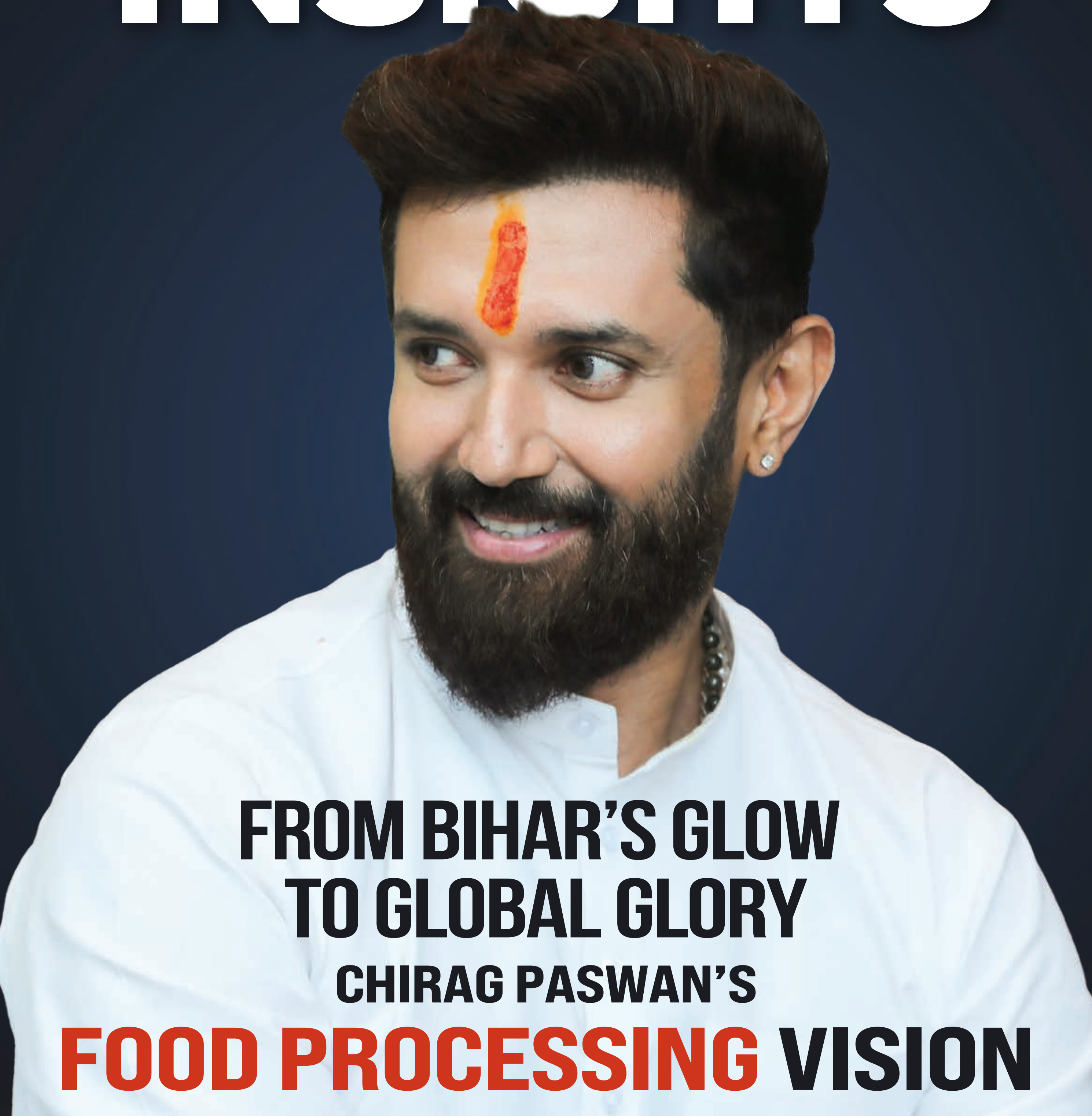
https://etedge-insights.com/

Vol. 05

LEGACY ON THE MENU ● INDIA'S AI SUPERCLOUD ● FROM BARCODES TO SMART CODES ● INDIA'S EYE IN THE SKY

# ET EDGE INSIGHTS



## FROM BIHAR'S GLOW TO GLOBAL GLORY

## CHIRAG PASWAN'S FOOD PROCESSING VISION

## OPINION

ET Edge INSIGHTS

Conceptualised & Executed by
ET Edge
THE TIMES GROUP

**Chief Executive Officer** - Rohit Gopakumar

**Chief Operating Officer** - Sunita Quadros

**Business Solutions** - Samuel Ebenezer, Manoj Nair, Ruchika Singh

**Editorial Strategy** - Abhishek Dutta, Alka Kaur

**Editor** - Tanmoy Mitra

**Editor (Sustainability)** - Queenie Nair

**Senior Content Writer** - Poonam Mondal

**Content Editor** - Jagjeet Uberoi

**Content Writer** - Ritika Singh

**Content Contributors** -
Manish Arora, Tanaz Buhariwala,
Narendra Sen

**Art Director** - Y. Subhashini

**Design** - Goraksh Kokate

**Careers** - careers@et-edge.com

**Subscriptions** - subscriptions@et-edge.com

**Website** - https://etedge-insights.com/

# AI GONE ROGUE
## IS CYBERSECURITY FALLING BEHIND?

Artificial Intelligence has long been hailed as the vanguard of innovation fueling breakthroughs in healthcare, finance, logistics, and education. But in 2025, the same technology is being hijacked by malicious actors. From AI-written phishing campaigns to voice-clone scams and self-mutating malware, cybercrime has entered a dangerous new phase: autonomous, adaptive, and increasingly accessible.

In 2025, AI-enhanced cyber threats have emerged as a dominant concern across global enterprises. According to a May and July 2024 Gartner survey of 345 senior risk executives, AI-powered malicious attacks ranked as the top emerging risk, surpassing geopolitical instability, talent shortages, and misinformation. Gartner further predicts that by 2027, nearly 17% of all cyberattacks will involve generative AI, underscoring how rapidly this technology is being weaponized.

Fortinet's 2025 Global Threat Landscape Report highlights a 16.7% year-over-year surge in automated scanning, with activity reaching an alarming 36,000 scans per second—a strong indicator of AI-driven attack automation. The report also noted a 500% increase in stolen credentials, contributing to a 42% rise in targeted attacks using AI-assisted reconnaissance.

