER SECURITY CORPORATION

"As someone with a forensic background, I can tell you that many of us trust platforms like WhatsApp for personal, professional, and confidential communication. Today, I've been hearing discussions around data privacy, the DPDP Act, and related concerns. To illustrate the point, let me share an example: my friend Rohit sent me an image on WhatsApp, but I received something entirely different. Now, people hesitate to share their numbers with me, as what you see isn't always what you get. This raises an important question: can we truly trust digital evidence?

This brings us to the need for effective cyber attack mitigation, which consists of three critical approaches:

Proactive Measures: Implementing firewalls, endpoint security, and threat intelligence to prevent attacks before they happen.

Reactive Measures: Establishing incident response plans, conducting forensic investigations, and taking legal action after an attack occurs.

Regulatory Compliance: Ensuring legal compliance, as many organizations fail to meet full compliance despite technical safeguards, leaving security gaps.

Many organizations focus on reactive measures rather than proactive ones. Let's take a look at some real-world breaches:

Cosmos Bank (2018): Rs. 94 crore lost due to weak cybersecurity measures.

IRCTC Data Leak: Personal data of 2 crore users exposed.

SpiceJet Ransomware Attack: Caused severe flight delays.

To mitigate cyber threats, organizations should use AI tools for phishing detection, implement immutable backups, adopt zero-trust access, and ensure continuous security posture management. With average breach losses of Rs. 12.8 crore and DPDP Act penalties up to Rs. 250 crore, proactive cybersecurity is essential, especially for critical infrastructure sectors.

Lastly, the example I showed earlier highlights a key issue with forensic admissibility under the Bharatiya Sakshya Adhiniyam 2023. If manipulated digital evidence is submitted in court, it could be mistaken for genuine evidence. This reinforces why forensic validation is critical before accepting digital content as truth."

Empowering Digital India: The Need for Strong Data Protection Frameworks

MS. DEEPA OJHA

MANAGER - PRIVACY & POLICY - DSCI

"As a policy expert in cybersecurity and data protection, I emphasize the critical role of data security in empowering individuals, businesses, and national security. India's regulatory framework is key to ensuring a secure digital ecosystem while promoting trust, compliance, and innovation.

WHY DATA PROTECTION MATTERS

With the rapid adoption of AI, IoT, and smart technologies, digitization has transformed industries but also increased cyber threats, data breaches, and privacy risks. A robust data protection framework is essential to balance business needs and individual rights.

KEY REASONS FOR DATA PROTECTION:

- Safeguarding Individual Privacy – Giving users control over their personal data.
- Building Business Trust – Compliance enhances consumer confidence.
- Enhancing National Security – Strengthening cybersecurity for critical infrastructure.

INDIA'S DATA PROTECTION LAWS

India's data protection journey evolved from the 2017 Puttaswamy judgment, which recognized privacy as a fundamental right, leading to the Digital Personal Data Protection Act (DPDPA) 2023. This law enforces purpose limitation, data minimization, and consent-driven processing. The Digital Personal Data Protection Act (DPDPA) 2023 aims to safeguard digital personal data while allowing lawful business operations. It ensures regulatory compliance by providing flexibility for data transfers and privacy innovations, enabling businesses to adapt to evolving data protection needs. Additionally, the law promotes industry-led cybersecurity practices, strengthening data security safeguards to mitigate risks. By balancing privacy protection and business interests, DPDPA 2023 fosters a secure, transparent, and trustworthy digital environment for individuals and enterprises alike.

By balancing privacy and business needs, the law fosters trust, transparency, and compliance in India's data-driven economy.

While DPDPA 2023 presents challenges—such as consent mechanisms, security obligations, and cross-border data flows—it also drives privacy innovation and cybersecurity advancements. At DSCI, we actively collaborate with government and industry stakeholders to create policy frameworks, cybersecurity guidelines, and training programs. Ensuring a secure digital ecosystem requires ongoing collaboration, innovation, and compliance."

Top prominent scams in 2024: fake stock trading, crypto investment scams and digital arrest

DR. RAKSHIT TANDON
CYBER SECURITY EVANGELIST AND RISK ADVISORY EXPERT

"According to recent data from the Indian Cybercrime Coordination Center (I4C), India reported 12 lakh (1.2 million) cybercrime complaints in the first nine months of 2024—equating to one cybercrime every minute. Financial losses from these scams amounted to a staggering ▯11,333 crores. Among the most significant cyber scams were fake stock trading, crypto investment frauds, and digital arrest scams, all contributing to massive financial damage. These scams exploited victims by manipulating trust and leveraging advanced cyber tactics.

Reflecting on the past, early cybercrimes primarily relied on social engineering. Scammers would call unsuspecting victims, posing as bank officials and tricking them into sharing OTPs—an infamous tactic originating from fraud hotspots like Jamtara. However, cybercriminals have since evolved significantly, adopting cutting-edge technology to enhance their deception. Even before companies could harness AI-driven cybersecurity, hackers had already begun using voice cloning, deepfakes, and AI-powered malware to exploit individuals. One of the most alarming threats today is the distribution of malicious APKs (Android Package Kits) through trusted contact attacks.

APKs function as advanced Trojans capable of stealing SMS data and banking credentials from infected devices. Hackers typically disguise these files as legitimate KYC verification updates from banks, convincing users to download and install them. Once installed, the malware grants hackers unauthorized access to sensitive information, leading to major financial losses. These APK-based cyberattacks remain a persistent challenge, as users often fail to recognize the deceptive nature of these files. Despite advancements in cybersecurity, India continues to struggle with preventing unauthorized APK installations, making it a pressing issue for law enforcement and tech security firms. Cybercrime has evolved from basic social engineering to AI-driven fraud, making awareness and proactive cybersecurity measures more critical than ever. As hackers grow more sophisticated, stronger security protocols, AI-enhanced fraud detection, and public awareness campaigns are essential to combat this escalating menace."

Navigating AI and Data Security: A Proactive Approach to Protecting Our Future

AMAN THAREJA
MD, FORCEPOINT INDIA & SA

"In today's rapidly evolving tech landscape, Artificial Intelligence (AI) is undoubtedly the fastest-growing technology, with a billion people expected to use it in just seven years. The impact on our lives will be profound, and it's crucial to integrate AI into every aspect of society, especially cybersecurity.

Cybercriminals are primarily after one thing: your data. With the global cost of a data breach averaging $4.5 million, organizations must prioritize data protection. In fact, cybercriminals are operating in a multi-trillion-dollar economy, underscoring the need for robust security measures.

Data protection regulations, such as DPDP, are evolving to ensure accountability throughout the data lifecycle—from collection to storage. Organizations must handle data responsibly, ensuring privacy and security, with strong systems in place to meet global standards.

At Forcepoint, we've developed an AI-powered Data Security Posture Management (DSPM) solution that autonomously identifies, classifies, and profiles data, helping organizations mitigate risks like access and retention vulnerabilities. Our AI leverages scalable, contextual decisions to improve efficiency and compliance, offering a dashboard that provides visibility and helps pinpoint high-risk areas.

In summary, a proactive, data-first approach is crucial for protecting sensitive information. Forcepoint is committed to delivering comprehensive data security, helping organizations adapt to new challenges and safeguard their most valuable assets."

Ensuring DPDP Compliance with Data Safeguard's ID Redact

LEE NOCON
CO-FOUNDER AND CTO, DATA SAFEGUARD

"Today, I'll focus on how Data Safeguard, dedicated to data privacy and synthetic fraud prevention since 2010 with strong presence in both the U.S. and India, helps businesses achieve DPDP compliance. While previous speakers have covered its key aspects, my focus is on practical solutions.

THE SHIFT FROM CYBERSECURITY TO DATA PRIVACY

For decades, investments have poured into cybersecurity, yet data privacy has been overlooked. With rising data breaches, the priority is no longer just preventing access but ensuring stolen data remains unusable. This shift is driving major investments in privacy and synthetic fraud prevention.

Smart devices collect vast amounts of personal data—over 500,000 PII elements per device. DPDP enforces strict privacy laws, mirroring global trends where fines surged from $8B to $16B in 2022. With enforcement expected in 12–18 months, businesses must act now.

ID REDACT: A COMPREHENSIVE DPDP SOLUTION

ID Redact is a comprehensive data privacy solution designed for global and Indian markets, integrating consent management, data discovery, access requests, redaction, privacy impact assessments, compliance audits, and real-time privacy monitoring. It enables businesses to manage cookie preferences, parental consent, and data processing while ensuring compliance with evolving regulations. With deployment in just two weeks and ROI in four, ID Redact prioritizes Privacy by Design, embedding robust security and compliance into every business process."

Beyond Passwords: The Future of Seamless Security

TARUN PRATAP SINGH

ASSOCIATE VP - CYBER SECURITY PRACTICE, HITACHI SYSTEMS INDIA

"In today's digital landscape, authentication is the foundation of security. Whether accessing a system, entering an office, or retrieving data, authentication plays a crucial role. However, traditional authentication methods, including passwords and two-factor authentication (2FA), are vulnerable. At Hitachi Systems India, we are pioneering a next-gen authentication platform that moves beyond passwords, ensuring seamless and secure access.

Today I will explore how advanced authentication methods—such as biometrics, behavioral analytics, and passwordless authentication—are transforming security frameworks. By integrating AI-driven adaptive authentication, organizations can detect anomalies in real-time and prevent fraudulent access. The rise of decentralized identity management and zero-trust architecture is further reshaping authentication, ensuring that security is continuous and context-aware rather than a one-time checkpoint.

However, as security tightens, user experience must not suffer. Striking the right balance is key to driving adoption and operational efficiency. We will discuss real-world case studies of organizations successfully implementing frictionless authentication while reducing risks and enhancing compliance with evolving regulations.

Looking ahead, innovations such as passkeys, blockchain-based identity verification, and continuous authentication will redefine digital trust. As cyber threats evolve, authentication must be dynamic, seamless, and intelligent.

Join us as we dive into the future of authentication, uncovering strategies to enhance security without compromising user convenience. The next era of authentication is here—are you ready to embrace it?"

Navigating AI and cybersecurity smartly in 2025 is critical

RAM VAIDYANATHAN

CYBERSECURITY EVANGELIST - MANAGEENGINE

"Today, we are at an interesting crossroads where artificial intelligence (AI) and cybersecurity intersect. On one hand, cybercriminals are leveraging AI to enhance their attacks, becoming more sophisticated and effective. On the other hand, as cybersecurity professionals, we need to use AI for all the good reasons to defend against these growing threats. The question we face is how we can harness its potential to strengthen defenses while managing the risks it brings. At Manage Engine, we develop a unified SIEM solution called Log360, designed to monitor and alert users when something goes wrong in their network.

A DOUBLE-EDGED SWORD

Cybercriminals are increasingly using AI to improve attacks. For example, AI-driven ransomware can target specific individuals or organizations, making the attack more personalized and harder to detect. It also powers malware that can adapt in real time to evade traditional defenses. Techniques like data poisoning or input manipulation allow attackers to bypass security systems. On the flip side, AI plays a vital role in defending against cyber threats. AI enables real-time threat detection, anomaly analysis, and faster forensic investigations. Integrating AI into identity security and access management reduces risk.

PREDICTIVE, PRESCRIPTIVE, AND REACTIVE

The three primary use cases for AI in cybersecurity are predictive, prescriptive, and reactive. Predictive AI helps with dynamic access control and proactive threat hunting. Prescriptive AI aids in anomaly detection, identifying unusual behaviour or phishing attacks. Reactive AI helps with post-breach analysis, learning from past incidents to prevent future attacks. In short, while AI introduces new challenges, it offers immense potential to enhance cybersecurity. We must leverage it to stay ahead of cybercriminals."

Qualys enables proactive risk management in cybersecurity

NAKUL KHANDELWAL

DIRECTOR, PRODUCT MANAGEMENT – QUALYS

"Digital transformation is expanding attack surfaces across hardware, software, IoT, and AI workloads, making the cybersecurity landscape more complex. Many organizations now use up to 70 cybersecurity products to address specific risks, but these tools often create security silos, making it harder to manage risks holistically. This is where a Risk Operation Center (ROC) becomes essential. Unlike traditional Security Operation Centers (SOC), which are reactive, a ROC focuses on proactive risk management. By aggregating indicators of exposure like vulnerabilities, misconfigurations, and identity risks across all assets, a ROC helps mitigate risks before they cause major security incidents.

