July 10, 2026

Listing Compliance, **BSE Limited** P. J. Towers, Dalal Street, Mumbai - 400 001 (Scrip Code: 526881)	Listing Compliance, **National Stock Exchange of India Limited** Exchange Plaza, Bandra Kurla Complex, Bandra (E), Mumbai - 400 051 (Scrip Code: 63MOONS)

Dear Sir/Madam,

Sub: Information update for Q1 (FY 2026-27) received from our Subsidiary – 63SATS Cybertech Ltd.

Pursuant to the applicable regulations of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, we are pleased to attach an Information update for the June 2026 quarter received from our material subsidiary 63SATS Cybertech Ltd., sharing the progress milestone of the company. The 'Limited Review' quarterly results shall be included in the consolidated results to be submitted by 63moons technologies Limited, in full spirit of compliance within the statutory timelines.

We wish to add that our other non-material subsidiaries are at various stages of incubation and progression and that the Company will include and share their limited reviewed results once received from them alongwith the consolidated results of the Company for the Quarter ended June 2026, within the statutory timelines.

You are requested to kindly take the information on your records.

Thanking You,
Yours faithfully,

For 63 moons technologies limited

Hariraj Chouhan
Sr VP & Company Secretary

Encl.: a/a

63 moons technologies limited

Corporate Office: FT Tower, CTS No. 256 & 257, Suren Road, Chakala, Andheri (East), Mumbai - 400 093, India
T: +91-22-6686 8010 | F: +91-22-6686 8050 | E: info@63moons.com | W: www.63moons.com
Registered Office: Shakti Tower-II, 4th floor, Premises-J, 766, Anna Salai, Chennai - 600002.
T: +91 44 4395 0850 | F: +91 44 4395 0899 | CIN No.: L29142TN1988PLC015586

63 SATS™ Cybertech

YOUR OWN CYBERSECURITY FORCE

Q1 INFORMATION UPDATE

FY 2026–27 | Quarter Ended 30 June 2026 | Order-Book & Momentum Update

₹288 Cr
Q1 Order Book
Already achieved 82% of FY27 target

₹53 Cr+
AI CyberOps (Cumulative)
₹13 Cr booked in Q1

2 Mn+
CYBX Downloads
3,25,000+ paid subscribers

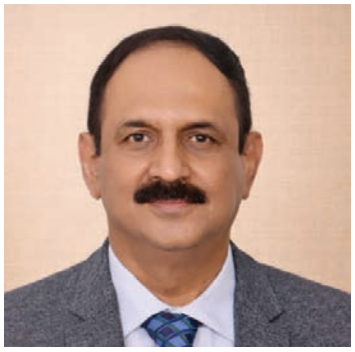
65+
DPDP Clients Onboarded
New compliance engine

CYBX™ for B2C

CYBER SECURITY FORCE™ CSF 63SATS for B2B

CYBERDOME® for B2G

01
CHAIRMAN'S MESSAGE



Lt Gen M. U. Nair (Retd.)
Chairman of the Board
63SATS Cybertech Ltd.
Former National Cyber Security Coordinator (NCSC), Government of India

A quarter into the new financial year, I want to offer a perspective shaped less by celebration and more by observation. In national defence, we learn early to distinguish between activity and readiness. What 63SATS has demonstrated in Q1 FY27 is readiness converting into result.

An order book of ₹288 crore secured in a single quarter is not merely a commercial milestone. It is evidence that the market now recognises 63SATS as a dependable line of defence, and that the demand for cybersecurity in India is real, sustained, and non-discretionary. This is structural, not cyclical.

I note with equal approval the discipline with which this update is presented. The company reports committed order book, not billed revenue, because the year is still

running. In my experience, institutions that are candid about what they have secured, as distinct from what they have earned, are the institutions that endure.

This quarter we have also strengthened the Board with two accomplished leaders, whom I welcome warmly.

Governance is not a formality at scale. It is the mechanism through which ambition is held to account, and it becomes more important, not less, as the company grows.

The task ahead is clear. Demand has been secured. The discipline of delivery, at this new scale and without compromise, will define the remainder of FY27.

The foundation is sound. The direction is deliberate. Execution will now speak for itself.

02
MD & CEO'S MESSAGE

Neehar Pathare
MD, CEO & CIO
63SATS Cybertech Ltd.
Co-Chairman of the Cybersecurity Committee/Task Force at CII

When we closed FY26, I wrote that we were building an institution, not chasing short-term gains. One quarter into FY27, that conviction is being validated faster than we anticipated.

The clearest signal is our order book: ₹288 crore committed in Q1, covering close to 82 percent of our full-year target. But the number I return to most often is a different one. CYBX has now crossed two million downloads and three lakh+ paid subscribers.

That figure matters to me because it represents a belief we have held from the start, that cybersecurity must be democratised. Protection cannot remain a privilege of large enterprises. Every citizen who downloads CYBX is a household brought under institutional-grade protection, often for the first time. Building India's first cybersecurity super app to this scale, and getting people to pay for it, tells us the category is real.

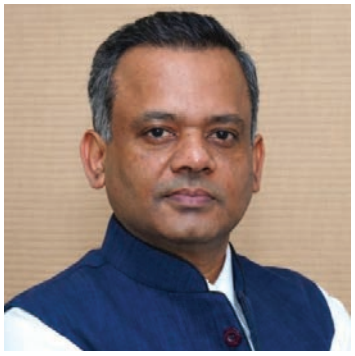
On the enterprise side, our IP engine continues to compound. CYBX AI CyberOps has crossed ₹53 crore in cumulative order value. The shift from a services company to an IP-led institution, which we set out to prove, is now visible in the numbers.

I am also honoured to have been invited to Co-Chair the cybersecurity mandate at the Confederation of Indian Industry. I regard this less as recognition and more as responsibility, to help shape the standards and posture of an industry that now sits at the heart of national resilience.

To our investors, partners, and every member of the 63SATS team: thank you for the belief. The foundation is built. FY27 is where we scale it.

03

JT. MD & JT. CEO'S MESSAGE



Srinivas L
Jt. MD & Jt. CEO
63SATS Cybertech Ltd.

Q1 FY27 has confirmed what FY26 set in motion from ₹3.6 Cr in FY25 to ₹87 Cr in FY26 to ₹288 Cr in FY27. The foundation we built last year is now converting into scale, faster than we planned for.

The clearest proof is the order book. In a single quarter, we have booked ₹288 crore in committed orders. That is more than three times our entire FY26 revenue, and it already covers roughly 82 percent of our full-year FY27 target. This is not pipeline. It is signed demand.

Our IP thesis is holding. CYBX AI CyberOps has crossed ₹53 crore in cumulative order value, ₹13 crore of it added this quarter. This is our IP centric path and is no longer a plan on a slide. It is a compounding revenue line.

I want to be precise about what this update reports. The financial year is running, so we show committed order book and traction, not billed revenue. We would rather show you what is contracted than what is convenient.

Which brings me to the only thing that matters for the rest of FY27. Demand is no longer our constraint.

Delivery is. Converting this order book to revenue, on time and without compromising quality, is now the entire game. It is a harder discipline than selling, and it is exactly the one we have built the team, the certifications, and the alliance leverage to master.

We said FY27 would be the year we scale. Q1 is the proof. Now we execute.

> *We are no longer building capability.*
>
> *We are converting it.*

04

Q1 FY27 SCORECARD

A quarter of committed demand, IP acceleration, and consumer scale.

Metric	Q1 FY27	Context & Trajectory
Q1 Order Book	**₹288 Cr**	Already achieved 82% of the ₹350 Cr FY27 revenue target, secured in one quarter
CYBX DNA AI CyberOps — Cumulative Order Value	**₹53 Cr+**	₹13 Cr booked in Q1; extends the ₹40 Cr FY26 base
CYBX Super App Downloads	**2 Mn+**	Up from 18.87 lakh at FY26 close
CYBX Paid Subscribers	**3,25,000+**	Up from 2.32 lakh at FY26 close
DPDP Clients Onboarded	**65+**	New compliance-led revenue engine, live in Q1
Board Strengthening	**+2 Directors**	Governance and institutional depth expanded
Institutional Recognition	**CII**	Co-Chairmanship of the CII Cybersecurity Committee

The one number that matters

₹288 Cr

Q1 order book equals roughly **3.3x the whole of FY26 revenue (₹87 Cr),** booked in a single quarter, and covers **82% of the FY27 target** before the year is a quarter old. The FY27 question has moved from demand generation to delivery execution. These orders are on a phased wise execution in the same financial year and ₹100 crore out of ₹288 crore is already executed and billed including payment of equivalent GST and other applicable taxes.