Complementing this, GetApp's 2024 Data Security Report revealed that 37% of U.S. IT leaders identified AI-enhanced threats as their top cybersecurity concern, with 60% citing AI-generated malware as the most pressing challenge. Meanwhile, KnowBe4's Phishing Threat Report documented a 17.3% rise in phishing emails between late 2024 and early 2025, with 82.6% of those attacks leveraging AI in some capacity. Together, these findings paint a stark picture: AI is not just transforming cybersecurity, it's redefining the threat landscape itself.

Prompt injection attacks, once a niche concern, have now become the top security risk for large language model (LLM) apps able to trick chatbots into executing malicious commands without human oversight. And yet many companies remain dangerously underprepared.

As attacks rise in both volume and complexity, we delve deeper into expert perspectives from Dr. Sanjay Katkar, Joint Managing Director of Quick Heal Technologies Limited, and Jaydeep Singh, General Manager for India at Kaspersky, to explore how enterprises can rethink their defense strategies in a world where AI is no longer just a shield but a sword in the hands of attackers. Together, they outline how organizations can prepare for an era where cybercrime is no longer manual but autonomous.

### The AI writes the lure, the payload and the playbook

Dr. Sanjay Katkar doesn't mince words when describing the sophistication of modern attackers.

"We're now seeing what I call self-driving malware. It lands on a host and uses open-source coder LLMs to generate new commands on the fly no operator required. AI now writes the lure, the payload, and, more alarmingly, the entire end-to-end playbook itself."

He notes that attackers are increasingly using models like **WormGPT** and **FraudGPT** to mass-produce personalized spear-phishing campaigns. By feeding them with breach data or scraped LinkedIn profiles, these black-hat LLMs can generate multilingual, flawlessly written lures often accompanied by deepfake voice notes.