SHAPING THE FUTURE OF RISK MANAGEMENT

The key to building an effective ROC is the right tools. Qualys' Enterprise True Risk Management platform is pivotal, unifying asset inventories, aggregating security findings, and offering a single view of risk posture. This enables organizations to measure, communicate, and act on risks in a timely manner, reducing silos and strengthening security. Additionally, the rise of AI and large language models (LLMs) introduces new risks. As LLMs become more widespread, many organizations lack visibility into the risks they pose, such as data leakage via prompt injection. Securing AI workloads is now a must.

STAY AHEAD OF FUTURE THREATS

Qualys offers solutions to detect vulnerabilities, prevent data theft, and protect AI systems. With increasing AI use, securing LLM workloads is critical. In conclusion, building a ROC and adopting a proactive risk management approach is more important than ever. With the right tools, like Qualys, organizations can manage the growing complexities of cybersecurity and stay ahead of emerging risks."

SOTI's secure, scalable solutions help businesses optimize their mobile operations

RAJARAM VENKATESAN

GEO LEAD- INDIA-SOUTH AND SRI LANKA, SOTI

"SOTI is a 30 years old and is headquartered at Mississauga, Canada. When you consider air travel, the moment you walk into the airport, you are checked in by the CISF people who scan your bags on all kinds of rugged industrial devices; we manage those devices. Then when you walk into the aircraft, the person who checks your boarding pass, then lets you in and again when you exit, there are devices which the service engineers use to do the inspections. These devices are also managed by us. So that is the spread of devices that we manage. In terms of growing our business, we always believe in investing back into the business. In India, we are headquartered in Gurgaon, and we also have a development center in Kochi. So half the strength of our global population will be out of India. We manage about 2.2 crore devices; some of our partners are the device partners as you need to have all the devices certified. We work very closely with them because it's not easy working with so many devices and to have SKUs of devices that could be made in the US or China. Unless you have those alliances ready, you cannot end up managing those devices single-handedly. Some of our customers could be anybody from the SMEs to the Fortune 100 companies. In India too, we have customers in BFSI, e-commerce, quick commerce, government, retail and so on. BFSI is a large vertical for us. In the drone industry, has a company called "SOTI Aerospace," which is a division of SOTI Inc. dedicated to advanced aerial drone and robotics research, essentially providing software solutions for managing and operating drones."

GenAI is a reality for enterprises today

AKSHAY GARG

SENIOR PRESALES & BUSINESS MANAGER – VARONIS SYSTEMS

"Generative AI is no longer a futuristic concept; it’s here, reshaping enterprise operations. Tools like Copilot and Gemini enhance productivity but also bring significant security risks, expanding the "blast radius" of accessible data and exacerbating vulnerabilities. Traditional, perimeter-based security strategies struggle to manage this evolving landscape. The core issue is a lack of focus on data itself. Many organizations don't know where sensitive data resides, who has access to it, or how it's being used. This knowledge gap, paired with GenAI's data-hungry nature, creates substantial risk.

PROACTIVE DSPM FOR GENAI SECURITY

A robust Data Security Posture Management (DSPM) strategy is essential. It should go beyond data discovery and classification, offering automated remediation for excessive permissions, identifying attack paths, and addressing identity misconfigurations. This proactive approach is key to securely adopting GenAI. Key DSPM capabilities include: comprehensive data discovery across all platforms, real-time risk assessment, automated remediation, and granular monitoring of data activity. GenAI governance is equally critical, ensuring visibility into tool usage, user prompts, file access, and conversations to prevent data exposure.

SECURING GENAI WITH VARONIS

Varonis Systems addresses these challenges with a platform that extends beyond basic DSPM, offering automated permission remediation, attack path analysis, and identity misconfiguration management. It provides the visibility and control organizations need to securely adopt GenAI. Varonis’ unified solution integrates DSPM and GenAI governance, empowering organizations to leverage AI’s benefits while minimizing risks. This shift from reactive breach response to proactive protection is the key to safely navigating GenAI's increasing presence."

CDS 2025: Calls for Action for a Secure, Resilient, and Digitally Empowered Future

DR. DEEPAK KUMAR SAHU

EDITOR-IN-CHIEF, VARINDIA

"The Cyber Data Security (CDS) Summit unites experts, thought leaders, and innovators from India and Singapore to shape the future of cybersecurity and digital transformation. Today, we honor the CIOs, CTOs, CISOs, and digital pioneers strengthening India’s cybersecurity landscape. Our Annual Cybersecurity and Rising Cybercrime Survey highlights India’s AI progress and growing cyber threats. The government’s push for an indigenous Large Language Model (LLM) within ten months marks a step toward AI independence. However, cyber risks are escalating rapidly.

India ranks second globally in cyberattacks, with 95% of organizations experiencing breaches in 2024. The financial, healthcare, government, and IT sectors remain prime targets. Cloud breaches are rising, affecting 67% of organizations due to misconfigurations and human errors. India accounts for 20% of global data breaches, often caused by unsecured APIs and weak encryption.

AI-driven cyber threats are a growing menace. 96% of deepfake content online is non-consensual, targeting women and public figures. India is among the top nations for AI-powered phishing and fraud attacks, with scammers using ChatGPT-like tools for sophisticated schemes. Generative AI is fueling phishing, voice cloning, and identity fraud, making detection harder.

To counter this, India has introduced the DPDP Act 2023 and CERT-In mandates for rapid cyber incident reporting. The National Cybersecurity Strategy 2024 emphasizes AI-driven security and cyber resilience. With 93% of IT leaders planning AI-driven security, the Indian cybersecurity market is set to reach $13.6 billion by 2027. The question remains—Is India prepared to combat these challenges? Now is the time to act. Let’s collaborate to build a secure, resilient, and AI-powered future."

TOP 10 OEMS IN THE CYBER SECURITY (PRODUCT & SOLUTIONS)

BEST COMPANY INTO CLOUD SECURITY SOLUTION -	QUALYS SECURITY TECHSERVICES PVT. LTD.
BEST DATA LOSS PREVENTION (DLP) PRODUCT -	FORCEPOINT SOFTWARE CONSULTING INDIA PRIVATE LIMITED
BEST UNIFIED ENDPOINT MANAGEMENT -	MANAGEENGINE, A DIVISION OF ZOHO CORPORATION
BEST THREAT INTELLIGENCE PLATFORM -	CYBLE SOLUTIONS PVT. LTD.
BEST SD-WAN SOLUTION PROVIDER -	FORTINET TECHNOLOGIES INDIA PVT. LTD.
BEST UNIFIED ENDPOINT MANAGEMENT -	SOTI INDIA PVT. LTD.
BEST COMPANY INTO NETWORK SECURITY -	CISCO SYSTEMS INDIA PVT. LTD.
BEST COMPANY INTO DATA SECURITY -	VARONIS SYSTEMS, INC
BEST COMPANY INTO DATA PRIVACY -	DATA SAFEGUARD INDIA PRIVATE LIMITED
BEST COMPANY INTO IT & OT SECURITY -	CHECKPOINT SOFTWARE TECHNOLOGIES INDIA PVT. LTD.

TOP 10 VARs IN THE CYBER SECURITY (PRODUCT & SOLUTIONS)

BEST VAR - CYBER SECURITY -	ADIT MICROSYS PVT. LTD.
BEST CLOUD SECURITY PARTNER -	INTENSITY GLOBAL TECHNOLOGIES PVT. LTD.
BEST MANAGED SECURITY SERVICE PROVIDER -	ALSTONIA CONSULTING LLP
BEST PARTNER INTO PROVIDING DATA PRIVACY SOLUTION-	HITACHI SYSTEMS INDIA PVT. LTD.
FASTEST GROWING CYBERSECURITY PARTNER -	ACPL SYSTEMS PVT. LTD.
BEST VALUE ADDED DISTRIBUTOR -	IVALUE INFOSOLUTIONS PVT. LTD.
BEST CRITICAL INFRASTRUCTURE SECURITY PARTNER -	VALUE POINT SYSTEMS PVT. LTD.
BEST NEXT GEN CYBER SECURITY -	BLACKBOX LTD.
EMERGING VAD IN INDIA -	FRUX TECHNOLOGIES PVT. LTD.
BEST DISTRIBUTOR INTO CYBER SECURITY -	RAH INFOTECH PVT. LTD.

CDS 2025 AUDIENCE

PANEL DISCUSSION I: DATA PRIVACY: A TICKING TIME BOMB FOR THE INDUSTRY

(FROM L TO R) MAHI GUPTA, DIRECTOR (PRIVACY STRATEGY) - DATA SAFEGUARD; SAMEER MATHUR, FOUNDER & CEO - S M CONSULTING; ANIL KAUSHIK, FOUNDER & VICE CHAIRMAN, CYBERCORP LTD; SHANTANU SAHAY, PARTNER- ANAND AND ANAND; MAJOR SUBHENDU MAHUNTA, DIRECTOR-FINANCIAL CRIME PREVENTION - FPL TECHNOLOGIES; SUSHANT MOHAPATRA, SR. LAWYER- SUPREME COURT OF INDIA AND DR. DEEPAK KUMAR SAHU, EDITOR-IN-CHIEF-VARINDIA

The first panel discussion for the day was on the topic - Data Privacy: A Ticking Time Bomb for the Industry and it was moderated by Dr. Deepak Kumar Sahu, Editor-in-chief-VARINDIA. The panelists who joined the session were Sameer Mathur, Founder & CEO - S M Consulting; Sushant Mohapatra, Sr. lawyer- Supreme Court of India; Shantanu Sahay, Partner- Anand and Anand; Major Subhendu Mahunta, Director-Financial Crime Prevention - FPL Technologies; Anil Kaushik, Founder & Vice Chairman, Cybercorp Ltd and Mahi Gupta, Director (Privacy Strategy) - Data Safeguard.

Talking about the critical challenges businesses face in handling personal data. Major Subhendu Mahunta mentioned the complexities of adapting to changing regulatory landscapes. “We are talking about the DPDP Act, the European Union’s GDPR laws and China again has its own regulations. So addressing all these challenges across different landscapes is a big constraint for every business. Many countries are adapting to these changing regulations, and how we address these challenges is a difficult task for the legal fraternity, because being non-compliant attracts regulatory penalties, including lawsuits. Secondly, any cross border transactions have its own ramifications. But in reality there is no standardization here. There are also complexities involved in taking the user consent, because not all the users are okay to share the data across the boundaries.”

Sameer Mathur explained, “Since I come from the Technology Advisory side and we conduct workshops on the DPDP Act compliance, there are 2-3 challenges that we see from the actual implementation side. One, the base of this law is the consent from the concerned data principal; taking and managing consent has become a very big challenge, especially for organizations where the number of data principals or number of PII holders is very, very large. So, whether it's a BFSI or ecommerce company or a logistic company or NBFC, managing consent is one of the biggest challenges. Another is about spreading awareness within the organization in terms of how do you convince people that this is not a cybersecurity issue, but a personal privacy issue. So we conduct an exercise called harm audit, where we try to convince the customer about the kind of harm that the loss or breach of personal data will incur.

Mahi Gupta further reiterated the point by adding that the biggest concern is to try understanding where does privacy end and what are the operational requirements for a business to conduct business. “I think the biggest challenge is that organizations think that with the advent of privacy laws, or cyber security regulation, doing business will be very tough. That's not what the intent of the regulation is. The regulation is saying that if you want to do certain things, just put certain guardrails around so that everybody's in a win-win situation. It's not like one side wins all and the other side loses everything. The balance that needs to be created is what the regulations demand.

