Trade Promotion Council of India

****

TPCI organises the India AI Advantage Summit 2026 in New Delhi

- *Cyber fraud losses increase by more than 200%; need for 13 lakh cybersecurity professionals to tackle risk*
- *The government advise stakeholders to be compliant with the DPDP Act and stick to the baseline practices and guidelines.*

New Delhi; 27th October 2026: To build a resilient, secure framework for India's expanding artificial intelligence infrastructure, the Trade Promotion Council of India (TPCI) organised the flagship India AI Advantage Summit 2026 at ITC Maurya, New Delhi. The opening plenary witnessed participation from senior voices from MeitY, CERT-In, STPI and Capgemini. The summit featured six sessions on generative AI, deepfakes, agentic AI, data privacy and governance, AI in cyber defence, and trust in digital transactions.

Shri K K Singh, Joint Secretary, MeitY, was the Chief Guest of the India AI Advantage Summit 2026. The other distinguished guest included: Shri Mohit Singla, Chairman, TPCI, Shri Diwakar Jaiswal, Additional Director, Software Technology Parks of India (STPI), Ms Padmashree Shagrithaya, EVP & Head of Insights & Data – India, Capgemini, Shri Ashutosh Bahuguna · Scientist 'F'/Director, CERT-In, MeitY, Shri Nikhil Malhotra · Chief AI & Innovation Officer, Tech Mahindra, Shri Nitin Kaushik · Director Cloud Engineering, Oracle India, Shri `Ritesh Jain · Partner, PwC, etc.

The India AI Advantage Summit 2026 saw the unveiling of a report conducted by TPCI and CyberPeace titled AI-Generated Deepfakes and Voice Cloning Targeting Indian Enterprises. According to the report, the cyber fraud losses in India rose from ₹7,465.1 crore in 2023 to ₹22,845.7 crore in 2024, a rise of about 206%. Incidents registered on the National Cyber Crime Reporting Portal rose by 42%, from about 16 lakh to more than 22.6 lakh. No official figure separates out deepfake or voice-clone losses, so this paper works from the cases that are on the public record.

In the same survey, 47% of Indian adults said they had been affected by an AI voice scam, either personally (20%) or through someone they know (27%). In one study, only 0.1% of 2,000 participants correctly sorted every real and fake sample, while over 60% were confident they could spot a deepfake. A control that depends on someone noticing something odd will fail sooner or later.

The live deepfake attack simulation and case studies were also demonstrated during the session. The Summit witnessed participation of 250+ CXOs, CISOs, CTOs and policymakers.

Delivering his keynote address, Shri K. K. Singh, JS, MeitY, said, “The Digital Personal Data Protection Act (DPDP Act) has been notified. "So, we believe that the industry is prepared; it is going to be operational from somewhere in mid-2027. This is also an opportunity for the industry because many solutions will be required to handle the privacy and preservation aspects. Therefore, the industry will have to come up with solutions that are affordable and more efficient…Today we have 5 lakh cybersecurity professionals, and there is a need for 13 lakh professionals to tackle the risks," he noted.

Further, Shri Singh observed that cyber defence is a critical sector; many fraud incidents are not even reported. We don’t have a separate regulation as the current IT rules are sufficient to address the challenges. If there is a need, we can consider having separate regulations.” If the industry is able to manage its governance, available tools, and protocols, alongside whatever advisories are issued, we believe we will be in a better position to tackle and handle these cybersecurity risk matters, he added.

Looking at the software industry, he noted, “All of you are aware that we have around a 315 billion US dollar industry, out of which around 246 billion US dollars are exported to the USA alone. We also have over 60 crore worth of digital transactions every day, making trust a very important aspect of cybersecurity.”

Addressing the AI Summit Shri Mohit Singla said, “Every great technology has its moment of arrival. Steam took decades to leave the mine and reach the factory. Electricity took decades more to reach the home. The internet took years to reach the pocket. Artificial intelligence has done what none of them did. It has reached the boardroom, the classroom, the clinic and the smartphone almost at once. In barely four years, it has travelled from the laboratory to the language of everyday life.”

Our mandate is to ask what will decide whether an Indian business wins or loses in global markets in the years ahead, and to help industry prepare before that question becomes a crisis. AI is now one of those questions. The numbers show how quickly it is being answered. A recent survey of Indian organisations found that 47 per cent are already running multiple generative AI use cases, and 93 per cent plan to bring AI agents into their operations within the next 12 to 18 months. This is no longer a pilot phase. It is a race, and in a race the question is not whether to run, but how. India's opportunity is real. AI can solve structural challenges, lift productivity across sectors, and strengthen the position of Indian enterprises, large and small, in every market they serve, he added.

Further, Chairman TPCI underlined that the Council wants that advantage to belong to the many, not just the few. But AI is a double-edged sword, and it would be a failure of leadership to speak only of the edge that cuts in our favour. The same technology that drafts a contract can forge a voice. The same intelligence that detects fraud can manufacture an identity. Deepfakes, voice cloning and synthetic identity fraud are no longer concerns of the future. They are at the door of the boardroom today. And trade runs on trust. When a buyer abroad transfers payment because a voice sounded familiar, or a supplier ships goods because a face on a screen looked genuine, trust is the currency. When that currency can be counterfeited, the cost of doing business rises for everyone. AI accelerates everything. Guided wisely, it carries us towards growth faster than we have ever travelled. Deployed without security, privacy and governance, it carries us to the wrong place at the same speed. Industry must understand both edges of this technology, and prepare for both, now. That is why this Summit has been so carefully curated.

The top three demands that emerged from the study conducted and inputs of the industry during the summit are as follows:

1. Adopt a policy that no payment, credential change or data release is approved on the basis of voice or video communication alone, and apply it to the CEO and the board first.
2. Build a consolidated reporting playbook that covers the bank, the 1930 helpline, CERT-In, the sector regulator, the Data Protection Board and the police.
3. Test the whole arrangement within 90 days through a tabletop exercise built around a deepfake scenario that escalates to the board.