05

THE ORDER-BOOK BREAKTHROUGH

₹288 crore of committed order book in Q1 fundamentally de-risks the FY27 plan.

₹288 Cr
Q1 FY27 order book

Already achieved
82%
of FY27 ₹350 Cr target

3.3 X
of full-year FY26 revenue

₹45 Cr
opening order book, 1 Apr 26

Why this changes the FY27 story

- **Demand is no longer the risk.** Entering FY26 we were proving we could capture demand. Entering FY27, approx. 82% of the annual target sits in the order book after one quarter. The strategic question shifts entirely to disciplined, ontime delivery.
- **The three-engine model is compounding**. Order book is being fed simultaneously by CSF enterprise expansion, CyberDome government and critical-infrastructure mandates, and CYBX DNA IP. No single engine carries concentration risk.
- **Alliance leverage is multiplying reach.** The structured OEM channel continues to act as an off-payroll field force, converting pre-established credibility into registered, qualified demand.
- **Order book converts to revenue across the delivery cycle.** Recognition follows deployment and milestones through FY27. Billed revenue will be reported at the full-year close.

Founder-grade transparency. A large order book is an asset only if it is delivered. We have deliberately front-loaded capacity planning, certification density, and delivery leadership so that conversion keeps pace with intake. Delivery execution is our stated priority for the remainder of FY27.

06

CYBX DNA — THE IP ENGINE ACCELERATES

The services-to-IP thesis is not a plan any more. It is a proven, compounding revenue line.

₹53 Cr+

Cumulative order value for **CYBX DNA AI CyberOps,** our AI-powered SOC orchestration platform, with **₹13 crore booked in Q1 FY27** on top of the ₹40 crore FY26 base. Proprietary IP, sold at enterprise scale, at premium margins.

What is driving the acceleration

- **Outcome, not tooling.** CYBX DNA AI CyberOps automates threat detection, incident response, and security operations, reducing SOC team dependency by up to 60%. Enterprises are buying measurable risk reduction, not another console.
- **Land-and-expand is repeatable.** IP now travels alongside CSF advisory and managed services, converting trusted service relationships into high-margin product revenue inside the same accounts.
- **Valuation logic favours IP.** Product revenue commands a structural premium over services. Every rupee that shifts from services to IP re-rates the quality of the overall revenue base.

Product	What it does	Status
CYBX DNA AI CyberOps	AI-powered SOC orchestration and automated response at enterprise scale	**₹53 Cr+ cumulative**
CYBX Super App	Consumer protection against scam calls, phishing, UPI fraud and malicious apps, with embedded cyber insurance	**2 Mn+ downloads / 3.25 L+ paid subscribers**
CYBX Coin	Security-intelligence token driving ecosystem engagement and rewards	**FY27 launch**
IronDroid IP	Privacy-first, hardened mobile ecosystem for B2B and B2C	**In progress**

07

CYBX DNA — CONSUMER SCALE

India's first cybersecurity super app has crossed the two-million mark, and the subscriber base is scaling with it.

2 Mn+
total downloads

3,25,000+
Paid subscribers

₹10 L
cyber insurance cover / user

18.87 L -> 20 L+
Downloads: FY26 close -> Q1 FY27

2.32 L -> 3.25 L+
Paid Subscribers: FY26 close -> Q1 FY27

Momentum, and the levers still to fire

- **Organic proof before paid scale.** Growth to two million has been achieved largely organically. The paid acceleration layer, through the Publicis partnership entering in FY27, is still ahead of us.
- **Subscriber conversion is holding.** A 3.25+ lakh paying base on a 2 million+ install base validates genuine willingness to pay for consumer cybersecurity, a category most of the market still gives away free.
- **CYBX Coin as an engagement engine.** The FY27 launch of CYBX Coin introduces a gamified rewards layer designed to drive both downloads and retention.
- **Accessible by design.** Availability across multiple Indian languages keeps CYBX aligned to a mass-market, trustfirst philosophy rather than a metro-only premium play.

08

DPDP — EARLY MOVER IN A MANDATED MARKET

As India's Digital Personal Data Protection regime moves toward enforcement, 63SATS has already converted the mandate into clients.

65+
DPDP clients onboarded in Q1

₹250 Cr
penalty exposure per violation

₹100 Cr
FY27 focus-area GTM target

Why this is a structural, non-discretionary spend

- **Compliance is now law, not choice.** With penalties stacking up to ₹250 crore per violation, DPDP readiness has moved from a nice-to-have to a board-level obligation for every data-handling enterprise in India.
- **We are positioned ahead of the deadline.** Our DPDP GTM, built on signed OEM alliances and an AI cyber overlay, gives clients an execution partner rather than another advisory report. 63SATS builds & runs the compliance posture; it does not merely recommend one.
- **Twenty logos in one quarter is a defensible head start.** Early reference clients across regulated verticals create the credibility flywheel that compounds through the enforcement window.

We have onboarded more than 65 customers for DPDPA compliance. Partial list of some of them are:

paisabazaar.com · Joyalukkas World's favourite jeweller · ZEELEARN · FANUC INDIA · NLC INDIA · Kaleesuwari · PURAVANKARA · PON PURE CHEMICALS · Albertsons Companies · CRYSTAL · MES CENTRAL SCHOOL · Bonanza make money. not mistakes. · Vadilal INDUSTRIES LTD. · HARRISONS MALAYALAM LIMITED · IKS HEALTH · EQUIFAX · GUJARAT AMBUJA EXPORTS LIMITED NURTURING BRANDS · Shalina Healthcare · MF Utilities · Pitambari INNOVATIVE PRODUCTS · V-TRANS Driving Excellence · ASIRVAD · KITEX lifestyle · gtn SINCE 1966 · and counting...

09

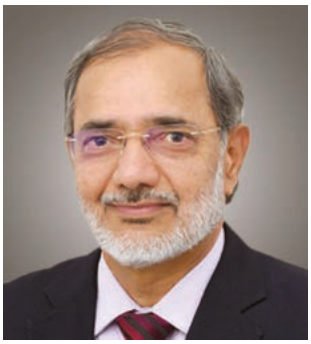
STRENGTHENING THE BOARD

Governance depth is scaling alongside the business. Two accomplished leaders joined the 63SATS Board in Q1 FY27.

Ms. Shruti Shah

Board Member

- Independent Director – Indian Institute of Corporate Affairs
- Board Member – ACC, Balkrishna & Kalyani Group
- Partner – Pravin P. Shah & Co.
- Director – Health & Education Foundation



Mr. Chandrasekhar Kanekal

Board Member

- Independent Director – 63 Moons Technologies Ltd.
- Independent Director – TruAlt Bioenergy Ltd.
- Former Director – TransUnion CIBIL & NABARD
- Former General Manager – Union Bank of India

Why it matters

Each addition extends the institutional weight already anchored by Lt Gen M. U. Nair (Retd.), Neehar Pathare, and the wider Board and Advisory Board. As the order book scales past ₹288 crore, board-level governance, risk oversight, and network reach become force multipliers for disciplined execution.

10 INSTITUTIONAL RECOGNITION

63SATS is increasingly recognised not as a vendor in the market, but as a voice shaping national cybersecurity policy.