On how he sees the current data privacy regulations evolving to emerging digital threats, Sushant Mohapatra said, “If we all remember, towards the end of 1999, there was this whole issue of Y2K that referred to the year 2000 and the potential computer issues that could have occurred when entering that year. It was also known as the millennium bug and it was said that everything will stop working, even banks for that matter. But slowly and efficiently we have migrated from that. So talking about this privacy law, these laws are already there in many areas, like CIBIL, the credit rating agency with which all our data is shared. But it is an integral part of the civil law itself of how the data should be protected. So instead of having fears about the implementation of this law, one should have an openness towards it because it is easy to comply with if you are aware of all the laws and rights.

Shantanu Sahay said, “One pertinent question as lawyers we always keep on asking ourselves is whether the law is caught up with the pace of technology. And the answer is no; there will always be some gaping lapses in terms of the way the technology has developed. Also, as a lawyer, and especially when I am focusing on issues of copyright violation and issues of other legal matters, I am confronted with the situation of whether the law in cases of a violation and also in a situation of Regulation, is in the position to deal with these issues with the right technology process. But I am 100% positive today, that so far as the substantive law is concerned in India, we are pretty much certain that we have the structure to deal with these lapses.”

On how organizations ensure ethical and secure data use, Anil Kaushik said, “The ownership of the data is with the creator of the data or the data principal, which is the bottom line. Secondly, no data privacy can go without the liabilities attached to that. So liabilities will be increased, they will be there and those could be even more stringent in the future. The lapses which I could see in the system is the absence of provision for keeping the data, of how to store the data and where to store the critical data.”

PANEL DISCUSSION II: MITIGATING SECURITY RISKS IN EMERGING TECHNOLOGIES

(FROM L TO R) PAWAN CHAWLA, CISO & DPPO- TATA AIA LIFE INSURANCE; MAYANK MEHTA, CISO- BAJAJ ALLIANZ LIFE INSURANCE; ROHIT RAMAN, MANAGING PARTNER & APAC HEAD – ETEK INTERNATIONAL; DEEPAK MAHESHWARI, SR. CONSULTANT- CENTRE OF SOCIAL & ECONOMIC PROGRESS; AMIT DHAWAN, CEO - NETWORK INTELLIGENCE; SUJOY BRAHMACHARI, CIO & CISO- ROSMERTA TECHNOLOGIES LTD. AND MANOJ SRIVASTAVA, CIO- EASEMYTRIP

The second panel discussion for the day was titled - Mitigating Security Risks in Emerging Technologies and it was moderated by Deepak Maheshwari, Sr. Consultant- Centre of Social & Economic Progress. The panelists for this session included Pawan Chawla, CISO & DPPO- TATA AIA Life Insurance; Mayank Mehta, CISO- Bajaj Allianz Life Insurance; Rohit Raman, Managing Partner & APAC Head – ETEK International; Amit Dhawan, CEO - Network Intelligence; Sujoy Brahmachari, CIO & CISO- Rosmerta Technologies Ltd. and Manoj Srivastava, CIO- EaseMyTrip. The session delved on how with the surge of cyber intrusions over the past decade that causes data breaches, disruptions, and financial losses, highlights the urgent need for strong cybersecurity to protect critical information and infrastructure.

Deepak Maheshwari opened the discussion by saying that while threat actors (Chor) and defenders (Police) all use the same technologies and tools, but it is just a matter of who is ahead in the game. “But when it comes to the use of Gen AI, or AI in general, the speed at which things are happening, the scale at which things are happening, that's something which becomes extremely important for us to look at.”

On how his organization ensures cybersecurity and data protection while deploying new technologies, Pawan Chawla said that both cyber security and data protection go hand in hand. “But as an organization, we can't play around with multiple tools. We have a limited set of tools with which we need to work upon. Hacking has become an organized crime and I would say the hacking industry is much more regulated than any other industry. Data is not only the fuel for the organization, but it is the real-time fuel. The market is changing so fast that you need to have real time data to change your dynamics as well. So when it comes to adopting a new technology, it is important to identify the vulnerabilities before adopting it. It should fit within your environment.”

Speaking about some of the ambiguities that still exist in the present system, Mayank Mehta stated that while in certain cases it required six hours to report an incident, the DPDP Act draft rules says that any breach that takes place needs to be reported within 72 hours. “Since in the insurance industry, we happen to report any such incidence to IRDA, will this framework fit into these newly set rules. All these things need to be unified so that organizations can take the critical approach. Most of the time, because of this ambiguous nature, organizations who are ethical will always try to go according to the rules while some will take their own call.”

While explaining how his organization ensures data protection, Sujoy Brahmachari said that there should be a right balance between an organizations’ application as well as UX, which is customer experience and the security of the application product. “So it's a combination of both. Cyber security and data security should not be an after-thought and it should be implemented from Day 1 after testing it properly. You need to have a good, robust mobility application which every user can use. The ease of use is very important. And apart from that, you need to have a good access control and authentication mechanism as well as a monitoring mechanism, so that both things go hand in hand.”

Manoj Srivastava said that his company has been into travel technology for the last 20 years. “Today, talking about data protection or cyber security, we have to go through a lot of due diligence since we deal with a lot of customer data. Firstly, we need to look into compliance by sharing all the necessary documents. Next is the technical part, when we have a lot of regression testing on our software before making it live. Before going live, we also take care of data protection so that it does not go into the wrong hands. Also, we are connected in real time and so there is no chance for error.”

Amit Dhawan said that on a lighter note, the threats will never be technical, but it comes out of the human firewall. “You can have a billion-dollar equipment, but then somebody will create a server or an MTP server and leak out data. So the human firewall element is one of the most important things. We can talk about users who are using it, but the security folks themselves are at fault most of the time. And I keep repeating very often that a fool behind a tool is always a fool. You can get any amount of infrastructure in place, but if you do not have the right capability to manage it, it is going to fail.”

Talking about the unique challenges and opportunities in the healthcare sector, Rohit Raman said, “Being a cybersecurity specialist, I understand that with the use of AI and digitalization in the health sector, there has been a lot of improvement. At the same time, we also see that it is bringing out a lot of good things in terms of informed decisions by the health practitioners, whereby ultimately, the benefit goes to the patient in terms of high rate of success in treatments. AI and database information will help you diagnose the problem in a much better manner. But the biggest challenge, however, is the integration. There is no formal standardization of data in the health sector, at least in India.”

PANEL DISCUSSION SESSION III : FROM RISK TO RESILIENCE

(FROM L TO R) GYANA SWAIN, CONSULTING EDITOR- VARINDIA; VIJAY SETHI, CHIEF MENTOR- DIGITAL TRANSFORMATION AND SUSTAINABILITY EVANGELIST; KHUSHBU JAIN, ADVOCATE- SUPREME COURT OF INDIA & FOUNDER - ARK LEGAL; BHAVESH KUMAR, CHIEF INFORMATION SECURITY OFFICER & DPO – SK FINANCE LIMITED; BHASKAR RAO, CISO - THE BHARAT COOPERATIVE BANK MUMBAI LTD. AND BHARAT B ANAND, GROUP CHIEF INFORMATION & TECHNOLOGY OFFICER- CONNECT GLOBAL

The third panel discussion session entitled - From Risk to Resilience was moderated by Gyana Swain, Consulting Editor- VARINDIA. The panelists joining this session were Vijay Sethi, Chief Mentor- Digital transformation and sustainability evangelist; Khushbu Jain, Advocate- Supreme Court of India & Founder - Ark Legal; Bhaskar Rao, CISO - The Bharat Cooperative Bank Mumbai Ltd.; Bhavesh Kumar, Chief Information Security Officer & DPO – SK Finance Limited and Bharat B Anand, Group Chief Information & Technology Officer- Connect Global.

Gyana Swain began the discussion by citing data from RBI (Reserve Bank of India) which says that in the last two decades, there have been a loss of more than $20 billion through cyber-attacks. “Another report says that more than 2500 cyber attacks happen in the BFSI sector every week, which is also hard to believe since daily transactions are close to Rs 18 crores in the country alone, against which this figure is quite minuscule.”

Speaking about the biggest security challenges in 2025, Vijay Sethi said that while AI is increasing a lot, the AI-based threats are also increasing at the same pace. “Rather than just the traditional threats that have been there, AI would be now used more to exploit the vulnerability. Also all the phishing attacks and the ransomware attacks, which have been there for quite some time now, would become much more sophisticated because of AI. I am convinced that the attackers know more about AI than the defenders or any organization. The second major risk that I see is the third party risk. The BFSI with its huge number of stakeholders become a huge entry point for threats. So while one can get into zero trust or any other security measures, the reality is most of the organizations are not working on that.”

Khushbu Jain said that while talking about the threat that comes with the use of AI, we also have to look into the aspect of what are the vulnerabilities when we are using AI. “It is good to inculcate AI in your organization when it comes to fighting cyber crimes or when it comes to creating the ecosystem for cybersecurity, but by utilizing that you have to have a lot of things in mind. Today you talk about privacy by design, but it's very difficult to implement privacy by design. And that's where you need to understand the biasness, or how vulnerable those AI things would be, or what all data sets are you utilizing for building different AI models. What are the laws prevalent now; the DPDP Act is there, but apart from this, GDPR and a lot of other privacy laws are existent worldwide. So you will have to be mindful of that. You will have to see that the company who is providing you with data, is there a proper consent for that mechanism? If you don't have that consent, tomorrow you will land up in litigation and this will create difficulties for you.”

Agreeing with both the panelists, Bhaskar Rao said, “We are a cooperative bank, and we are more dependent on the third party. The supply chain, I think, happens to be one of the most vulnerable spots as most of us are dependent on the services provided by the third party. If you recall an incident 4- 5 months back, there was an attack on one of the prominent banking technology providers and this led to 300 banks being cut off and experiencing a major outage. The hackers have come to realize the dependency of the banks on a central repository and they target that for stealing data, eventually disrupting the entire supply chain and the entire banking functionality in the process.”

Bhavesh Kumar said that while talking about cyber risk or compliance risk, the compliance or regulatory requirement is laid down by a different regulator to protect the stakeholders from cyber and fraud risk. “So if we are protecting or implementing effective controls, automatically we will comply with the compliance. In BFSI, since we are a fiduciary for our customer as we have in possession the confidential or personal information of our individual customers, and so to address the risk the first thing we should do is to fix our basics. So when we say basics, we must implement effective technology, processes and effective awareness mechanisms in our organization to disseminate each and every regulatory compliance related information and cyber related information.”

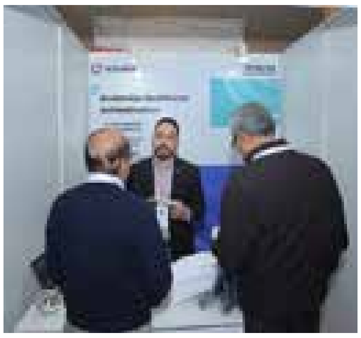
Bharat B Anand “So we are name-dropping AI these days. It's just like the Cloud in early 2000 and digital in 2010-12 onwards and now it's the AI. But AI is both an opportunity and a challenge, and we as a technologist, as well as the business owners or the vertical head, we need to take care of both the aspects. As much as you need to shore up your fences using whatever you can, it is just not about the devices you have put but it's more about what policies, what SOPs, what frameworks you put in practice. It is also about very close monitoring which you need to do, and auditing those monitors which you have put up besides creating awareness within the organization.”

CDS 2025 EVENT AT A GLANCE

ICICI BANK

DATA SAFEGUARD INDIA

MANAGEENGINE


1KOSMOS | HITACHI

FORCEPOINT | IVALUE

FRUX TECHNOLOGIES

HERITAGE CYBER WORLD

QUALYS

SOTI

PICUS | REGENT

LUCKY DRAW WINNER

LUCKY DRAW WINNER

LUCKY DRAW WINNER

LUCKY DRAW WINNER

LUCKY DRAW WINNER

SPONSORS

PARTNERS

SUPPORTED BY

AI HUB

POWERED BY

VARONIS

PRINCIPAL PARTNER

SOTI

PLATINUM PARTNER

1KOSMOS | HITACHI Inspire the Next

PRIVACY PARTNER

datasafeguard Privacy Management

GOLD PARTNERS

ManageEngine

Qualys.

