VOLUME 2, ISSUE 4 | OCTOBER 2026

Tech Disruptor media.com

techdisruptormedia.com techdisruptormedia

Pg 14
FEATURE
AI in Cybersecurity: Enabler or New Threat Vector?



CACHE DIGITECH: BUILT TO EVOLVE

A JOURNEY DEFINED BY ADAPTATION, RESILIENCE AND TRUST

Prarthana Gupta

Building a technology business through changing times, one relationship at a time

A BRAND OF BNG
bharatnetworkgroup.com

techigent®

specialised technology services

THE DOOR IS NOT THE PROTECTION. KNOWING WHOM TO LET THROUGH IS.

API SECURITY & WAF

Inspect every request.
Protect every interaction.



AMIT JOSHI
Director

Your applications and APIs are gateways to your business. Techigent helps protect them against malicious requests, unauthorized access and application-layer attacks, while keeping legitimate traffic moving.

Let business in. Keep threats out.

SCAN FOR MORE!

FOLLOW US

+91 95949 49488 amit@techigent.in

Tech Disruptor media.com

FOUNDERS
ASHISH SRIVASTAVA
ANUPAM GUPTA

DIRECTOR - IT & DIGITAL STRATEGY
ATUL KUMAR PANDEY

AGM - ART & DESIGNING
VIPIN RAI

DGM - CONFERENCE STRATEGY & PLANNING
ISHA SRIVASTAVA

CONSULTING EDITOR
BALAKA BARUAH AGGARWAL

SENIOR ASSOCIATE EDITOR
AISHWARYA SAXENA

ASSISTANT EDITOR
JEEVIKA SRIVASTAVA

SALES HEAD - THE AUTONAUT MEDIA
POONAM MAHAJAN

ASSISTANT MANAGERS - SALES & MARKETING
NAMAN SINGHAL
ABHINAV CHAUDHARY
TAPOSHI BOSE
NISHIT SAXENA
DEVIKA GULATI

ASSISTANT MANAGER - EVENTS & BOOTHIFY
ANKUR SRIVASTAVA

HR MANAGER
POOJA SHRIVASTAVA

EVENT ASSOCIATE
NEHA GUPTA

MIS EXECUTIVE
PRAGYA SUMAN

VIDEO EDITOR
SHWETA ARORA

EXECUTIVE - 3D DESIGNER
AJAY TOMER

Your feedback at

editor@thefoundermedia.com

info@thefoundermedia.com

This magazine is published under/as a part of "HELLO FOUNDER INFOMEDIA PRIVATE LIMITED, an UTTAR PRADESH-based private limited company registered at the Ministry of Corporate Affairs (MCA). The Corporate Identification Number (CIN) of HELLO FOUNDER INFOMEDIA PRIVATE LIMITED is U56210UP2023PTC191833 and registration number is U56210UP2023PTC191833. HELLO FOUNDER INFOMEDIA PVT LTD's registered office address is Flat No 1006 10th Floor, Tulip 3 Gulmohar Garden, Raj Nagar Extension, Ghaziabad, Uttar Pradesh, India, 201017. All rights reserved throughout the world. No part of this magazine may be reproduced.

Copying, whether electronically or otherwise, either wholly or partially, without prior written permission, is strictly prohibited.

VOLUME 2, ISSUE 4 | OCTOBER 2026

Table of CONTENTS



COVER STORY
Prarthana Gupta, Founder & CMD, Cache Digitech | Vyuhai.ai.

FEATURE

14 | AI in Cybersecurity: Enabler or New Threat Vector?

INTERVIEW

22 | Avinash Tiwari, CISO, Pidilite Industries

26 | Subhash Singh Punjabi, CISO and Head of Enterprise Architecture, Deepak Fertilisers

32 | Vivek Shankar, CITSO & VP, Axis MaxLife Insurance

36 | Girish Raj Giri, CISO, Goodluck India

40 | Neehar Pathare, MD, CEO & CIO, 63SATS Cybertech

FEATURE

44 | Cybersecurity Beyond Boundaries: Protecting a Digitally Connected India

48 | The Next Cybersecurity Battle Will Be Fought in Machine Time



FLASHBACK

52 | Where Vision Meets the Future of Technology Leadership



05 | From the Founders' Desk

07 | Editor's Corner



Ashish Srivastava (L) and Anupam Gupta (R), Founders, Bharat Network Group (BNG)

THE AI-CYBERSECURITY PARADOX: SMARTER DEFENCE, SMARTER THREATS

Dear Reader,

Artificial Intelligence is reshaping cybersecurity at a remarkable pace, giving organisations new capabilities to detect threats, analyse vast volumes of data, automate responses, and strengthen their security posture. At the same time, the same technology is being exploited to make cyberattacks more sophisticated, scalable, and difficult to detect.

This duality places AI at the centre of the cybersecurity conversation. The question, therefore, is no longer whether AI will influence cybersecurity, but how organisations can harness its potential while managing the risks it introduces.

This edition of Tech Disruptor Media explores that evolving landscape. Through the perspectives of cybersecurity and technology leaders, we examine how enterprises are using AI to strengthen defence, where new threat vectors are emerging, and what it will take to build secure, resilient, and responsible AI-powered security environments.