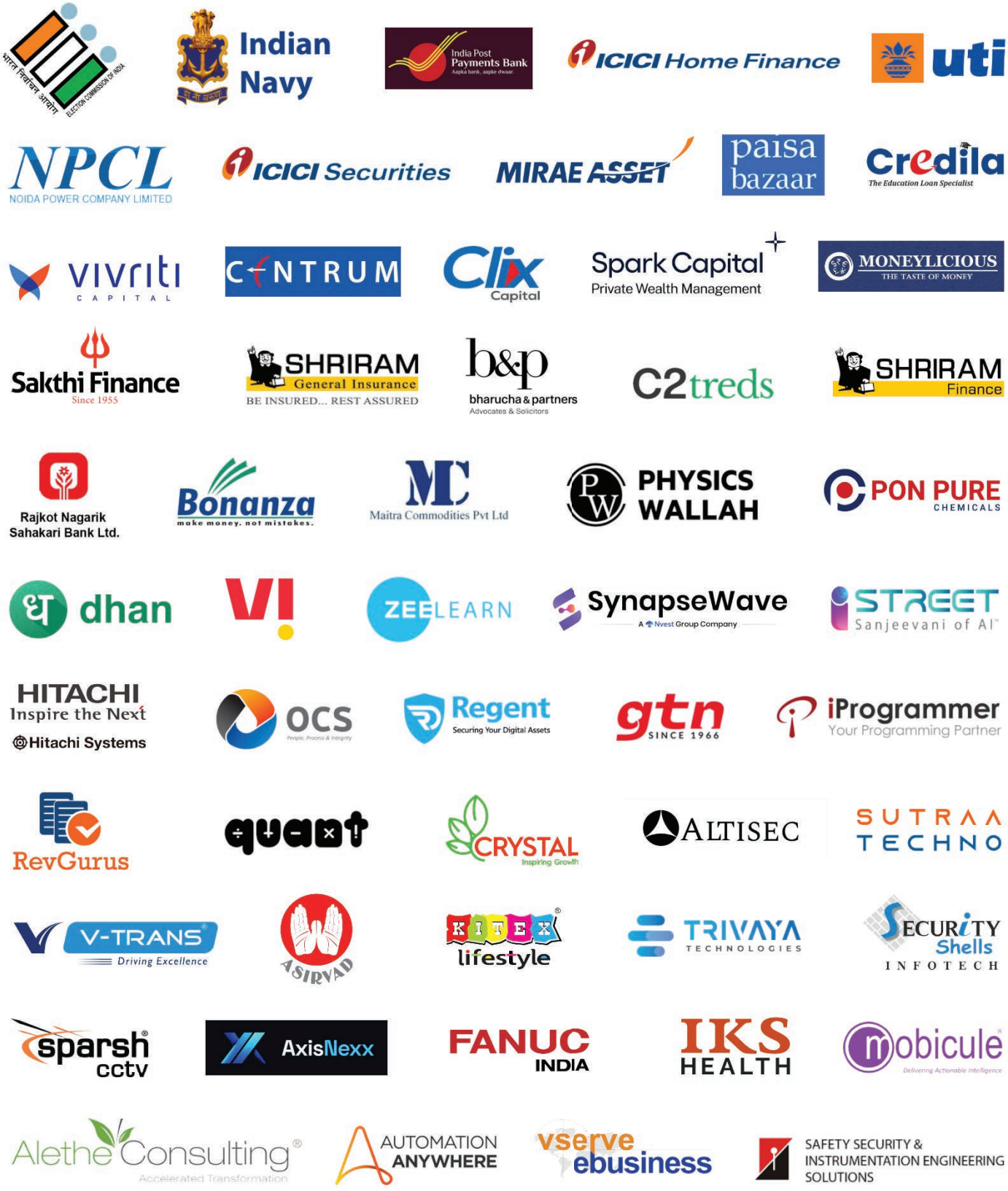
Neehar Pathare, MD, CEO & CIO of 63SATS, has been appointed **Co-Chairman of the Cybersecurity Task Force at the Confederation of Indian Industry (CII),** one of India's most influential industry bodies.

What this signals to investors

- **A seat at the policy table.** Co-chairing a CII cybersecurity mandate places 63SATS inside the conversations that shape industry standards, regulatory posture, and national priorities, rather than reacting to them after the fact.
- **Credibility that compounds into pipeline.** This kind of institutional standing is the trust infrastructure that converts, over time, into enterprise and government mandates. It is the clearest external validation that 63SATS is viewed as a serious, credible, India-first cybersecurity institution.
- **Consistent with our positioning.** It reinforces the sovereignty-led narrative that runs through everything we build: Secured by Design, Sovereign by Default.

11

PARTIAL LIST OF OUR VALUED CUSTOMERS



indus TOWERS
KALYANI | BHARAT FORGE
BAJEL Projects
adani Ports and Logistics
TMEIC We drive industry
Noida International Airport
GFL GUJARAT FLUOROCHEMICALS
APRAAVA ENERGY
LOGUS INTERNATIONAL FZE
PRECISE ALLOYS PVT. LTD.
SWAN
HIKAL
PSA MUMBAI
AEQUS ecosystems of efficiency
EXIDE ENERGY
AVAADA
TWIN Engineers Pvt. Ltd.
SheelaFoam
The Great Eastern Shipping Co. Ltd.
THE TIMES GROUP
TATA CLiQ
UFO CINE MEDIA NETWORK
EMAAR
SMARTWORKS
Berger Paint your imagination
THE TIMES OF INDIA
Raymond
ASHOK GOEL TRUST
ANAND RATHI INVESTMENT SERVICES
TATA
Radhakrishna Foodland The Supply Chain Solutions Specialist
marico
SLK AMIN HOLDINGS
CRC GROUP
GenesisLabs LABORATORY OF CHOICE
paisabazaar.com
Joyalukkas World's favourite jeweller
Kaleesuwari
PURAVANKARA
Vadilal INDUSTRIES LTD.
MES CENTRAL SCHOOL
GUJARAT AMBUJA EXPORTS LIMITED NURTURING BRANDS
Livlong 365
Shalina Healthcare
MFU MF Utilities
LUPIN
HARRISONS MALAYALAM LIMITED
SURYA Hospitals
GKNM HOSPITAL We care. And it shows...
INDIRA IVF FERTILITY & IVF CENTRE
Albertsons Companies
EQUIFAX
NLC INDIA
Pitambari INNOVATIVE PRODUCTS
and counting...

12

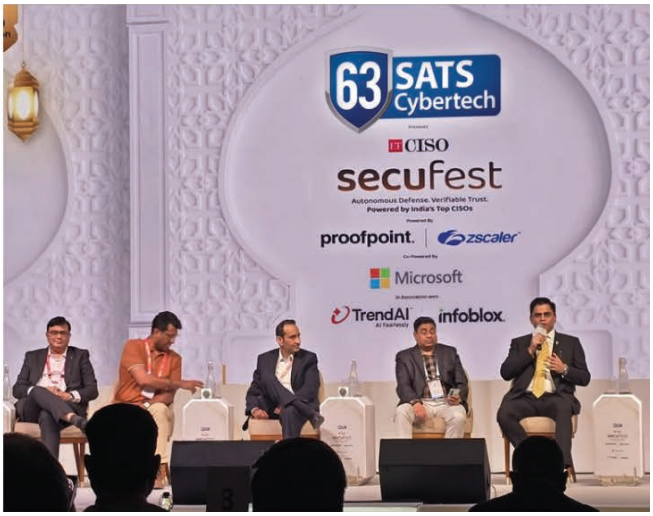
63SATS IN THE MARKET

Mindshare first, market share next. Q1 saw 63SATS build visible brand presence across events, advertising, and out-of-home media.

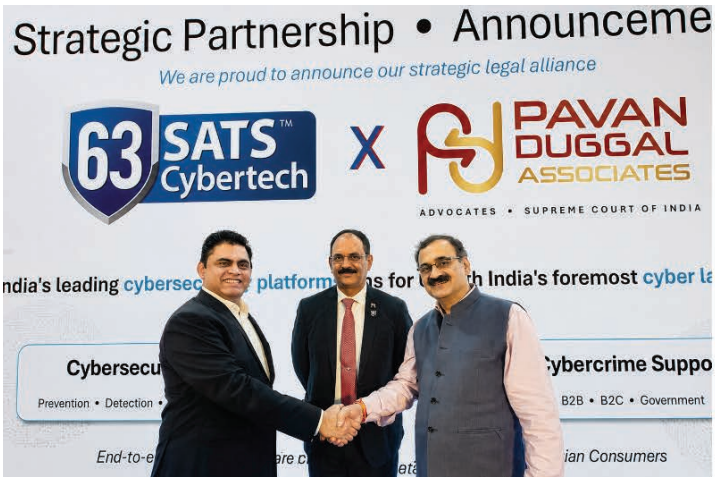
Events & thought leadership

Through Q1, 63SATS leadership carried the company's point of view into the rooms that matter, from industry forums to CISO and boardroom platforms, reinforcing our position as an outcome-driven, India-first cybersecurity institution. Each appearance is analytically led and non-promotional by design, building authority rather than pushing product.