Forcepoint | iVALUE

NETWORKING PARTNER

Sandyne Technologies

EXHIBIT PARTNERS

HERITAGE CYBERWORLD LLP

FRUX

PICUS | Regent

SUPPORTING PARTNERS

ISODA Infotech Software Dealers Association

PCAIT

A Tech-Driven Roadmap for India's Digital Future

THE UNION BUDGET OF INDIA, AS MANDATED UNDER ARTICLE 112 OF THE CONSTITUTION, SERVES AS THE NATION'S DEFINITIVE FISCAL BLUEPRINT, OUTLINING THE GOVERNMENT'S ANNUAL FINANCIAL TRAJECTORY CONCERNING CAPITAL ALLOCATION, REVENUE STREAMS, AND EXPENDITURE FRAMEWORKS. DERIVED FROM THE OLD FRENCH TERM BOUGETTE, MEANING A SMALL BAG OR WALLET, THE BUDGET METAPHORICALLY ENCAPSULATES THE GOVERNMENT'S ECONOMIC PRIORITIES AND STRATEGIC INVESTMENTS. VARINDIA DELVES INTO THE INTRICACIES OF THE FISCAL PLAN TO DECIPHER ITS IMPACT ON THE TECHNOLOGY SECTOR, EVALUATING KEY ALLOCATIONS, REGULATORY SHIFTS, AND STAKEHOLDER RESPONSES.

In an era of rapid digital transformation, the Union Budget 2025 plays a pivotal role in shaping India's technology landscape, driving innovation, infrastructure development, and regulatory advancements. Presented by Union Minister of Finance and Corporate Affairs Smt. Nirmala Sitharaman on February 1, 2025, the budget lays out a strategic vision to position India as a global leader in cutting-edge technology and digital infrastructure.

With a strong emphasis on artificial intelligence, semiconductor manufacturing, deep-tech R&D, and broadband expansion, the financial blueprint is expected to accelerate the country's digital ambitions. Echoing Telugu poet Gurajada Appa Rao's sentiment—"A country is not just its soil; a country is its people"—the Finance Minister unveiled the budget under the theme "Sabka Vikas", promoting inclusive growth. However, VARINDIA's focus remains on deciphering its impact on India's IT and telecom sectors, examining how the fiscal allocations and policy shifts will influence the industry's trajectory in the coming years.

BUDGET KEY TAKEAWAYS:

- No Income Tax on Average Monthly Income of Upto Rs 1 Lakh; To Boost Middle Class Household Savings & Consumption
- Union Budget Recognizes 4 Engines of Development – Agriculture, MSME, Investment and Exports
- Significant Enhancement of Credit With Guarantee Cover to MSMEs From Rs. 5Cr To Rs. 10Cr
- A National Manufacturing Mission Covering Small, Medium And Large Industries For Furthering "Make In India"
- 50,000 Atal Tinkering Labs in Government Schools in Next 5 Years
- Centre Of Excellence in Artificial Intelligence for Education, With A Total Outlay of Rs. 500 Crore
- Modified Udan Scheme to Enhance Regional Connectivity to 120 New Destinations
- To Boost Battery Production, Additional Capital Goods for EV And Mobile Battery Manufacturing Exempted

Driving Growth & Ease of Business

DR. JAIJIT BHATTACHARYA
PRESIDENT, CENTRE FOR DIGITAL ECONOMY POLICY RESEARCH

"The Union Budget 2025-26 reinforces Ease of Doing Business while boosting agriculture, MSMEs, and healthcare. A key highlight is the nil tax for income up to Rs. 12 lakh, which will spur consumption and increase indirect tax revenue. The budget prioritizes foreign and domestic investments, maintaining fiscal discipline with a 4.4% fiscal deficit target to control inflation and build investor confidence. Trust-based governance reforms aim to unlock entrepreneurial potential, while investments in shipbuilding, energy, and nuclear power will drive MSME growth. Though multi-year in scope, these initiatives signal strong intent. However, budgetary focus on air pollution could have been beneficial. Overall, the budget ensures continuity, supporting businesses, citizens, and economic expansion."

A Boost for Economic Growth & AI Innovation

PRABHAKAR IYER
EXECUTIVE DIRECTOR AND CFO, INGRAM MICRO INDIA

The Union Budget 2025 fosters economic growth with tax concessions, increasing disposable income and driving consumer demand. Key highlights include the Deep Tech Fund to support IT startups, broadband expansion in rural schools and health centers, and a new presumptive taxation scheme (Section 44BBD) to attract foreign electronics manufacturers. The Rs. 500 crore allocation for an AI Centre of Excellence underscores India's commitment to AI, robotics, and machine learning, positioning the country as a global leader in digital innovation. These measures, alongside policies promoting foreign investment and digital infrastructure, create a strong foundation for India's technological advancement and economic expansion.

The Budget Promotes public-private collaborations in cybersecurity

GENIE SUGENE GAN
DIRECTOR, GOVERNMENT AFFAIRS & PUBLIC POLICY, KASPERSKY

“The Union Budget 2025 reinforces India’s digital economy with a strong focus on cybersecurity, innovation, and resilience. Support for MSMEs, deep-tech investments, and AI-powered Centers of Excellence will strengthen the cybersecurity ecosystem. The Deep Tech Fund and Export Promotion Mission will accelerate India’s global tech leadership. Investments in digital public infrastructure, geospatial missions, and streamlined tax compliance will enhance data security and foster public-private collaboration. Kaspersky welcomes the government’s trust-first approach, easing business operations while ensuring compliance. As India advances in AI and digital trust, Kaspersky remains committed to strengthening cybersecurity and securing the nation’s digital future.”

A Balanced and Equitable approach to development

YEZDI NAGPOREWALLA
CEO, KPMG IN INDIA

“The Union Budget 2025 lays a visionary and inclusive foundation for India’s economic growth, aligning with the Viksit Bharat vision. The government’s commitment to reducing the fiscal deficit to 4.4% while ensuring robust economic growth is commendable. Key initiatives like 50,000 Atal Tinkering Labs and the AI Centre of Excellence will equip youth for the digital economy. Support for startups, women entrepreneurs, and rural development ensures balanced progress. Trade initiatives like the Export Promotion Mission and BharatTradeNet will boost global competitiveness. The new Income Tax Bill and personal tax reforms, including higher exemptions and TDS/TCS rationalization, simplify compliance and enhance disposable income.”

Union Budget 2025 focus especially in AI and Deep Tech

PUNEET GUPTA
VP & MD, NETAPP INDIA/SAARC

“The Union Budget 2025 reinforces India’s focus on innovation, skill development, and AI-driven growth. Establishing a Centre of Excellence in AI for education and expanding IITs and IISc reflect a future-ready workforce strategy. Integrating AI and digital skills into mainstream education will enhance accessibility to technology. Government support for MSMEs, along with investments in Centres of Excellence and tinkering labs, will accelerate AI adoption and boost India’s tech capabilities. As AI-driven workloads grow, modern data management is essential. NetApp remains committed to empowering businesses and startups with intelligent data infrastructure, aligning with the government’s vision for economic growth and global impact through technology.”

The Budget 2025 aims to bridge the talent gap

SWAPNA BAPAT

VP & MD- INDIA AND SAARC, PALO ALTO NETWORKS

“The Government of India's ₹500-crore investment to establish a Centre of Excellence in Artificial Intelligence for education marks a decisive step toward realizing AI’s full potential. We appreciate the government’s commitment to upskilling the young workforce for emerging technologies. The creation of national centers for skilling with global expertise under ‘Make for India’, alongside provisions for 10,000 fellowships for technological research in IITs and IISc, will play a pivotal role in bridging the talent gap and preparing professionals for the future of work. The India AI Mission drives AI adoption while addressing security risks. Initiatives like India AI Innovation Centre, Future Skills, and Safe & Trusted AI ensure responsible implementation, fostering a secure, innovation-driven ecosystem for businesses and society.”

Boosting AI & Security Innovations

MR. ASHISH P. DHAKAN

MANAGING DIRECTOR & CEO -PRAMA HIKVISION INDIA PVT. LTD.

The Union Budget 2025-26 lays a strong foundation for steady reforms and technological growth. It provides significant relief for the middle class while fueling India's video security industry. Key highlights include a Rs. 500 crore AI Centre of Excellence for Education, fostering AI-powered security advancements. Investments in domestic semiconductor manufacturing will enhance camera sensors and processing capabilities. Customs duty exemptions on critical minerals like lithium-ion battery scrap will benefit security device production. Expanding broadband connectivity in rural schools and health centers opens new avenues for video security solutions. Additionally, incentives for Make-in-India initiatives will accelerate growth in electronic security. This budget is a step forward in building a more secure and technologically advanced India.

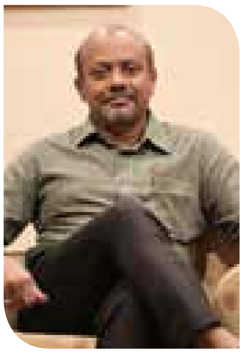
Overall a Progressive Budget targeted at inclusive growth

KAPAL PANSARI

MANAGING DIRECTOR, RASHI PERIPHERALS LIMITED (RP TECH)

“The Budget 2025 strengthens India’s commitment to domestic electronics manufacturing and aligns with the vision of 'Make in India' and 'Digital India.' The increase in the tax-free income threshold to ₹12 lakh is a welcome step that will raise disposable incomes, driving higher demand for consumer electronics, IT peripherals, and gaming products—key focus areas for RP Tech. Additionally, the government's support for the electronics industry and rationalization of customs duties on key components will enhance local manufacturing competitiveness, further strengthening India's position as a global electronics hub. The push to promote Global Capability Centers (GCCs) in Tier-2 cities will accelerate digital adoption and create new opportunities in emerging markets, supporting the broader goals of the 'Digital India' initiative.”

This budget lays a strong foundation for India’s digital future



RAMESH NATARAJAN

CEO, REDINGTON LIMITED

"The Union Budget 2025 presents a forward-looking vision that strengthens India’s digital and technology ecosystem. The continued focus on local manufacturing through reduced import duties on key components is a welcome move, further boosting the Make in India initiative and enhancing supply chain efficiencies. Redington is optimistic about the government’s emphasis on AI, semiconductor development, and skilling initiatives, which will drive innovation and create a future-ready workforce. The incentives for MSMEs and startups will also accelerate digital adoption across industries, fostering a more connected and resilient economy. The increased income tax exemption threshold and greater outlay of funds through welfare schemes is expected to boost both urban and rural consumption of technology products."

The Budget is committed to enhance India’s global competitivenes

SUBHASIS MAJUMDAR

MANAGING DIRECTOR - VERTIV

“The Union Budget 2025 is a pivotal step in India’s journey toward global leadership in manufacturing, technology, and innovation. The National Manufacturing Mission strengthens domestic capabilities, integrates India into global supply chains, and advances the ‘Make in India’ vision. Industry 4.0 adoption will unlock opportunities by harnessing youth talent, fostering a competitive, self-reliant economy. The budget’s transformative reforms, particularly in the power sector, enhance global competitiveness, while a modern regulatory framework and ease of doing business initiatives support enterprise growth. Strategic investments in skilling, AI, and deep tech, including National Centres of Excellence and PM Research Fellowships, ensure India remains a leader in digital transformation, driving sustainable, inclusive economic growth.”

Veeam ProPartner Summit 2025 Emphasizing on AI Powered Data Resilience

Veeam successfully concluded its ProPartner Summit 2025 at Marriott Resort & Spa, Jaisalmer, from February 20 to 22, 2025, bringing together 45 channel partners from 41 organizations along with industry leaders. The event focused on strategic networking, innovation, and collaboration, shaping Veeam's growth strategy in India & SAARC. Discussions aligned with India's "Viksit Bharat" vision, emphasizing data protection, cybersecurity, and digital infrastructure to support the nation's goal of becoming a developed economy by 2047. With a strong focus on cloud adoption and partner collaboration, Veeam is poised to drive digital transformation and security across the region in the years ahead.

CELEBRATING PARTNER EXCELLENCE: JAISALMER JEWELS NIGHT

A key highlight was the "Jaisalmer Jewels Night" awards ceremony, where Veeam honored top-performing channel partners for their outstanding contributions in 2024. This recognition underscored the importance of Veeam's partner ecosystem in driving data resilience amid increasing cyber threats.