### Jaydeep Singh of Kaspersky concurs

"AI is making cyberattacks faster, stealthier, and shockingly personalized. From phishing emails to voice impersonations to malware creation AI tools are being used to mimic human behavior and evade legacy detection systems."

## DR. KATKAR OUTLINES A THREE-PRONGED APPROACH:

1

Regulation – Recent global policy shifts are increasingly holding AI vendors accountable. The EU AI Act, for example, includes provisions for adversarial machine learning defenses and mandates timely incident reporting. Similar regulatory language is beginning to appear in U.S. executive orders and OECD frameworks, signaling a growing consensus on the need for accountability in AI deployment.

2

Enforcement – Targeted sanctions and crackdowns on digital identity fraud are emerging as effective deterrents against AI misuse. Measures such as penalizing those behind AI-enabled ransomware attacks demonstrate that digital offenses can—and should—have real-world consequences.

3

Transparency – Global tools like the OECD’s AI Incident Monitor are fostering a collaborative approach to AI risk. By encouraging organizations to share information about breaches and failures, these platforms aim to prevent repeated mistakes across industries. As one expert notes, “There’s no reason every company should have to learn the same hard lesson in isolation.

### Are enterprises ready?

The short answer? Not quite.

A recent TechRadar study revealed that 78% of CISOs see AI-powered threats as a major concern, yet nearly half admit their organizations are unprepared.

Both Quick Heal and Kaspersky urge companies to stress-test their systems against AI threats, by focusing on three key layers: identity, code, and content.

Dr. Sanjay Katkar emphasizes a layered approach, urging companies to stress-test the key surfaces AI attacks exploit: identity, code, and content. “Red-team simulations that use generative models to craft phishing emails and deepfake calls can reveal weaknesses in awareness programs,” he warns. If your staff still falls for synthetic media, your training is outdated.

A robust evaluation involves mapping the software supply chain against compliance frameworks like the NIST AI Risk Management Framework and the EU AI Act’s “resilience to manipulation” clause. Both demand advanced model hardening and protection against data poisoning.

He underscores the growing importance of AI-driven defense systems that enable Security Operations Centers (SOCs) to detect and respond to anomalies in real time. “Human-speed tickets don’t cut it anymore you need machine-speed reflexes,” Dr. Sanjay Katkar notes, emphasizing the urgency of adapting cybersecurity to match the speed and sophistication of modern threats.

Jaydeep Singh of Kaspersky echoes the urgency. “The first step is assessing whether your security stack already includes AI-enhanced detection, behavioral analytics, and automated response systems.”

Organizations must run frequent, realistic cyber drills and tailor awareness programs to reflect today’s advanced threats. Singh advises leveraging threat intelligence services and APT (Advanced Persistent Threat) simulations to benchmark your real-world readiness.

Importantly, Singh frames readiness as a growth enabler. “Investing in cybersecurity isn’t just about defense it’s a strategic decision. Digital trust underpins modern business, especially in a rapidly digitizing market like India.”

He also stresses the need for leadership training and AI governance awareness. Readiness isn’t complete unless boards understand the risks and regulations tied to AI misuse.

Dr. Sanjay Katkar

Jaydeep Singh

### Dark web dealers are selling AI like Netflix subscriptions

The commoditization of AI has created a new era of cybercrime where skill is no longer a prerequisite. As Dr. Sanjay Katkar describes, “Subscription-based LLMs (large language models) like WormGPT and Grok-powered forks are now sold for as little as $60-200 per month.”

Buyers gain access to phishing prompts, exploit code, and even step-by-step laundering tutorials. “Now, even people who don’t understand tech can buy cyberweapons. All they need is a wallet,” Katkar notes grimly.

He warns of a geographic shift in threat origination. “We’re seeing well-crafted scams from regions that previously struggled with English grammar or localization. AI bridges that gap.”

Jaydeep Singh shares, “We’ve tracked a surge in dark web chatter around AI models used for malicious purposes deepfakes, exploit scripts, even AI APIs offered on a subscription basis.”

This democratization of AI cyber tools has opened the gates to a wider pool of attackers, including low-skill actors who now deploy sophisticated campaigns.