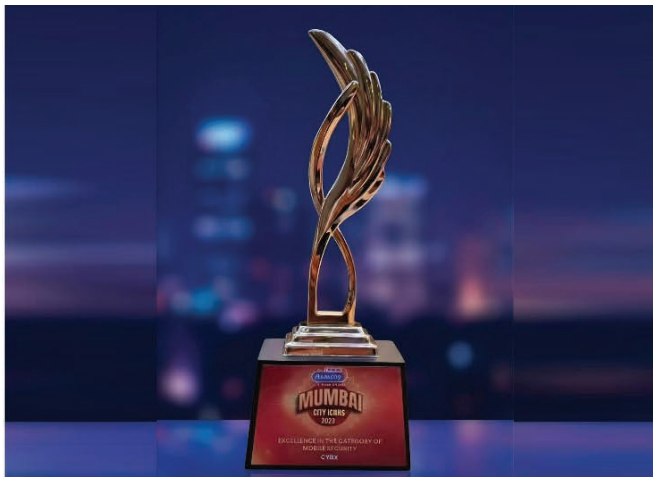
Protecting Digital India: 63SATS Cybertech participated as the Title Partner at CII's 'Cybersecurity 360° Summit' alongside top government and defence leaders in New Delhi on July 3, 2026.



Leading From The Front: 63SATS Cybertech took the centre-stage as the Presenting Partner at the 'ET CISO SecuFest' which was held in Lucknow in March 2026 to showcase its cutting-edge expertise directly to top CISOs.



Strengthening Digital Defences: 63SATS Cybertech cemented its cybersecurity leadership by formalising a strategic tie-up with legal expert Dr. Pavan Duggal (right) at 'CyberSec India Expo 2026' in Mumbai on April 23.



Gold Standard For Mobile Defence: 63SATS Cybersecurity demonstrated its elite cybersecurity expertise as the revolutionary CYBX super-app bagged the Radio City Mumbai City Icons Award for 'Excellence in Mobile Security'.

63SATS IN THE NEWS

THE ECONOMIC TIMES
Special Report – June 30, 2026

'Be Indian, Buy Indian' and build the digital trust that holds it all together

Defending Digital Economy Indigenously: 63SATS Cybertech's 'Cyberdome' and 'CyberSecurity Force' shield national infrastructure with purpose-built AI defence and robust DPDP Act compliance

> In a digital economy, trust is not a sentiment. It is infrastructure. And like any infrastructure, it can be indigenous or imported, sovereign or dependent... if "Buy Indian" is to mean anything in the digital age, it must extend to the security that protects the very things we are so proud to have built at home
>
> - Neehar Pathare | MD, CEO & CIO of 63SATS Cybertech

"Be Indian, Buy Indian" has powered a remarkable national project. We have learned to make our own goods, build our own digital rails, and increasingly write our own software and train our own AI. The campaign has always been about more than economics; it is about self-reliance, confidence, and the conviction that a nation should own the systems on which its future runs.

But there is a dimension of self-reliance that rarely makes the headlines, and it is the one that decides whether everything else holds. A country can manufacture its own products, host its own data, and deploy its own AI and still be undone if the trust beneath all of it is borrowed, brittle, or controlled from elsewhere. In a digital economy, trust is not a sentiment. It is infrastructure. And like any infrastructure, it can be indigenous or imported, sovereign or dependent.

This is the conviction on which 63SATS Cybertech is building its products and offerings. While many fine Indian companies are building the nation's digital and AI economy, the mandate of 63SATS Cybertech is to safeguard it and to be the strategic trust layer on which national resilience rests. "We are an operator, not an advisor". 63SATS Cybertech builds and runs sovereign, India-first defence systems for enterprises, governments, and citizens. If "Buy Indian" is to mean anything in the digital age, it must extend to the security that protects the very things we are so proud to have built at home.

TRUST IS THE NEW "MADE IN INDIA"

For decades, "Made in India" was a statement about products you could hold: like a car, a phone, a vaccine. The next chapter is about something you cannot hold but cannot live without: The assurance that your data is safe, your identity is yours, your transactions are real, and the AI making decisions on your behalf has not been tampered with. That assurance is digital trust, and it is fast becoming the most valuable thing a nation can produce for itself.

Here lies a quiet strategic risk. A great deal of the security stack that Indian organisations rely on is designed, owned, and operated from outside the country. Threat intelligence, detection logic, and even the keys to critical systems can sit on foreign soil and under foreign jurisdiction. In ordinary times this is merely a dependency. In a crisis, be it geopolitical, regulatory, or adversarial, it becomes a vulnerability. A foreign vendor can be subpoenaed by its own government, cut off by a sanctions regime, or simply deprioritise a market far from its headquarters. The data that defines an Indian citizen, the model that runs an Indian bank, the alert that should have stopped an attack on Indian infrastructure – none of these can be hostage to decisions made elsewhere. Sovereign digital trust means the ability to defend ourselves with capability we control, on our own terms, aligned to our own laws such as the Digital Personal Data Protection (DPDP) Act and the directions of CERT-In, SEBI and RBI.

SAFEGUARDING THE AI ECONOMY INDIA IS RACING TO BUILD

India is adopting AI faster than almost any major economy, and with it comes an entirely new class of asset to protect. When an organisation deploys an AI model, it is not adding another application. It is introducing something that thinks, learns and responds, with attack surfaces no firewall or antivirus was built to defend. There is no signature for a poisoned dataset, no patch for a prompt injection. If AI is becoming critical national infrastructure, it deserves an Indian defence capability built specifically for it.

That is the purpose of 63SATS CYBX DNA – AI Cyberops Division, a dedicated research and operations capability focused on protecting AI systems themselves. Its mandate spans model assurance, adversarial validation, AI-supply-chain integrity, and sovereign defence-grade research, organised across six pillars covering offensive AI security, AI asset management, secure AI development, autonomous defence, threat intelligence, and AI governance. It is, quite deliberately, Indian capability for an Indian AI economy so that the intelligence we build at home is also defended at home.

DEFENDING THE ENTERPRISES THAT POWER THE ECONOMY

The institutions at the heart of Indian growth, namely banks, capital markets, insurers, manufacturers, can no longer be defended with annual tests and perimeter tools while their attackers operate in AI time. They need continuous, expert-run defence, and they need it from partners who understand Indian regulation from the inside.

The enterprise practice, 63SATS CSF (CyberSecurity Force), is built for exactly this. Instead of point-in-time assessments, it runs continuous red-teaming and managed detection and response, now re-architected to ingest AI telemetry with model inputs, outputs and agent actions alongside conventional logs. Its advisory and vCISO (virtual Chief Information Security Officer) teams run DPDP-aligned AI usage audits that surface "shadow AI", the unsanctioned tools quietly handling sensitive data inside most organisations, and put governance around them. Because this capability is built and staffed in India, the institutions it defends are never waiting on a support desk in another time zone while an attack unfolds in real time. For boards answering to SEBI's CSCRF (Cybersecurity and Cyber Resilience Framework) and RBI's IT directions, this is the difference between knowing your posture and assuming it.

> While many fine Indian companies are building the nation's digital and AI economy, our mandate is to safeguard it...As we celebrate the Indian brands building our digital and AI future, we must decide whether the trust that protects them will also be Indian or quietly outsourced
>
> - Srinivas L. | Joint MD & Joint CEO of 63SATS Cybertech

SOVEREIGN DEFENCE FOR THE GOVERNMENT THAT GOVERNS IT

Nowhere is the case for indigenous trust stronger than in government. Ministries, state digital infrastructure and critical sectors cannot have their monitoring, data or defensive keys sitting under another country's control. Sovereignty here is not a preference; it is a precondition of national security.

This is the mandate of CyberDome, 63SATS Cybertech's government-facing practice, which invests in sovereign-grade monitoring for ministries, state systems and critical-sector deployments where data residency, indigenous control and CERT-In alignment are non-negotiable. It is "Buy Indian" in its most consequential form: The systems that protect the nation's digital backbone, designed and run within the nation.

PROTECTING THE CITIZEN, WHO IS THE REAL ECONOMY

A digital economy is ultimately its people. India's largest attack surface is not its servers but its citizens who are being targeted by deepfake-driven fraud, AI-generated scam calls and identity theft that scale faster than any regulation can. A campaign to buy Indian means little if the Indian buyer is being defrauded at the point of every transaction.