A UNIQUE CULTURAL & BUSINESS EXPERIENCE

Beyond strategic discussions, attendees experienced the grandeur of Jaisalmer, with visits to Jaisalmer Fort and the stunning sand dunes, offering a perfect blend of business networking and cultural immersion.

Data Resiliency in a Box: Veeam's Commitment to Zero Data Loss

VARINDIA explored the data protection strategies Veeam adopts and the India specific initiatives, in a chit chat with Mr. Sandeep Bhambure, VP & MD, Veeam India & SAARC.

Veeam's strategy for zero data loss is centered around five key pillars: data protection, data recovery, data security, data portability, and artificial intelligence. These elements work in tandem to provide businesses with an end-to-end solution for safeguarding their critical information.

Data Protection: Organizations invest heavily in securing their data, and Veeam ensures that data is protected at all times with the most advanced backup and recovery mechanisms.

Data Recovery: Veeam enables businesses to restore data at the click of a button, ensuring that operations resume seamlessly.

Data Security: In alignment with Zero Trust architecture, Veeam enhances security by enabling immutable backups and preventing cyber threats from corrupting stored data.

Data Portability: With 75% of organizations facing ransomware attacks in the past year, the ability to recover data from an immutable copy is critical. Veeam ensures that data can be restored to a hosted site, a secondary location, or even a hyperscaler cloud environment, making recovery flexible and efficient.

Artificial Intelligence: Veeam has integrated AI into its platform to detect malware proactively, automate recovery, and ensure that reinfections do not occur during the restoration process.

DISASTER RECOVERY WITHOUT DISRUPTIONS

One of the primary concerns for organizations is ensuring disaster recovery testing without affecting production workloads. At the time of recovery, businesses fear reinfection of their clean data, with studies showing that 56% of companies worry about recovering compromised files. Veeam mitigates this by offering an isolated sandbox to test immutable backups for malware using AI-powered detection like inline entropy analysis, ensuring secure restoration.

Industries like healthcare, finance, and manufacturing rely on Veeam to prevent breaches. Companies such as Mahindra & Mahindra, Hero MotoCorp, and MIT University have strengthened data resiliency, cutting recovery windows by 50% and reducing costs. Veeam ensures seamless, secure recovery, safeguarding business continuity with advanced data protection solutions.

BEST PRACTICES FOR CSOs

As enterprises shift from VMware to alternate hypervisors, migration complexity remains a challenge. Veeam simplifies this with a universally restorable backup format, enabling seamless workload migration across Hyper-V, cloud, or physical servers with minimal effort.

Data protection is now a boardroom priority, driving collaboration between CSOs and CIOs. Veeam's Zero Trust-aligned solutions integrate security and backup, ensuring compliance and resilience. A common myth is that cloud workloads don't need backups, yet Microsoft and AWS recommend third-party protection. Veeam safeguards data across on-prem, hybrid, and cloud environments, ensuring continuous availability and rapid recovery.

THE $15 BILLION POWERHOUSE

Valued at nearly $15 billion with $1.7 billion in annual recurring revenue, Veeam leads global data resiliency. Outpacing Commvault, Rubrik, and Cohesity, Veeam's hardware-agnostic, AI-driven approach ensures seamless disaster recovery and security. Its flexible, software-defined solutions make it the top choice for enterprises seeking robust data protection.

Veeam, recognized by IDC as India's top data resiliency company, is committed to Viksit Bharat through its Cyber Suraksha campaign. With R&D investments in Bangalore, academic collaborations, scholarships, compliance guidance, and industry best practices like 32110, Veeam ensures businesses stay secure, driving a more resilient and secure Bharat.

As organizations navigate an increasingly complex digital landscape, Veeam continues to lead the way in ensuring that no business suffers from data loss. Whether combating ransomware, securing cloud workloads, or enabling effortless migrations, Veeam's commitment to data resiliency remains unwavering, proving that true data protection is indeed "Data Resiliency in a Box."

The Evolving Cyber Threat Landscape and Veeam's Resilience Strategy

During the Veeam ProPartner network, Anthony Spiteri, Regional CTO- APJ, Veeam spoke to VARINDIA. Below are the excerpts..

Cyberattacks are becoming increasingly sophisticated, targeting enterprises at multiple levels. At one end, there are lone-wolf hackers—individuals launching attacks for amusement rather than financial gain, similar to the "script kiddies" of the past. On the other end, highly organized ransomware groups now operate as full-fledged businesses. Groups like Akira, Fog, and Blackbuster, which barely existed a few years ago, have developed into professional operations. They even have help desks, contacting victims post-attack to guide them through ransom negotiations, almost treating them as repeat customers. Given this level of organization and advanced tooling, enterprises today must assume they will be targeted.

VEEAM'S APPROACH TO CYBER RESILIENCE

With 18 years of experience in backup solutions, Veeam has evolved beyond traditional backup strategies to focus on resilience. Recognizing that backup alone is insufficient, Veeam ensures organizations can recover with confidence by implementing immutability, securing backup servers, and maintaining off-site copies. More recently, Veeam has integrated AI-driven malware detection to scan backups and prevent reinfection, addressing the high rate of repeat cyberattacks. In addition, Veeam collaborates with security ecosystem partners—MDRs, EDRs, and SIEM providers—ensuring a comprehensive defense strategy. Through its Coveware acquisition, Veeam also offers incident response services, helping businesses navigate ransom negotiations and minimize operational disruption.

PREPARING FOR NEXT-GENERATION THREATS

As cybercriminals continue to refine their tactics, Veeam leverages real-time intelligence from Coveware's 50 to 100 monthly incident responses. This provides deep insights into attackers' evolving Tactics, Techniques, and Procedures (TTPs), including their target files, hiding strategies, and dwell times. By continuously enhancing AI-driven malware detection and backup scanning, Veeam strengthens its ability to detect and neutralize threats before reinfection occurs. While cybercriminals remain a step ahead, Veeam's proactive approach ensures enterprises are prepared to recover quickly and effectively when an attack inevitably happens.

Veeam ProPartner Network : Valuable Learning Opportunities Through Partner Collaboration and OEM Insights

Speaking with VARINDIA Amarish Karnik, Sales Director & Country Manager- Enterprise & Cloud Services Provider- India & SAARC shared the vision behind Veeam ProPartner network. Below are the excerpts..

The past year has been an incredible journey of growth, with our success reflected in every major industry report, whether from Gartner, IDC, or others. However, this achievement is not ours alone—it is built on the strong foundation of our partners. Without them, we would not have reached this milestone.

STANDING TALL WITH OUR PARTNERS

With over 550,000 customers worldwide, maintaining such a vast customer base is only possible through a robust and diverse partner network. This includes not just traditional partners but also cloud-native partners, service providers, value-added resellers, and implementation specialists. Our partners play a crucial role in delivering the right solutions, and their success needs to be celebrated.

The Pro Partner Summit is an opportunity for partners to learn from one another, exchange best practices, and understand how we collectively solve customer challenges. It's not just about our collaboration; other OEMs, hyperscalers, and hardware vendors also come together, creating a dynamic environment for knowledge sharing.

This year marks the fourth edition of the Pro Partner Summit. We started in Varanasi, moved to Kashmir, then Ayodhya, and now we're in Jaisalmer. The event is all about combining learning with fun, fostering strong relationships, and driving mutual growth.

VEEAM'S COMMITMENT TO ORCHESTRATION AND CYBER RESILIENCE

Veeam Orchestration has significantly improved disaster recovery (DR) for many industries. While we cannot disclose specific customer names due to NDAs, one notable example is a large capital market firm operating entirely on the public cloud. They needed a seamless orchestration solution to manage DR within the same cloud environment.

Veeam enabled them to efficiently transition workloads from their data center (DC) to disaster recovery (DR) sites, ensuring compliance with SEBI and RBI regulations. The automation and reliability provided by Veeam instilled confidence in their business operations, guaranteeing rapid recovery in case of an incident.

Veeam has always followed an agnostic approach—starting with hardware, then hypervisors, and now cloud environments. As we continue to evolve, our orchestration capabilities will expand to additional hyperscalers and hypervisors. In fact, we have already released General Availability (GA) for another hypervisor, with more expansions on the roadmap.

VEEAM'S DIFFERENTIATION IN CYBER RESILIENCE

Cyber resilience has become a boardroom priority, and Veeam is at the forefront of helping businesses prepare for and respond to incidents. Many organizations lack structured processes, so we have been actively engaging with CISOs and CIOs to develop emergency response frameworks.

A key differentiator is our integration of cybersecurity capabilities through the acquisition of Coware last year. Our premium product editions now feature advanced scanning and availability functions, setting us apart from competitors. Additionally, our 3-2-1-1-0 backup strategy ensures zero errors in data protection. Lastly, our transparent partner ecosystem—whether through alliance partners, VARs, or hyperscalers—provides unmatched clarity and trust for both customers and partners.

VOICE OF VARs FROM THE EVENT

The best energizer to keep you invigorated for the whole year

RAHUL TAKKALLAPALLY
CO-FOUNDER, BHARATHCLOUD

"Our association with Veeam is close to 3-4 years now. I enjoyed attending this event as we get to meet a lot of other industry leaders and a lot of insights are shared. It has met more than my expectations in the way this event has been organized. It keeps you energized and the whole energy level remains with you the next one years."

A good place to network and upgrade industry knowledge

ARPIT TRIVEDI, SENIOR VICE PRESIDENT, HITACHI SYSTEMS INDIA

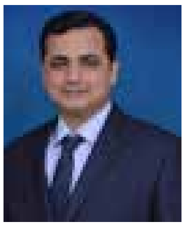
"I personally have been associated with Veeam since its inception in India, almost 2014. Attending these Veeam events help us to upgrade our strategies with respect to what is happening in the market, besides giving ample opportunities in networking and meeting up with industry folks, which again is an add-on. The content that they choose is very precise and is relevant with the industry standards that have been set with similar kinds of events happening these days."

We are aligned with Veeam's vision and goals

JITEN MEHTA, CHAIRMAN, MAGNAMIOUS SYSTEMS

In just two years of partnering with Veeam, our first ProPartner Summit was a highly insightful and motivating experience. It provided clear direction for the upcoming financial year, setting us up for growth. Our team is now aligned with Veeam's vision and goals, and we pledge to actively combat cybersecurity challenges, contributing to our country's development.

Understanding current market scenario and the security landscape



SURESH BACHWANI, CHIEF TECHNOLOGY OFFICER, ORIENT TECHNOLOGIES

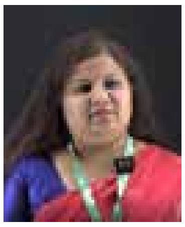
"Events like these give a lot of insights into the current market and they especially touch upon the day to day challenges that we have been facing, which help us in a lot of ways. The key takeaway is the data security and the data resiliency part that is addressed very well in this ProPartner Summit. Moreover, Veeam helps its partners to address the challenges that customers face."

Driving innovation and consistent growth with Veeam

TUSHAR SRIVASTAVA, FOUNDER & CEO, RIA INFOSOLUTIONS

We've been partnered with Veeam for the last five years, growing from humble beginnings to gold partners with multiple VMCs. The Veeam ProPartner Summit offers valuable insights into market growth, data resiliency, and emerging technologies. Veeam consistently exceeds our expectations, ensuring we stay ahead in the evolving tech landscape. It's been a rewarding journey.

Our Veeam partnership drives growth and innovation



REVA SAWANT, BUSINESS MANAGER, SAVEX TECHNOLOGIES

Since our partnership with Veeam in 2020, we've experienced impressive growth and profitability. We're focused on expanding further, particularly in new regions, which is one of our strengths. Attending the Veeam ProPartner Summit was an excellent experience, and we are thrilled to hear about Veeam's AI collaboration and their readiness to embrace new technological advancements moving forward.

Veeam Summit strengthens partnership and strategy

JOSE PRAKASH, EXECUTIVE DIRECTOR, SKYLARK INFORMATION TECHNOLOGIES

We're associated with Veeam for nearly 15 years, and this is my fourth time at the Veeam ProPartner Summit 2025. Each summit offers valuable insights into new trends, products, and features. These learnings help us improve our customers' experience with Veeam solutions, while also ensuring our team is well-equipped to effectively bring these innovations to the market.