To counter this, Singh urges a proactive defense posture. “Real-time monitoring, digital footprint tracking, and strong AI detection systems are essential. You can’t rely on legacy systems anymore.”

### AI vs. authority: Who governs the machines?

Governments must create clear, enforceable frameworks that define acceptable use of AI. Just as we have laws for nuclear energy or pharmaceuticals, AI especially when deployed in critical sectors like defense, healthcare, or finance requires strict oversight. Both leaders agree regulatory intervention is now essential to tame AI’s misuse in cybercrime.

Jaydeep Singh points to national initiatives like CERT-In’s AI cybersecurity guidelines as proof that local governments are stepping up. Kaspersky fully supports these moves, viewing them as crucial to shoring up both public and private defenses.

He calls for enhanced cross-border intelligence sharing and public-private partnerships. As Singh sees it, regulation is only one piece of the puzzle. “We need oversight, collaboration, and education to truly mitigate AI abuse.”

In India, regulations like the DPDP Act and RBI's cybersecurity guidelines have already begun shifting mindsets. "They've raised awareness and catalyzed investment in intelligence-led security," Singh remarks. Kaspersky is poised to capitalize on this regulatory momentum in the coming years.

### Cybercrime 3.0: AI with a personal touch

Looking ahead, both experts forecast a dystopian reality: autonomous, AI-powered social engineering engines that combine multi-modal deception with real-time adaptation.

Dr. Katkar paints a chilling picturwwe: "Imagine agents that scrape real-time data, mimic your voice and face, draft emails, schedule Zoom calls and if blocked, shift to another medium automatically."

These could integrate with backend exploit frameworks like MalGEN, generating zero-days, creating payloads, and executing personalized attacks within minutes.

"To defend against this," he says, "organizations must implement continuous identity assurance, edge-level deepfake detection, and AI-native security systems."

Jaydeep Singh agrees: "Generative AI will make social engineering hyper-personalized and dynamic." Future threats will adapt to victims in real-time, making them harder to detect and stop.

He anticipates a future where attackers fuse AI with breached personal data to automate reconnaissance and exploitation. This means less time between compromise and consequence.

He adds: "The rise of cybercrime-as-a-service will allow even non-technical attackers to deploy these sophisticated campaigns. The barrier to entry keeps dropping."

For staying ahead requires AI-enhanced detection, continuous threat intelligence, and digital footprint monitoring. "These are no longer optional they're foundational to modern cybersecurity," Singh expressed.

### A call to action for the AI era

The expert insights from Dr. Katkar and Jaydeep Singh reveal one clear truth: cyberattacks are evolving into autonomous, AI-driven threats that bypass legacy defenses with speed, scale, and subtlety. Organizations must adapt quickly or risk falling behind.

### Quick Tips for C-Suite Leaders

☑ Stress-test identity, code, and content layers

☑ Deploy AI-native tools

☑ Integrate continuous employee training with deepfake simulations

☑ Stay compliant with AI governance (NIST, DPDP Act, EU AI Act)

☑ Monitor the dark web using digital footprint intelligence

**To remain secure in this new reality, enterprises should:**

- Deploy AI-powered detection and response tools across their security architecture.
- Conduct red-team exercises using generative AI to stress-test identity, code, and content layers.
- Simulate advanced threats using threat intelligence services.
- Invest in cybersecurity awareness and leadership training aligned with modern risks.
- Stay ahead of compliance through AI governance frameworks like the EU AI Act and NIST guidelines.
- Collaborate with regulators, peers, and vendors to share knowledge and defense strategies.

In an age where even a deepfake voicemail can compromise an entire system, the margin for error is gone. "We must move from reactive to predictive security," says Katkar. "If AI writes the playbook, it's time defenders learn to speak the same language."

Jaydeep Singh concludes with a reminder of what's at stake: "The cost of inaction isn't just data loss it's business credibility, customer trust, and national security."

As the AI arms race intensifies, cybersecurity must evolve just as quickly. Enterprises that embrace AI not just as a threat, but as a core defense mechanism, will be the ones standing tall in 2025 and beyond. ●

***Poonam Mondal,***
*Senior Content Writer, ET Edge Insights*

Sources:
*gartner.com | fortinet.com | getapp.com | knowbe4.com*