This is the gap 63SATS Cybertech's consumer business, CYBX, was built to close. An Indian cybersecurity super-app that has already crossed a million downloads, bringing scam detection, secure calling and embedded cyber insurance directly to citizens and small businesses. It is protection designed for Indian threats, Indian languages and Indian payment habits, not a foreign product retrofitted to our context. The company's upcoming CYBX Digital Identity is a blockchain-anchored, self-sovereign identity capability that will let Indians prove who they are without surrendering control of their data to any intermediary, domestic or foreign. It is self-reliance applied to the most personal asset of all, one's own identity, the truest expression of "Be Indian" in a digital age.

THE TRUST LAYER IS A NATIONAL CHOICE

India has a rare advantage in this moment. We are as once one of the world's largest consumers of AI and one of its largest producers of cybersecurity talent. Our regulators SEBI, RBI, CERT-In, MeitY are engaged earlier than most of their global peers. Our digital public infrastructure has already shown the world that sovereign, scaled, secure systems are not just possible but world-leading. The talent, the intent and the proof points are all here.

What remains is a choice. As we celebrate the Indian brands building our digital and AI future, we must decide whether the trust that protects them will also be Indian or quietly outsourced. For 63SATS Cybertech, the answer is settled. The company is building that trust layer across the enterprise, government and citizen, and running it as infrastructure: sovereign, accountable and continuously tested. "Be Indian, Buy Indian" should not stop at what we make. It should extend to who we trust to defend it. The digital economy will be safeguarded by what is deployed at home, not by what is debased abroad.

FINANCIAL EXPRESS
Read to Lead
June 15, 2026

CURBS ON FRONTIER AI MODELS PUSH FOR INDIGENOUS COMPUTE

Restrictions on Anthropic revive sovereign AI debate

POULOMI CHATTERJEE
Bengaluru, June 14

ANTHROPIC'S DECISION TO disable access to its Fable 5 and Mythos 5 AI models for foreign nationals following a US export control directive has reignited concerns over India's dependence on foreign AI systems and sharpened calls for greater technological self-reliance.

The move, announced on Saturday, has raised questions about the risks of relying on AI capabilities controlled by overseas companies and governments at a time when businesses and public institutions are increasingly integrating advanced AI tools into critical operations. Earlier this month, a select group of Indian entities and government agencies had received early access to Anthropic's Mythos model, which was being evaluated for cybersecurity and software security applications.

Industry executives and policy experts said the development underscores a broader challenge facing India as AI becomes an increasingly important layer of digital infrastructure. "The sudden, unilateral withdrawal of Fable 5 and Mythos 5 by the US government creates an immediate and dangerous asymmetry of defence," Neehar Pathare, managing director and CEO of 63SATS Cybertech, told *FE*. The decision highlights the risks of depending on external providers for capabilities that may become essential for securing financial systems, digital infrastructure and critical services, he added.

The episode has also revived the debate around sovereign AI, or a country's ability to develop, deploy and govern critical AI technologies without excessive dependence on foreign providers. "If the most significant tech differentiator you are leveraging has external controlloops, then you have to accept you are vulnerable," Pratyush Kumar, co-founder and CEO of Sarvam AI, said in a post on X, adding that countries must increasingly be able to shape their own technological destinies.

Experts said that sovereign AI should not be viewed as a technological isolation but as the ability to retain strategic autonomy over critical technologies. "It is imperative that India works towards a long-term goal of sovereign AI," Kazim Rizvi, founder of technology policy think tank The Dialogue, said. According to Rizvi, investments in indigenous compute capacity, frontier research and a stronger domestic innovation ecosystem are essential to ensure that India can make independent choices regarding the development and deployment of AI systems.

The government has in recent months stepped up efforts to build domestic AI infrastructure under the IndiaAI Mission, including the creation of a national compute ecosystem and support for indigenous model development. Industry experts said such initiatives are necessary first steps but added that significant gaps remain in funding and computing resources.

"Building a Fable-class model is a compute and funding game," Paras Chopra, founder of AI research lab Lossfunk, said in a LinkedIn post. While leading global AI labs are estimated to have access to hundreds of thousands, and in some cases over a million advanced graphics processing units (GPU), India's compute base remains considerably smaller. Experts said that bridging this gap would require investments running into tens of billions of dollars and sustained policy support over several years.

TECH CONTROL

- Anthropic restricts foreign nationals from accessing Fable 5, Mythos 5 under US export control directive
- Decision triggers concern over India dependence on overseas artificial intelligence infrastructure stack

- Select Indian government, enterprise users had early limited exposure for cybersecurity evaluation purposes
- Executives flag abrupt model withdrawal risk creating strategic asymmetry in digital defence architecture
- Experts call for deeper investment in indigenous compute capacity and frontier research ecosystems

Business Standard
June 19, 2026

YOUR MONEY

Don't let dark patterns inflate your online bills

KARTHIK JEROME

Indian consumers are losing an estimated ₹25,000-28,000 crore annually to deceptive interface designs, commonly known as dark patterns, across online marketplaces, according to the *Dark Patterns in India's Online Marketplaces* report, released by market research firm Datum Intelligence.

The Reserve Bank of India (RBI) also recently flagged the issue of dark patterns, directing banks and their agents not to use digital interfaces that trick customers into taking actions they did not intend.

What are dark patterns?

Dark patterns are deceptive user interface (UI) and user experience (UX) design techniques. "They exploit human psychology, cognitive biases, urgency, confusion, or lack of attention to increase revenue for digital platforms at the expense of consumer choice and transparency," says Prashant Mali, cybercrime lawyer, Bombay High Court.

"Dark patterns subvert or impair consumer autonomy, decision-making or choice," adds Dhruv Kaushal, partner, King Stubb & Kasiva, Advocates and Attorneys, The Central Consumer Protection Authority's (CCPA) 2023 guidelines identified 13 kinds of dark patterns.

Drip pricing and forced add-ons

The customer sees an attractive low base price at the start of the purchase journey. "A number of fees — convenience, platform, insurance and handling charges — are added at the checkout stage," says Neehar Pathare, managing director, chief executive officer and chief investment officer, 63SATS Cybertech.

On reaching the payment screen, customers realise that the item costs more than advertised. Many continue with the transaction. "They become less willing to abandon the purchase after they have invested time and effort," says Pathare.

Forced add-ons include insurance, warranties, meaningless subscriptions, and charity donations that are pre-ticked. "Platforms rely on consumers not scrolling down and unchecking these add-ons," says Rohit Saksaria, co-founder, Arbi Mediatech.

False urgency and subscription traps

False urgency creates time pressure or artificial scarcity through the use of fake countdown timers that reset, or claims of low stock that remain unchanged for months. "Fake urgency triggers a panic and fear of missing out and tricks consumers to make impulse purchases," says Pathare.

Subscription traps rely on inertia and obfuscation to keep charging customers quietly. Customers are asked to enter their payment details while joining a free trial. Many forget to opt out before the trial ends. Auto-renewal charges them for the next period without requiring explicit confirmation.

Check final payable amount

To guard against drip pricing, compare the final payable amount, not the advertised price. "Proceed to the payment page before making a purchase decision," says Mali. Saksaria urges customers to check the price breakup before paying.

Scan for pre-checked boxes on reaching the checkout screen. "Assume that pre-selected items are not for your benefit and uncheck them first," says Saksaria.

When you see a countdown timer or low stock warning, pause and step away for five to 10 minutes. Check a competitor's site to test urgency claims. To protect yourself against a subscription trap, mark the date when the trial ends and opt out before that date.

"Revoke unused recurring mandates in your banking or Unified Payments Interface (UPI) apps regularly," says Pathare.

"Check comments posted by other customers about the seller and his products," says Anurag Kashyap, partner, EY Forensic and Integrity Services.

Sundry charges you may be saddled with

- Convenience fees were originally introduced to recover online booking system costs but have become a significant revenue source for many platforms
- Platform fees are charges imposed simply for using the marketplace
- They may be charged regardless of order size
- Handling fees are charged on top of delivery fees for handling the order
- They are vague by design

Preserve evidence

If you observe dark patterns, gather evidence. "Preserve screenshots, screen recordings, purchase receipts, emails, notification trails and bank or payment statements," says Piyush Agarwal, partner, AQUILAW. Screenshots and screen recordings should ideally be time-stamped.

Use available recourse

Report platforms that violate dark pattern rules. The CCPA receives complaints submitted through the National Consumer Helpline (1915). "Consumers can also approach the CCPA through the 2ncrtl.portal," says Agrawal.