Targeting to reach a million-dollar business with Veeam

RS SHANBHAG, FOUNDER & CEO - VALUE POINT SYSTEMS

"We have been associated with Veeam for the last five years and it has been an exciting journey so far. This year we have set ourselves a target of reaching a million-dollar business with Veeam and breaking it to Nifty 500 companies, besides partnering with cloud service providers. This event comes at the right time of our business planning for the next financial year. We get exposed to a lot of great insights, which also go a long way in making many meaningful partnerships for the future."

Proud to be a part of the Veeam ecosystem

DEEPAK JADHAV, DIRECTOR – VDA INFOSOLUTIONS

"We have been associated with Veeam for more than five plus years and have sold their solutions to some of the largest banks. For instance, Kasten is a very niche solution from Veeam and once the cyber resiliency and enterprise-focused innovation gets added up, it has become an industry-leading solution for our customers. We are proud to have been a part of this Veeam ecosystem."

Excited for continued growth with Veeam

CHERIAN THOMAS, CO-FOUNDER, WYSETEK SYSTEMS TECHNOLOGISTS

We've been working with Veeam for almost six years, and their partner program provides everything we need, benefiting both partners and sales teams. The rebate structure is impressive. I'm excited to collaborate closely with Veeam on their new network program. With Veeam's consistent growth, we're eager to build on this partnership and move forward together.

THREAT ALERT: HOW PREPARED ARE INDIAN ENTERPRISES AGAINST DEFENDING CYBERSECURITY RISKS?

As cybercrime evolves into a highly lucrative enterprise, the complexity and sophistication of cyber threats continue to grow. These threats often target businesses across various sectors, exploiting vulnerabilities in systems, networks, and processes.

In this environment, staying ahead of cybercriminals is not just a matter of technology but also strategy and awareness. Businesses that fail to prioritize cybersecurity risk not only financial losses but also their long-term survival.

In today's hyper-connected and rapidly evolving threat landscape, companies are targeted with a variety of techniques that range from phishing and ransomware to supply chain and social engineering attacks. And yet, as per the 2024 Cisco Cybersecurity Readiness Index, merely 4% of organizations in India have the readiness against modern cybersecurity risks, as compared to 3% globally.

However, 59% of organizations fall into the Beginner or Formative stages of readiness. A large number of companies are working towards building defences against these sophisticated attacks, yet they either struggle to defend themselves or are slowed down by their own overly complex security postures that are dominated by multiple-point solutions.

Cisco suggests that the gap that arises between confidence and readiness indicates that companies may appear to be confident in their ability to handle the threat landscape, but eventually fail to accurately assess the true magnitude of the challenges they encounter. That today's organizations need to prioritize investments in integrated platforms and lean into AI in order to operate at machine scale and finally tip the scales in the favor of defenders, is what Cisco recommends.

The readiness against the threats is further hampered by critical talent shortages. 59% of companies surveyed in the Cisco study said they had more than ten roles related to cybersecurity unfilled in their organization at the time of the survey.

According to another study done by global cybersecurity firm Sophos, nearly 65% Indian enterprises paid ransoms to recover data while dealing with cybersecurity attacks. The average ransom demand clocked in at $4.8 million (roughly Rs 40 crore), while the median payment came in around $2 million (roughly Rs 17 crore). Moreover, it took an additional $1.35 million (around Rs 11 crore), on an average, to recover the data.

Cybersecurity experts point out that this reiterates the state of readiness of Indian enterprises in combating cybersecurity and nearly 60% of Indian companies will be found functioning under the cybersecurity poverty line.

The good news is that Indian companies exhibited the most readiness within the AI fortification pillar, with 14 percent in the mature stage and 59 percent in the progressive stage.

Reliance on end-to-end encryption for protecting sensitive information

YOGENDRA SINGH
HEAD-IT/SAP, BARISTA COFFEE COMPANY

"Barista has a well-defined security policy and governance framework, which is effectively monitored, communicated, and enforced across the organization. Regular risk assessments are conducted to identify vulnerabilities and threats. Barista has a well-documented and tested incident response plan and recovery plan in place. Our infrastructure is robustly designed with firewalls, endpoint protection, EDR, XDR, and patch management tools. Additionally, Barista conducts regular security training and awareness programs for employees.

KEY CHALLENGES FACED

Cyber threats are constantly evolving, making it difficult to stay ahead of attackers. New vulnerabilities are discovered regularly, and sophisticated attack methods, such as ransomware or advanced persistent threats (APTs), pose significant risks. This makes it challenging to maintain an up-to-date and effective security posture. Limited budgets, personnel, or technical resources may hinder the ability to invest in advanced security tools, hire skilled professionals, or implement necessary processes. Without adequate resources, it becomes difficult to strengthen security measures, conduct regular risk assessments, or ensure comprehensive employee training. Despite having regular security training, employees may not always be fully engaged or aware of the latest security risks, leading to human errors or lapses in security. Third-party vendors, suppliers, and partners can introduce additional security risks if they do not adhere to the same security practices. We have implemented end-to-end encryption for both data at rest and data in transit to protect sensitive information from unauthorized access to ensure that even if data is intercepted, it remains unreadable without the proper decryption keys. We have also implemented data backup solutions and disaster recovery plans to ensure data can be recovered in case of an incident or breach."

Using AI and ML technologies to enhance cybersecurity defenses

DR. MAKARAND SAWANT
DIRECTOR & CTO - SEAFB

"We, at Samruddhi Enterprises AFB (SEAFB), have done a detailed assessment of our security posture to identify threat vectors and exposure. We have then compared these inputs with the industry standards and benchmarks to identify our current level of security maturity.

KEY CONCERN AREAS

Increasing use of digital platforms for delivering business services are making it more challenging for securing data. We therefore ensure to secure data at all exposure points without impacting business requirements and customer experience.

FOLLOWING INDUSTRY BEST PRACTICES IN SECURITY

We have implemented threat intelligence solutions with industry best practices and standards to monitor for the purpose of identifying and responding to any security incident. We are also implementing ISMS processes as systems as per DPDPA requirements. As far as a robust incident response plan is concerned, we have implemented threat intelligence solutions with automation to monitor, identify and respond to any security incident.

SEAFB is leveraging Artificial Intelligence and Machine Learning technologies to enhance our cybersecurity defenses. We are implementing threat intelligence solutions with AI/ML technologies to monitor, identify and respond to any security incident."

Dealing with ever evolving threats with adequate security measures

PARTHA PROTIM MONDAL
CIO, BERGER PAINTS INDIA

"In today's AI era, understanding your security threat landscape and the maturity to deal with modern age vulnerability is extremely crucial. We have assessed our strength and weaknesses against the predefined security maturity metrics to assure an enriching and mature security posture for the organization. For instance, we have enforced a stringent governance and control that ensures that we have formal security policies and governance structures in place. Again, having an Enterprise Risk Management strategy ensures that we have well defined security risks identified for the organization, have a risk register in place wherein every identified security risk has been prioritize based on severity and its probability of occurrence, mitigation plan for those identified risk with timeline and most importantly we ensure to review such risk periodically.

We also have adequate measures and tools in our arsenal to deal with ever evolving security threats. The modern-age technologies like MDR (Managed Detection and Response), Email Security Software, Zero Trust Framework always give us an edge to stay protected. Training and Awareness is the most crucial aspect of any security methodologies. Most of the security breach happens because of the inadequate knowledge on information security of users who fall prey to the cyber attackers easily.

KEY IMPEDIMENTS TACKLED

There were a few challenges and impediments while enforcing a stringent policy at our organizations. Implementing changes based on assessment findings often require a cultural shift within the organization. Resistance to change can hinder the effectiveness of security improvements. Also, the rapid evolution of cyber threats means that security measures and assessments must continuously adapt."

Assessing new dangers to improve defenses and resistance

RUSHIKESH JADHAV
CTO, ESDS SOFTWARE SOLUTION

"At ESDS, we take a holistic approach to security maturity that includes industry best practices, regulatory compliance, and advanced threat intelligence. Our security framework adheres to global standards such as ISO 27001, GDPR, and PCI DSS, ensuring a robust cybersecurity posture. Our security maturity varies from progressive to mature, with investments in continuous threat monitoring and a Security Operations Center (SOC) that operates 24/7. We detect abnormalities with AI-driven threat intelligence, encrypt data at rest and in transit, deploy Zero Trust Architecture (ZTA) to manage access and reduce insider threats, and conduct frequent vulnerability assessments and penetration testing (VAPT) to identify and mitigate risks.

To ensure data protection and compliance, we have implemented a comprehensive, multi-layered approach to protect sensitive information while following international and local regulations.

- Data Encryption and Access Controls- Data Encryption: We use AES-256 encryption for data at rest and TLS 1.3 for data in motion against unauthorized access. The Zero Trust Security Model controls access to sensitive data with multi-factor authentication (MFA) and least privilege principles.
- Compliance with Industry Regulations: ISO 27001 and PCI DSS Certified: We ensure that our data processing is in line with international security standards.

ESDS also has a very structured and well-documented Incident Response (IR) plan, which adheres to the best practices of NIST (National Institute of Standards and Technology). We are always using AI and ML to enhance our cybersecurity defenses to automatically detect and alert threats. AI and ML are the tools needed to predict, avoid, detect, and respond to cyberattacks."

Investing continuously in security R&D to improve threat detection capabilities

ANIL NAMA
CIO, CTRLS DATACENTERS

"At CtrlS, we maintain a high level of security maturity, bolstered by our extensive experience in the field. We maintain established protocols for evaluating and addressing security risks, which include criteria for the selection and application of security measures such as access controls, encryption, and firewalls. Additionally, we have formulated policies and procedures for the monitoring and identification of security incidents, encompassing reporting mechanisms and incident response strategies. Furthermore, we provide guidelines to ensure adherence to legal and regulatory obligations pertaining to security.

Access to user data within CtrlS Datacenters is strictly restricted to authorized individuals, governed by comprehensive policies that regulate access, scripting, updates, and remote connections. Data is stored within secure networks that are password-protected and not accessible to the public. Information transmission between users and CtrlS is encrypted ensuring industry-standard encryption strength. Our intrusion detection system, embedded within CtrlS, enhances our readiness, management, and defense against network threats, addressing a broad range of risks including DDoS attacks, port scans, and backdoor breaches. We conduct regular vulnerability assessments and penetration tests to identify and address potential security vulnerabilities. Furthermore, CtrlS is committed to ongoing investment in security research and development to improve threat detection capabilities, thereby ensuring the continuous protection of sensitive information."

Leveraging AI-based tools to detect breaches in real-time

PRINCE JOSEPH
GROUP CHIEF INFORMATION OFFICER, SFO TECHNOLOGIES PVT. LTD. (NEST GROUP)

"While progress has been made, there are gaps in addressing evolving threats. Even organizations that comply with audits and regulations often experience breaches due to vulnerabilities in attack surfaces. Rising cloud adoption and digital transformation require constant updates to security architecture. Security maturity involves not just periodic checks like VAPT or red teaming but meaningful efforts to strengthen all surfaces and ensure a proactive, robust posture against increasingly sophisticated attacks.

KEY CHALLENGES FACED

Key challenges include addressing vulnerabilities in dynamic environments, insufficient integration between traditional and cloud-native security solutions, and ensuring timely updates to security postures. Breaches often expose gaps despite regulatory compliance. Additionally, exercises like VAPT and red teaming, while common, lack depth when treated as checkbox activities. Organizations must move towards proactive, adaptive strategies that consider all attack vectors, including emerging risks from AI-driven and cloud-based architectures.

We ensure compliance with strict regulations through continuous audits, data encryption, and multi-layered access control. A comprehensive incident response plan is in place, incorporating rapid threat detection, containment, and recovery protocols. However, the dynamic nature of cyber threats necessitates ongoing reviews and drills to strengthen readiness. The plan is supported by a well-equipped Security Operations Center (SOC) and we are looking to leverage AI-based tools to detect breaches in real-time. It emphasizes collaboration across teams to mitigate damage and ensure business continuity effectively."