Kaushal informs that a customer may file a complaint before the relevant District, State or National Consumer Disputes Redressal Commission, depending on the quantum of claim.

THE TIMES OF INDIA
June 14, 2026

US 'export ban' on Anthropic models may weaken cyber defense: Experts

Aabhas Sharma & Manash Gohain | TNN

File pic

New Delhi: Just over a day after Anthropic hailed India as its "second-largest market" and unveiled a partnership with Tata Consultancy Services (TCS), Indian developers, enterprises and researchers found themselves locked out of the company's most powerful artificial-intelligence tier — Claude Fable 5 and Claude Mythos 5 — following a US govt export-control order.

The two use the same underlying model and are distinguished only by their safeguards: Fable 5 is the safeguarded version released to the public, while Mythos 5, with the restrictions lifted, had been reserved for a small group of vetted partners.

Cybersecurity experts warn that the US govt move could undermine defensive security efforts, even as they accelerate calls for sovereign AI capabilities.

In a statement on Saturday, Anthropic said the US govt, citing national security authorities, had ordered the company to suspend access to Fable 5 and Mythos 5 for all foreign nationals, both inside and outside the US. The company said it was working to restore access and that it believed the move stemmed from a misunderstanding.

The decision has quickly become a flashpoint in the broader debate over whether frontier AI models should be treated as strategic technologies subject to export controls, similar to advanced semiconductors and other dual-use technologies.

Jaspreet Bindra, co-founder and CEO of AI & Beyond, said, "In cybersecurity, the same model can be both a weapon and a shield." While restrictions could reduce offensive cyber risks, particularly from less sophisticated actors, he cautioned that a blanket ban could also weaken legitimate defenders. "The question is who gets access, under what controls and with what auditability."

STRATEGIC TECHNOLOGY?

Neehar Pathare, managing director, and chief information officer of 63SATS Cybertech, was more critical, describing the move as a "geopolitical seizure" rather than a security safeguard. Pathare argued that cybercriminals are unlikely to depend on commercial AI services like Claude and can instead turn to open-source or locally hosted alternatives.

The issue comes at a time when AI models are increasingly being used to automate vulnerability discovery, software testing and security analysis. Pathare cited Anthropic's earlier claims that advanced cyber-capable models could accelerate vulnerability research, helping security teams identify weaknesses before they are exploited.

The development echoes a warning issued just weeks ago in JPMorganChase Center for Geopolitics's report, Beyond the Benchmarks: A Systemic View of US-China AI Competition, which argued that AI has become "the whole ballgame" geopolitically and identified Anthropic's Mythos as a model whose significance extends beyond technology into national security. On Friday, that reading turned to reality.

For India, which is rapidly positioning itself as a major AI market and innovation hub, the episode raises difficult questions. The country has the talent, the demand and increasingly the investment. Yet the sudden loss of access to Anthropic's most advanced models shows participation in the AI revolution may also be shaped by strategic competition.

businessline.
April 15, 2026

63 moons' cybersecurity arm pilots GPS-spoofing solution at Indian airports

Our Bureau
Mumbai

Srinivas L, Joint MD & CEO of 63SATS Cybertech

63SATS Cybertech, the cybersecurity business unit of 63 moons Technologies, is collaborating with two airports to develop a solution to combat GPS-spoofing, a major threat to the aviation industry, a top official in the cybersecurity firm said.

"We have a solution from Israel that we are actively piloting with two airports in India," Srinivas L, Joint MD & CEO of 63SATS Cybertech, told *businessline*, adding that Noida International Airport is among its customers.

SIGNAL SPOOFING

Srinivas explained that GPS spoofing works by transmitting a fake ground-based GPS signal that is stronger than those sent by satellites.

Aircraft normally rely on weak signals from satellites thousands of kilometres away, but when a stronger, false signal is broadcast, the their systems can pick that up instead.

As a result, the aircraft may interpret its position incorrectly, believing that it is in a different location than its actual one. This could also mislead air traffic control, which may see the aircraft positioned somewhere it is not.

Last December, GPS spoofing was detected at major airports, including Delhi, Mumbai and Bengaluru.

The proliferation of connected devices, particularly in homes, and increasing threats because of that had prompted 63SATS to develop solutions under its CYBX brand, its superapp.

"It is about convenience versus security. That's the toughest piece to solve," said Srinivas. "So, in the next two to three years, you will see a lot of IPs coming out of our stable," he added.

The company has rolled out an upgraded version of CYBX, positioning it as an all-in-one solution. The new version integrates multiple security layers, ranging from encrypted calling and Wi-Fi protection to defence against over 100 attack vectors.

Srinivas said the app was seeing good traction, clocking 700,000 downloads and blocking nearly 1.4 million cyberattacks within a month of its launch in August 2025.

Beyond retail users, 63SATS operates across enterprise and government segments through its Cyber Security Force and Cyberdome platforms.

The company is also working with several State government bodies for securing the energy infrastructure network and providing AI cybersecurity, said Srinivas, adding that talks were on with the governments of Gujarat, Uttar Pradesh, Haryana and Tamil Nadu.

"Now, we are focusing on the energy sector and the telecom sector, specialising in operational technology security," he added.

In its enterprise business 63SATS has tied up with top global brands such as Palo Alto, Check Point and Fortinet for providing cybersecurity solutions to sectors such as BFSI, manufacturing, automotive and critical infrastructure.

63SATS IN THE NEWS

THE ECONOMIC TIMES

June 14, 2026

GLASSWING MELTS

US Govt Suspends Early Access to Fable 5, Mythos 5 within Days of Rollout

Tanya Pandey & Subhayan Chakraborty

New Delhi: India's access to one of the world's most advanced artificial intelligence (AI) models appears to have lasted barely a few days.

After Anthropic expanded access to its closely guarded Claude Mythos system to a handful of Indian organisations, a US government directive led the company to suspend local access to Mythos 5 and Fable 5. This raises questions about whether frontier AI models are becoming geopolitical assets similar to advanced semiconductors that remain the exclusive preserve of a chosen few.

The Centre, an official told **ET**, would continue to engage with both Anthropic and Washington to understand the scope of the restrictions and whether they are limited to Mythos 5 and Fable 5 or could extend to other models in the Mythos family.

"It's to be seen if the latest directive is only for Mythos 5 and Fable 5, or will it also impact the other models in the Mythos class, going forward. We hope that's not the case," said the official cited above.

Cybersecurity experts say concerns around Fable 5 are more about speed and scale of its operations

The significance of this suspension lies in how Anthropic rolled out the models. Mythos 5, among the company's most advanced AI systems, was initially kept restricted and made available only to a small group of researchers, cybersecurity experts and trusted partners because of its powerful cyber and reasoning capabilities.

Through Project Glasswing cybersecurity initiative, Anthropic gradually expanded access to select organisations. It then launched Fable 5, a more widely accessible version, just a few days ago.

Now access to both these models has been suspended following the US directive.

The development is particularly significant for India. Several organisations across cybersecurity, telecom, finance and banking had secured early access to Mythos under Project Glasswing, ET reported last week. While the number of such entities was in the single digits, officials described it as a key win in India's engagement on technology policy. Indian Computer Emergency Response Team (CERT-In) and other public sector entities were expected to receive access.

Need for Framework ▸▸ 7

"Fable 5 introduced long-horizon autonomy and proactive self-verification. When an AI can compress months of human penetration testing into a matter of hours, the sheer velocity of vulnerability discovery alters the risk landscape," said Neehar Pathare, chief executive of 63SATS Cybertech, a cybersecurity company.

However, Pathare cautioned that restricting access may not be enough to contain such capabilities. "The belief that a centralised government directive can permanently restrict access to advanced AI capabilities is a regulatory fantasy," he said, highlighting the rapid progress of open-source models.

Business Standard

May 11, 2026

Banking buckles up to meet Mythos threat

Industry races to upgrade infrastructure as advanced AI model poses risks to cybersecurity, report **Avik Das & Subrata Panda**

"It [current cybersecurity technology] was designed for a world where the attacker also needed time. That world no longer exists. When Mythos can identify and chain a working exploit in hours, a 90-day patch SLA is not a risk management posture — it is an open invitation," Pankit Desai, cofounder and CEO of cybersecurity firm Sequretek, wrote in a LinkedIn post, referring to a contractual agreement for identifying and fixing vulnerabilities in software within 90 days of discovery.