Securing data across multiple environments is our top priority

NARAYAN MISHRA
CO-FOUNDER & CTO, TUMMOC

“At Tummoc, we have built a strong security framework that aligns with industry best practices, placing us at an advanced stage of security maturity. However, cybersecurity is an ongoing process, not a static one. We continuously enhance our measures to stay ahead of evolving threats and regulatory requirements.

SECURING DATA, EDUCATING USERS

The biggest challenge we face is the constantly changing nature of cyber threats, like phishing and ransomware. As a cloud-native platform, securing data across multiple environments remains a top priority. We also focus on educating users and employees about security best practices, recognizing that technology alone cannot prevent all risks.

LAYERED SECURITY FOR PROTECTION

Data privacy is a core principle at Tummoc. We employ a multi-layered security approach, utilizing AES-256 encryption for data at rest and TLS encryption for data in transit. Our compliance framework is in line with GDPR, the IT Act 2000, and CERT-In guidelines. Role-based access control (RBAC) and multi-factor authentication (MFA) safeguard against unauthorized access. Regular security audits and penetration testing are key to identifying vulnerabilities. While we do not yet leverage AI/ML for cybersecurity, we employ rule-based monitoring and a mix of manual and automated tools. Continuous monitoring and security patching are integral to our strategy, ensuring we stay ahead of potential threats.”

Saviynt meets all global and local compliance standards

AKSHAY SIVANANDA
CISO, SAVIYNT

“We evaluate our security maturity using industry-standard frameworks like the NIST Cybersecurity Framework (CSF) to assess our overall security posture and control effectiveness. This approach helps us identify and manage cybersecurity risks in a way that is clear to both the board and the organization. We also use common control frameworks to implement detailed controls and maintain compliance with various certifications. A central focus of our security strategy is resilience—ensuring that we can recover operations swiftly within defined recovery timeframes while restoring systems and business processes to acceptable levels of performance and data accuracy.

EVOLVING THREATS POSE A BIG CHALLENGE

The biggest challenge we face is the rapidly evolving threat landscape. Cybercriminals are increasingly leveraging automation, advanced engineering, and AI to create complex attacks, making traditional defense methods insufficient. Ransomware, including Ransomware-as-a-Service (RaaS), remains a major concern. Another challenge is the unmanaged proliferation of generative AI within organizations. While GenAI can enhance productivity, it poses risks that need to be carefully managed.

ROBUST COMPLIANCE AND RESPONSE

To address these issues, Saviynt maintains a strong compliance posture, holding certifications like SOC 1 Type 2, SOC 2 Type 2, ISO 27001, and FedRAMP Moderate. Our robust Incident Response (IR) plan includes standardized communication and transparency with customers. Additionally, we leverage AI/ML technologies in our cybersecurity defenses to manage evolving threats and enhance security.”

Compass strengthens security maturity with global assessments

MANISH MAMTANI
CIO, COMPASS GROUP INDIA

“We assess our security maturity through a global security assessment framework, with each country submitting quarterly responses, complete with evidence and artifacts. These assessments are reviewed by the Regional Risk Security Officer and Group CISO, complemented by independent evaluations from cybersecurity organizations. Additionally, we undergo 12-15 annual assessments from our multinational clients, ensuring compliance with global standards and driving continuous improvement of our security practices.

MANAGING CYBERSECURITY ACROSS LOCATIONS

The biggest challenge is managing cybersecurity across our distributed workforce, with employees at over 600 customer sites. Ensuring all are informed about cybersecurity, data privacy, and IT policies is crucial. We address this through clear, simple communication via targeted campaigns, making complex topics easier to understand. Our data privacy and security controls align with regulations, and the Security Assessment Framework ensures their effective implementation. Quarterly assessments ensure ongoing compliance and adaptation to evolving regulatory requirements.

STRENGTHENING DEFENCE WITH AI

We also have a robust incident response plan, part of our Security Incident Response Management (SIRM). To validate its effectiveness, we regularly conduct tabletop exercises. Additionally, we leverage AI/ML technologies to enhance our cybersecurity defenses. Advanced solutions are deployed across key areas such as internet gateways, malware protection, spam management, Security Operations Centers (SOC), and Cloud Security Posture Management (CSPM), adding an extra layer of protection against emerging cyber threats.”

We prioritize crisis management with future-ready security

DR. HARSHA THENNARASU

FOUNDER & CISO, HKIT SECURITY SOLUTIONS

"We assess our security readiness by thoroughly understanding cyber threats, including their origin, methods, and solutions. We focus on crisis management when threats arise and prevent future risks by maintaining global security intelligence. This is achieved through collaboration with research forums and ethical hackers. Our approach involves continuous threat forecasting, strategic development, and acquiring future-ready skills. We refine policies and governance to stay ahead of emerging threats, focusing on people, organizational structures, technology, and physical controls.

KEEPING UP WITH THREATS

One of the biggest challenges we face is the rapid pace of technological transformation. We must adopt and implement new technologies swiftly while training teams and securing leadership's support for cybersecurity. Financial constraints and the recruitment of skilled cybersecurity experts also pose challenges. The speed of technological adoption must match the evolving tactics of cybercriminals, creating a constant race against time.

MULTI-LAYERED SECURITY DEFENCE

To ensure data privacy and compliance, we've transformed leadership's understanding of cybercrimes and their business impact, including penalties and service disruptions. By discussing business case studies and legal implications, we foster a top-down approach to drive awareness among stakeholders. We've deployed a multi-layered incident response plan that incorporates real-time, reactive, proactive, and forecast responses. Additionally, we're developing AI-based tools to combat emerging threats."

We strengthen cybersecurity through structured continuous improvements

JASPREET SINGH

PARTNER AND GCC INDUSTRY LEADER, GRANT THORNTON BHARAT

"We start by defining our security objectives and selecting a suitable cyber maturity assessment framework. A self-assessment evaluates current practices, highlighting strengths and weaknesses. Based on the findings, we create an improvement plan, prioritize actions, and allocate resources. The plan's implementation is closely monitored, with regular updates to ensure continuous improvement and alignment with emerging challenges. This approach gives us a clear understanding of our security posture, guiding necessary improvements.

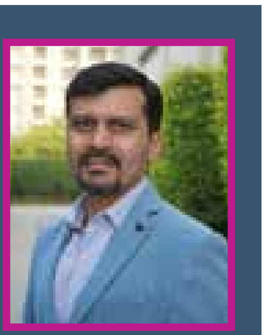
OVERCOMING SECURITY CHALLENGES

However, we face several challenges, including rapidly evolving cyber threats, complex IT infrastructures, and securing remote workforces. Cybercriminals are becoming more sophisticated, using tactics such as AI-driven attacks, ransomware, phishing, and zero-day exploits. Securing cloud and on-premises systems while managing third-party risks adds complexity. The rise of remote work has also made securing access across multiple locations more difficult.

DATA PRIVACY MEASURES IN PLACE

To ensure data privacy, we implement data mapping, strong security controls, and compliance training. Our incident response plans are updated, and audits ensure alignment with regulations. Third-party risk management ensures partners meet security standards. We leverage AI and machine learning for enhanced cybersecurity, enabling faster threat detection, predictive analytics, and automated operations. AI plays a crucial role in strengthening our defenses against cyber threats, ensuring rapid incident response and protection."

We align security practices with industry standards



TEJAS SHAH

HEAD – IT, PRINCE PIPES AND FITTINGS

"Our approach to assessing security maturity focuses on aligning practices with industry standards and best practices. We ensure robust security through regular updates, risk assessments, and strong policies. Key priorities include role-based access control (RBAC), multi-factor authentication (MFA), and password management. We emphasize patch management, user training, and continuous evaluation of firewalls and endpoint protection. Regular security audits and vulnerability assessments help proactively identify and mitigate risks, ensuring our security framework adapts to emerging threats.

ADDRESSING SECURITY ADOPTION BARRIERS

A major challenge in enhancing security is overcoming user resistance to change and the cultural shift required for adopting new security practices. Additionally, balancing limited budgets with the need for stronger security measures remains difficult. Addressing these hurdles requires ongoing efforts to foster security awareness and commitment at all organizational levels, ensuring full adoption and alignment with security goals.

ENHANCING DATA PRIVACY AND COMPLIANCE

To ensure data privacy and compliance, we implement strict measures like collecting only necessary data, enforcing RBAC, and requiring MFA for sensitive information access. Regular audits and assessments reinforce compliance and improve data protection. Additionally, AI and machine learning technologies play a crucial role in fortifying cybersecurity. AI-driven tools aid in proactive threat hunting, dark web monitoring, and attack surface management. Automated vulnerability scanning and AI-powered endpoint detection further enhance our security."

Evaluating cybersecurity readiness and capabilities at every level

DINESH KAUSHIK
CIO, SHARDA MOTOR INDUSTRIES

"We assess your current level of security maturity in the following ways -

· Interpretation: This question seeks to understand how the organization evaluates its cybersecurity capabilities and readiness.

· Addressing key points -

ü Use of maturity models (e.g., NIST Cybersecurity Framework, CMMI).

ü Regular security audits, assessments, and gap analyses.

ü Monitoring and metrics for security performance.

ü Training and awareness programs for employees.

To implement and ensure data privacy and compliance with relevant regulations, we do an interpretation to focus on legal and operational steps to protect sensitive data and maintain compliance. Other potential measures include encryption of data in transit and at rest, Access control mechanisms (e.g., role-based access), Regular data audits and monitoring, Compliance with standards (e.g., GDPR, CCPA, HIPAA) and Data retention and destruction policies.

Besides, we assess the adoption of advanced technologies in combating cyber threats. Examples of AI/ML use include threat detection and anomaly identification, predictive analytics for proactive threat management, automating routine tasks like log analysis, identifying and blocking phishing attempts and enhancing user behavior analytics."

Aligning with industry standards and best practices for assessing security maturity

DR. JAGANNATH SAHOO
HEAD – INFORMATION SECURITY, GUJARAT FLUOROCHEMICALS LIMITED

"Assessing your organization's security maturity involves evaluating how well its security practices, policies, and technologies align with industry standards and best practices. We follow the below steps to Assess Security Maturity -

- Defining the Security Maturity Model as per ISO 27001, NIST CSF Framework
- Establishing Evaluation of different Domains, GRC, Asset Management, Threat & Vulnerability Management, Incident response & recovery, Security Awareness training, Compliance & Audit.
- Benchmark Against Standards & Perform a gap analysis against chosen standards
- Conduct Internal and External Audits using scorecards and checklists & using Engage third-party auditors for unbiased evaluation
- Using e Security Maturity Tools like Security Scorecard
- Evaluate Metrics and KPIs, Monitor MTTD, MTTR, number of incidents, audit scores, and system compliance
- Incorporate Stakeholder Feedback by Gathering inputs from IT teams, business units, and external partners
- Create a Roadmap for Improvement
- Monitor Progress and Reassess.

Some of the challenges faced in assessing security maturity are lack of clear framework adoption, limited visibility, resource constraints, complexity of integration, dynamic threat landscape, compliance overload, stakeholder alignment and tools & technology gaps."

US seeks clarification from EU on Big Tech regulations

US House Judiciary Committee Chairman Jim Jordan has sought clarification from Teresa Ribera, the EU's Antitrust Chief, on the enforcement of the EU's Digital Markets Act (DMA) and Digital Services Act (DSA). This request follows US President Donald Trump's memorandum to scrutinize the EU's digital regulations, which affect American companies' dealings with EU consumers.

The DMA, designed to ensure fair competition, sets strict rules for major tech firms like Alphabet, Amazon, and Microsoft, targeting anti-competitive behaviour. However, US lawmakers argue the DMA could disproportionately burden US firms while benefiting European companies.

In a letter, Jordan and Scott Fitzgerald, Chairman of the Subcommittee on Antitrust, criticized the law's hefty fines and raised concerns that it could stifle innovation and favour Chinese firms. They requested Ribera's appearance before the Judiciary Committee by March 10 to discuss these issues, which the European Commission has denied.