Srinivas L, joint MD and joint CEO of cybersecurity solutions company 63Sats Cybertech, said that many banks in India still run on the old COBOL programming language, which makes them vulnerable to threats from Mythos. India will be a primary target of AI-powered cyberattacks, considering the volume of business that takes place in the country.

"The fear is coming with respect to all the enterprises because we were always skill-gated. Now, the attacks have become commodity. Before Mythos, if you had to exploit a very serious vulnerability, you really needed a lot of deep real technical skills. But then with this, you just have a small simple prompt-like offering and you are able to launch right from reconnaissance to finding a vulnerability and exploiting it. When this kind of democratisation of capability happens, that is with nation-state proxies or criminal enterprises, it becomes concerning," said Srinivas.

How can Indian banks build resilience in this new era? As AI reshapes cybersecurity, the question for the authorities is whether the financial system can withstand such severe stress. The outlook is sobering: most Indian institutions lack access to Mythos even for defensive testing in a sandbox environment.

THE ECONOMIC TIMES

BATTLE OF INTELLIGENT MACHINES

Greeshma.Giri
@timesofindia.com

Artificial Intelligence is now embedded across digital infrastructure. It powers fraud detection, automates network monitoring, optimises logistics and even writes code. As organisations depend more heavily on AI to run critical systems, cyber threat is evolving with equal speed. With both attackers and defenders using machine intelligence, the contest has become faster, more autonomous and far more adaptive.

STRUCTURAL SHIFT

For decades, cyber-attacks followed a recognisable pattern and security teams built layered defences designed to detect known signatures and contain breaches after they occurred. AI has disrupted this equilibrium. Neehar Pathare, MD, CEO and CIO, 63SATS Cybertech explains how AI-enabled cyberattacks has fundamentally changed the threat landscape for enterprises by accelerating speed, amplifying scale, and increasing sophistication across the attack lifecycle.

"Unlike traditional attacks that relied on manual reconnaissance and sequential execution, AI-driven threats automate discovery, exploitation, and execution, allowing attackers to operate continuously and at scale. AI-powered tools can rapidly scan vast enterprise environments, map infrastructure, identify vulnerabilities, and launch thousands of highly targeted attacks with minimal human intervention. What makes these attacks more dangerous is their adaptability."

Pathare points out that AI-driven malware can modify its behaviour in real time to evade detection, learn from defensive responses, and persist within environments far longer than static malware. He further says, "At the same time, AI has introduced deepfake-enabled fraud: enabling highly convincing impersonation attacks such as CEO fraud and Business Email Compromise. For enterprises, this means security models must evolve from reactive controls to intelligence-driven, proactive adaptive defenses that can match the speed and autonomy of AI-powered threats."

THE NEXT FRONTIER IS AGENTIC AI

Autonomous systems capable of executing trades, rebalancing portfolios or optimising liquidity with minimal human intervention. As finance becomes increasingly autonomous, explainability, data integrity and governance will determine whether innovation translates into enduring trust.

HIDDEN RISKS

This shift is particularly significant in a country like India, which operates some of the world's most sophisticated digital platforms in banking, payments, and public infrastructure. AI is increasingly embedded within these systems —optimising everything from fraud detection to citizen service delivery. Yet, beneath this progress lie risks that may not be immediately visible. A compromised model or dataset does not merely affect one endpoint; it contaminates decision-making across platforms.

Recognising the scale of these emerging threats, institutions are also strengthening research-led responses. The IIT Madras cybersecurity centre, CyStar, aims to develop a comprehensive, multi-faceted strategy to address emerging cybersecurity challenges driven by AI and the post-quantum era.

Pathare notes that large enterprises, government organisations and PSUs are increasingly implementing unverified third-party LLM models, libraries, and datasets including older components, that may contain latent vulnerabilities or malicious backdoors, remaining undetected until exploited at scale. "Biggest cases are of data poisoning, where subtle manipulation of training data can distort outcomes in areas like fraud detection or credit scoring, with catastrophic consequences," he adds.

"The ecosystem demands an ethical 'security by design' approach built on three pillars – privacy, proportionality and accountability.

Neehar Pathare
MD, CEO & CIO, 63SATS Cybertech

REACTIVE SECURITY TO CONTINUOUS INTELLIGENCE

In an AI-driven world, cybersecurity is shifting from episodic responses to continuous, predictive and self-learning systems. Daisy Chittilapilly, president, Cisco India and south Asia, points out that as cyber threats adapt in real time, security needs to evolve just as quickly. "When it comes to cybersecurity, the advantage has always been with the attackers—they only have to be right once, while defenders must be right every time," she says. Chittilapilly adds that organisations need AI-driven threat detection, real-time threat intelligence and behavioural analytics to identify emerging risks. These must be integrated with automation of responses, proactive vulnerability management and continuous monitoring— working together to uncover anomalies and prevent attacks before they happen.

"Integrating AI with security information and event management (SIEM) systems will allow security professionals to automatically analyse security alerts to identify genuine threats and filter out false positives. With a strategic and responsible approach to AI, we can shift the balance towards the defenders, creating a more secure digital future," she says.

As Daisy Chittilapilly notes, "India's digital economy is experiencing extraordinary growth, especially through investments in AI, security infrastructure and research and academic collaborations that promote digital trust. By integrating AI into secure-by-design architectures and establishing frameworks for responsible AI governance, India can play a major role in not only building resilient, but scalable cybersecurity solutions that address emerging threats worldwide, shaping the next generation of AI-driven security."

FINTECH AND DIGITAL TRUST

Finance has become one of the most consequential testing grounds for AI's promise and its risks. From credit assessment to fraud detection, artificial intelligence is restructuring how financial institutions evaluate risk, extend access and safeguard transactions. At the same time, cybersecurity challenges in fintech have grown more complex, making digital trust central to financial innovation.

THE HINDU businessline.

June 24, 2026

Tata Electronics' data breach exposes new cyber reality

Our Bureau
Mumbai/Hyderabad

The cybersecurity breach suffered by Tata Electronics on Monday highlights the need for an avant-garde approach to safeguarding enterprise information, according to experts *businessline* spoke to.

A Tata Electronics spokesperson confirmed the security breach after ransomeware group World Leaks posted company details related to Apple and Tesla

"A few weeks ago, Tata Electronics identified a cybersecurity incident on some of our systems. Our response protocols were deployed immediately, and the incident has had no impact on our operations across businesses, which remain unaffected," said the spokesperson. Reports indicate that the hackers were able to access purported component design and specification documents related to Apple and Tesla, both customers of Tata Electronics.

BLAST RADIUS

Such supply chain breaches are among the most damaging in cybersecurity, considering the blast radius that reached beyond the breached entity, according to Srinivas L, Joint MD and Joint CEO, 63SATS Cybertech.

With rising AI adoption, enterprises must embrace a new model of resilience

"When a manufacturer's network is compromised, the attacker inherits trust relationships, customer schematics and proprietary specifications belonging to clients. A single intrusion can expose multiple global corporations simultaneously, converting one vendor's weakness into systemic risk across the ecosystem," he said.

He also warned that the exfiltration of design and inspection documents exposes trade secrets, contractual confidentiality and downstream client liabilities all at once.

For this reason, PrivaSapien argued that the future of cybersecurity must adopt a 'breach by default' mindset, particularly in the face of growing AI-generated attacks.

The company noted that as data moves across increasingly interconnected ecosystems with rising AI adoption, enterprises must embrace a new model of resilience — one that protects data even while it is in use. "The game moves to proactive antidote for attacks. Even in the case of a breach, the need is that compromised data is protected beyond breach. That is where the industry must evolve next," said Abilash Soundararajan, Founder and CEO, PrivaSapien.

THE TIMES OF INDIA

July 4, 2026

Factory floor emerges as new cyber battleground

Vaitheeswaran.B
@timesofindia.com

CYBERATTACKS HIT MFG PUSH

- Threats to Indian plants and industrial control systems are rising sharply, including **AI-powered attacks**; Many attacks are beginning with basic gaps
- Integration of internet, **IoT, robotics, MES systems & real-time monitoring and AI-driven operations** expose legacy assets to vulnerabilities
- Cybersec decisions should move from the **IT realm to the boardrooms**
- Alleged breach of industrial **IPs of global OEMs undermines Indian efforts**

Chennai: Cyberattacks on two major Indian manufacturing facilities recently have highlighted growing cyber risks facing India's factory floors once again.

Bajaj Auto and one of its subsidiaries reported a ransomware attack that affected parts of their IT systems on June 23, while Tata Electronics disclosed a cyber breach a day earlier. Both companies said they activated incident response protocols and took steps to contain the incidents.

The back-to-back attacks underline how cyber threats are becoming a business risk rather than just an IT problem, as manufacturers embrace automation, connected factories and AI-driven operations. Vikash Yadav, head of enterprise for India at Kaspersky, said manufacturing remains one of the most targeted sectors.

According to Kaspersky's latest Industrial Control Systems (ICS) Threat Landscape report for the first quarter of 2026, manufacturing was the only major industry where the share of attacked industrial control systems increased globally, with Southeast Asia recording the highest level of such attacks.

"Threat actors are increasingly targeting internet-facing operational technology at remote sites," Yadav said. "As factories become more connected, they present a larger attack surface for ransomware groups, advanced persistent threat actors and supply-chain attackers exploiting smaller vendors."

The Indian Computer Emergency Response Team (CERT-In) has also urged organisations to strengthen vulnerability management, network segmentation, multi-factor authentication and continuous monitoring as AI makes cyberattacks more sophisticated.

Debashish Roy, chief digital and technology officer at CEAT, said many shop floors still rely on legacy equipment that were never designed with cybersecurity in mind. "Companies need stronger separation between IT and operational technology networks while using AI at the edge so innovation does not come at the cost of security," he said, adding that attacks on production systems can halt manufacturing, compromise worker safety and disrupt business continuity.

The implications go beyond production losses. While Tata Electronics and Bajaj Auto said operations remained unaffected, Reuters reported that the breach at Tata Electronics' Hosur facility allegedly exposed confidential Apple and Tesla information, including component details and images of unreleased Apple products.

Srinivas L, joint CEO of 63SATS Cybertech, said India's ambitions under the China-plus-one strategy depend as much on protecting intellectual property as on expanding manufacturing capacity. "If India acquires a reputation for IP leaks, it could erode the trust that underpins the China-plus-one opportunity," he said, adding that going ahead sector-specific cybersecurity guidelines and stronger incident reporting through CERT-In would improve resilience.

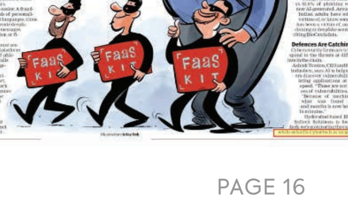
THE TIMES OF INDIA

Special Feature – July 6, 2026

TIMES *Special*

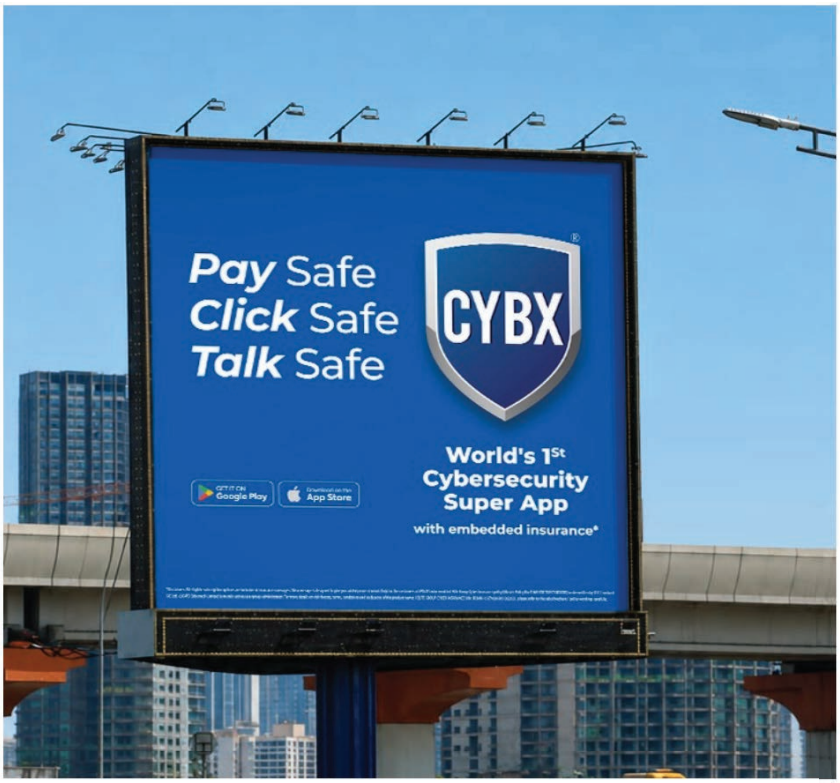
Fraud-as-a-Service: How cybercrime became a subscription business

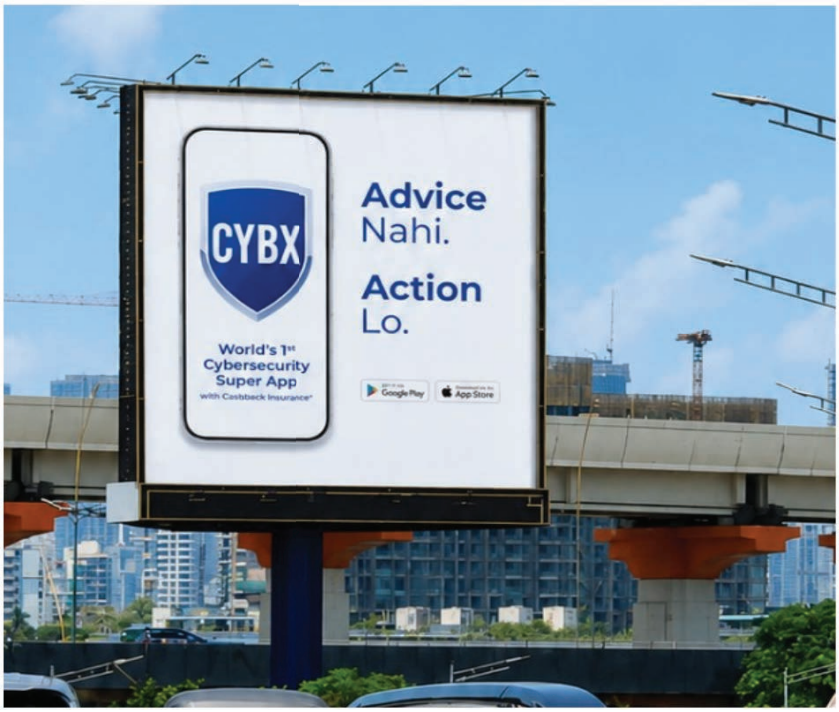
AI-powered 'FaaS' platforms are enabling low-skill fraudsters to deploy phishing, deepfakes and scams at scale, posing growing risks to India's digital economy



Out-of-home & hoardings

High-visibility out-of-home placements put the 63SATS and CYBX brands into physical public space, anchoring recognition and trust at scale.





13
FY27 TRAJECTORY

Q1 has moved the FY27 plan from ambition to execution. The remaining three quarters are about disciplined conversion.

Dimension	FY27 Position at Q1	Focus for H2 FY27
Order Book	₹288 Cr booked (Already achieved 82% of FY27 target)	Convert order book to billed revenue on schedule
IP Revenue	CYBX DNA AI CyberOps ₹53 Cr+ cumulative	Deepen IP mix; scale CYBX DNA AI CyberOps deployments
Consumer	2 Mn+ downloads, 3.25+ Lakh paid subscribers	Publicis-led acquisition; CYBX Coin launch
Compliance	65+ clients onboarded for DPDPA	Scale toward the ₹100 Cr+ DPDP GTM
Delivery Capacity	Team scaling toward 190	Hire and certify ahead of the delivery curve
Governance	Board strengthened by two directors	Institutionalise oversight at scale

The single strategic priority

With approx. 82% of the annual target already committed as order book in Q1, the decisive variable for FY27 is no longer demand. It is delivery execution at scale: converting order book to revenue on time, without compromising quality, while protecting the margin path toward our EBITDA objective.

Services create relationships. Products strengthen them. Intelligence sustains them.

Secured by Design. Sovereign by Default.

One year ago, a ₹3.6 Cr company. At FY26 close, ₹87 Cr. One quarter into FY27, ₹288 Cr already in the order book. The foundation is built. FY27 is where we deliver.