Apple collaborates with Alibaba to introduce AI features for iPhones in China

Apple has announced a strategic partnership with Alibaba to expand its AI offerings in China, navigating the country's strict regulations. While AI integration in iPhones has been slow, particularly in non-English-speaking countries, China's regulatory complexities made the market challenging. Instead of entering alone, Apple has teamed up with Alibaba to develop a localized version of its AI features that comply with government rules.

Reports suggest the collaboration's AI features have been submitted for approval by Chinese regulators, aiming to be integrated into future iOS updates. If approved, it could boost Apple's position in China, where iPhone sales have declined since 2024.

Apple previously explored partnerships with Baidu, Tencent, and ByteDance, but challenges led to the collaboration with Alibaba. With access to user data from platforms like Taobao and Tmall, Alibaba's AI expertise offers Apple the ability to tailor smartphone AI features to the local market.

CADYCE CA-CT568: The Ultimate Crimping Tool for Network Professionals

CADYCE has introduced the CA-CT568 Dual Modular Network Crimping Tool, a state-of-the-art solution designed to streamline cable crimping, stripping, and cutting for IT and networking professionals. This versatile tool enhances productivity by integrating multiple functions into a single, user-friendly design, making it an essential addition to any toolkit.

PRECISION, DURABILITY, AND EFFICIENCY

Engineered with high-quality materials and advanced mechanisms, the CA-CT568 ensures secure and consistent connections. Its ratchet mechanism minimizes hand fatigue, while its corrosion-resistant build enhances durability. Designed for data centers, home installations, and professional networking setups, this tool guarantees seamless performance, ensuring strong and stable connections every time.

SALIENT FEATURES OF CA-CT568 INCLUDE:

- Dual Modular Functionality: Allows crimping, stripping, and cutting with a single tool, streamlining workflow.
- Wide Compatibility: Supports RJ-45 (8P8C), RJ-11 (6P4C), and RJ-12 (6P6C) connectors, making it ideal for various cabling needs.
- Ratchet Mechanism: Reduces hand fatigue and ensures secure, consistent crimping.
- Corrosion-Resistant Build: Designed for long-term durability in demanding environments.
- Ergonomic and Compact Design: Provides a comfortable grip and ease of use in tight spaces.
- Precision Modular Holder: Ensures perfect alignment for reliable connections.

THE CADYCE CA-CT568 IS A MUST BUY FOR:

The CA-CT568 is a must-have for professionals seeking accuracy, efficiency, and durability in network installations. Its advanced design and robust construction allow for professional-grade crimping, ensuring strong and stable connections every time.

The CADYCE CA-CT568 is now available for purchase through CADYCE's official website and authorized resellers.

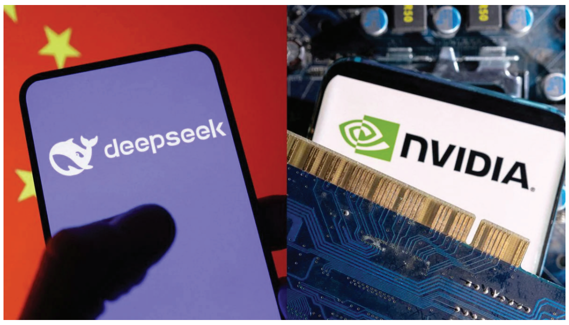
EU approves Nokia's $2.3 billion acquisition of US firm Infinera

The European Commission has given unconditional approval for Nokia's $2.3 billion acquisition of Infinera, a leading US-based optical networking provider. This decision allows Nokia to expand its presence in the optical transport equipment sector without raising competition concerns.

The acquisition, announced in June 2024, involves a cash and stock deal where Nokia will purchase Infinera's shares at $6.65 each, offering a significant premium over its market value at the time. The European Commission's assessment concluded that the merger would not hinder competition, noting that the combined market share of both companies remains moderate, with numerous competitors still exerting pressure in the sector.

The merger is expected to strengthen Nokia's position by expanding its product offerings and enhancing its competitiveness against larger industry players. Integrating Infinera's expertise in open optical networking and advanced optical semiconductors will boost Nokia's capabilities in digital signal processing and silicon photonics. The acquisition also increases Nokia's ability to supply optical networking solutions to major tech firms like Amazon, Alphabet, and Microsoft, which are heavily investing in data centers for AI growth.

Nvidia H20 chip orders surge as Chinese firms adopt DeepSeek AI



Chinese companies are ramping up orders for Nvidia's H20 artificial intelligence chip due to the boom in demand for DeepSeek's low-cost AI models. The increase in orders underlines Nvidia's dominance of the market and could help alleviate concerns that DeepSeek might cause a slide in AI chip demand. Tencent, Alibaba and ByteDance have "significantly increased" orders of the H20, a chip specific to China due to US export controls, ever since the Chinese AI startup burst into the global public consciousness recently.

In addition to their internal needs for advanced AI chips, the three tech giants provide cloud computing services through which other firms can access and use AI tools. Previously only deep-pocketed financial and telecom firms bought servers with AI computing systems. But now smaller companies in sectors like healthcare and education are also reportedly purchasing AI servers equipped with DeepSeek models and Nvidia H20 chips.

DeepSeek's large language models rival Western systems in performance at a fraction of the cost as they focus on "inference" or producing conclusions. That optimises computational efficiency rather than relying solely on raw processing power.

Ashu Virmani is the new National Head (Alliances) TP-Link India

TP-Link India has appointed Ashu Virmani as the National Head, Alliances, as part of its strategic efforts to strengthen its enterprise networking business. With Ashu leading the alliances, the company aims to establish key partnerships with major industry players. Bringing over 25 years of experience in strategic alliances, enterprise solution selling, and business development, Ashu is a valuable addition to the TP-Link team.

“We are excited to welcome Ashu to our team. His strategic vision and deep industry expertise will be pivotal in driving our growth through Tier 1 partners in the enterprise segment,” said Mr. Sanjay Sehgal, Director & COO, TPLink India.

Ashu has a strong track record of executing large-scale business strategies, forging impactful partnerships, and leading enterprise growth initiatives.

SAP gets new Regional President, Asia Pacific

SAP Asia Pacific (APAC) has announced Simon Davies as President for the newly-created APAC region, effective immediately. Based in Singapore, Davies will oversee strategy, operations, people, sales, services, partners, and profitability across Asia Pacific for SAP SE. After five years in the role, Paul Marriott returns to Europe to be closer to family.

With SAP market units operating in Australia and New Zealand (ANZ), Greater China, India, Japan, Korea, and Southeast Asia, Davies will be responsible for overseeing more than 31,000 employees across 78 offices. Across the APAC region, SAP services leading customers including NEC Corporation, Coles Group, Wipro, Fujitsu Limited, Shiseido, Hyundai Motor Company, Kia Corporation, Himalaya, Cochlear, and Japan Airlines.

Prior to this appointment, Davies has spent 25 years building, selling, and implementing IT solutions in Asia Pacific, working with some of the world's leading software companies.

Cloudflare promotes Goran Risticevic as VP & MD for APAC

Cloudflare has appointed Goran Risticevic as the new Vice President and Managing Director for Asia Pacific (APAC), reinforcing its commitment to expanding its presence and technological influence in the region. In this role, Risticevic will oversee business operations, strategic partnerships, and regional growth. As APAC experiences rapid digital transformation, his leadership is key to accelerating Cloudflare’s adoption among enterprises, governments, and startups across Australia, India, Japan, and Southeast Asia.

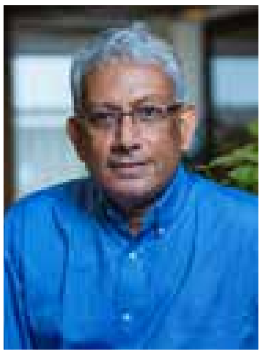
With over 20 years of experience in technology leadership, sales, and business strategy at companies like AWS, IBM, and NetApp, Risticevic has a proven track record in driving growth and market penetration. He joined Cloudflare in November 2022 and has since been building its Customer Success and Services team in the region. Based in Sydney, Risticevic will focus on enhancing security, optimizing performance, and improving internet reliability for businesses across key APAC markets.

Gopal Vittal appointed as Acting Chair of the GSMA Board

Gopal Vittal, Vice Chairman & MD, Bharti Airtel and Deputy Chair GSMA has been appointed as the Acting Chair of the GSMA board following the resignation of José Maria Álvares-Pallete, Chairman & CEO, Telefónica from the company. By virtue of this resignation, he is no longer able to continue in the position of the Chair of the GSMA.

Gopal was recently re-elected as the Deputy Chair of the GSMA board. He has also served the board as a key member for the term 2019-2020.

GSMA represents the global telecommunications industry with over 1100 companies from the telecom ecosystem across the world including telecom service providers, handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors.



Ravi Venkatesan joins ServiceNow global advisory council

ServiceNow has appointed Ravi Venkatesan as a member of its Global Advisory Council (GAC). Venkatesan will play a pivotal role in enhancing ServiceNow's engagement with its customers and industry leaders to solve their biggest challenges, leveraging his extensive experience as Chairman of the Global Energy Alliance for People and Planet (GEAPP) and his deep expertise in leadership, innovation, and global collaboration.

Ravi Venkatesan said, "I'm thrilled to join ServiceNow's Global Advisory Council at this pivotal moment. ServiceNow’s platform is leading the charge in redefining the future of work, and I'm particularly drawn to their commitment to unlocking human potential through AI. I look forward to helping forge strategic connections that help customers transform their business through human-centric AI solutions.”

Anurup Singhal joins Zscaler as the Head of India Commercial Business

Zscaler has appointed Anurup Singhal as the Head of India Commercial Business. With a robust background spanning over 19 years in companies like Microsoft and GoDaddy, Singhal is expected to lead Zscaler's initiatives to secure Indian enterprises in the evolving digital landscape.

Singhal's diverse experience includes leading Digital Sales for SMB across Asia at Microsoft, and serving as Chief Revenue Officer at 92.7 Big FM, where he gained deep insights into B2B sales and media strategy. His appointment is anticipated to drive Zscaler's mission of enabling secure digital transformation for businesses across India. His leadership is anticipated to drive the adoption of such collaborative solutions, fostering a more secure and resilient digital infrastructure for Indian enterprises.

On his appointment, Singhal commented, "I am grateful for the opportunity to build and lead a dedicated team, working together to expand and fortify the India Commercial Business. Our goal is to truly secure Indian businesses by leveraging Zscaler's cutting-edge cybersecurity solutions and promoting the adoption of Zero Trust architecture. I am committed to driving growth, fostering innovation, and delivering exceptional value to our clients, all while upholding and advancing the mission of Zscaler."

Instant On

HPE Networking Instant On Switch Series 1930

Delivers reliable connectivity to small and medium-sized businesses

*now with new HPE Networking Instant On transceivers and DOC cables

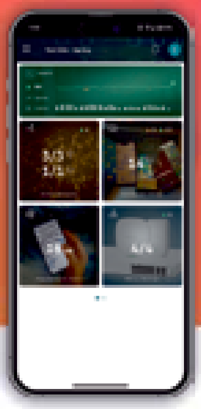
Smart-managed L2+ switches with fibre uplinks, now come in 7 models

Fiber uplinks
- SFP model: 8-port
- SFP/SFP+ models: 24-port and 48-port

POE models
- 8-port: 124W
- 24-port: 195W, 370W
- 48-port: 370W

Key features to help unlock your business potential

- Default firmware upgrade
- Jumbo frame
- Connectivity texts
- Authentication and security (802.1x)
- Power schedule
- Loop protection



- Managed through web GUI or Mobile app
- PoE budget (Availability)
- VLAN port tagging
- Limited lifetime warranty
- Advance onsite replacement

Perfect for: Boutique hotels | Cafes | Professional offices | Retail stores

Hewlett Packard Enterprise | savex TECHNOLOGIES

For more details contact
Geeta Arora | +91 9818817490 | geeta.arora@savex.in

RNI - NO 72399/1999

Reg. No: DL-SW-01/4030/24-26
Posted at LPC Delhi RMS Delhi - 110006

Date of Posting 20 & 21
Date of Publishing / Printing: 18 & 19

64 pages including cover