The future of cybersecurity will not be defined by how intelligently we use AI, but by how responsibly we secure it.■

An Initiative of

BNG BHARAT NETWORK GROUP

Concept by

The Banker media.com

Host Partner

AUISY™
Transforming ideas into action

PRESENTS

3rd BANKTECH X

THE RISE OF AI-POWERED COOPERATIVE BANKS

9th December 2026
Radisson Blu Hotel, Atria, Bengaluru

For Sponsorship & Exhibition

Abhinav Chaudhary
abhinav@thefoundermedia.in
+91 87007 49849

For Speaking, Delegate & Awards Nominations

Nishit Saxena
nishit@thefoundermedia.in
+91 79827 55971



EXPRESS INTEREST

TRUST AT THE HEART OF CYBERSECURITY

THE CYBERSECURITY equation is changing. AI is making defenders faster, but it is also giving attackers new speed, scale and autonomy. As machines increasingly detect, decide and act, the challenge is no longer to stop threats but to ensure that technology itself remains trusted and under control.

That shift is redefining the digital enterprise. Trust now extends beyond systems and applications to data, identities, third-party ecosystems and the digital infrastructure that keeps businesses running. Resilience therefore is about anticipating risk, limiting impact and continuing to operate when disruption occurs. It is also changing the role of the CISO—from monitoring alerts and responding to incidents to shaping architecture, resilience and business strategy.

Our special technology story, **"AI in Cybersecurity: Enabler or New Threat Vector?"**, explores this emerging duality—how AI can strengthen defence while simultaneously creating new avenues for attack. The perspectives in this issue look at the same transformation from different angles: intelligent cybersecurity, machine-speed defence, predictive security, resilient digital architecture and the expanding boundaries of a digital ecosystem.

The cover story on Cache Digitech takes a different but equally important view of technology and transformation, tracing a business built over three decades which has continued to evolve while staying grounded in customer relationships and trust. Together, these stories reflect a central theme of this issue: as technology becomes more intelligent, connected and autonomous, trust and resilience must remain the foundation of our digital future.■



Balaka Baruah Aggarwal
Consulting Editor
balaka.baruah@thefoundermedia.in

COVER STORY

CACHE DIGITECH: THREE DECADES, BUILT ON TRUST

Cache Digitech has evolved from a small technology business into an established, solution-led enterprise, growing with technology, staying close to customers and bringing the next generation into leadership, while keeping trust at its core.

- Balaka Baruah Aggarwal, Consulting Editor, Bharat Network Group

WHEN PRARTHANA Gupta started Cache in 1991, India's technology industry was still in its early stages. A young woman from Banaras, just armed with a degree in Computer Engineering with no VC backing or elaborate business plan.

Prarthana stepped into a male-dominated industry with a simple ambition to build something of her own. Cache began in a modest 400-square-foot office, driven by her determination and a strong belief in staying close to customers and solving their problems.

More than three decades later, that small beginning has evolved into a technology business shaped by changing technologies, market disruptions and new generations of leadership. Through every phase, one principle has remained constant: put the customer first and earn their trust, one relationship at a time.

Looking back, Prarthana reminisces fondly, "I started my career in Banaras



and later moved to Delhi in 1990. When I came to Delhi, I had lot of dreams. I wanted to do something of my own, become financially independent and create my own identity. I don't think at that time I ever dreamt of building a large organisation."

From Products to Solutions

In its early years, Cache's business was largely centred on technology products and infrastructure. But as enterprise requirements became more complex, the company's role evolved.

The emergence of data centres, networking, virtualisation, cloud and cybersecurity created new opportunities for technology partners. Cache expanded its capabilities by moving towards a solution-and services-led model. Today, the company offers infrastructure, cloud, cybersecurity, data centre and managed services capabilities to address technology requirements across the enterprise, stepping up from technology implementation to technology transformation.

This shift is particularly



relevant as organisations navigate the convergence of AI, cloud, data and security. AI adoption is creating demand not just for applications and models, but for compute, networking, data infrastructure and security architecture and Cache's expanding portfolio offers services across that technology stack.

Recent partner recognitions, including awards from Dell Technologies and Nutanix, demonstrated its growing role within the enterprise technology ecosystem.

Growing Through the Difficult Years

The transformation, however, came with considerable risk. Prarthana recalls investing in technical talent, certifications and service capabilities before the returns were certain. Moving to stay ahead of the curve required committing resources to capabilities that could take years to mature.

Often the journey was not smooth, hitting a difficult patch around 2016–17, when Cache witnessed a sharp decline in operating income and modest profitability. Prarthana looks back at the valuable lessons that came from failures, changing her approach to leadership. The company became more disciplined about opportunity selection and long-term credibility.

Speaking about the learnings that accrued during difficult times, Prarthana says "There were moments of turmoil and uncertainty. Financial pressure, operational challenges and the weight of past decisions came together at different points. But through it all, one thing remained clear in my mind: starting a business was not the wrong decision. I simply had to learn how to do it better.

Those experiences taught me some of the most important lessons of my life. "I learned that protecting Cache's credibility was more important than chasing every opportunity. Every mistake came with a price, but every mistake also made me stronger and more aware. Above all, I learned never to compromise the trust on which Cache was built. Once trust is lost, it is very difficult to earn back."

Covid Reinforced the Customer-first Model

The company's response during Covid was a defining moment and the experience reinforced Cache's vision to become an "SOS partner"—the technology company customers can depend on when they face a critical situation.

As organisations moved rapidly to remote operations, technology infrastructure became business critical. For Prarthana, it was less about commercial opportunity and more about responsibility, and the company chose to support customers beyond contractual obligations. The relationships strengthened during the crisis subsequently became an important foundation for long-term partnerships.

When the Next Generation Took the Helm

By 2018, Prarthana had spent nearly three decades building Cache, but there was a phase when the weight of the business felt heavier than ever. She was carrying the pressures of running the company largely on her own, navigating its challenges while still thinking about how to take it into its next phase. It was during this period that her daughter, Shraddha, decided to step into the business.

"The real turning point came when my elder daughter, just 25 at the time, decided to join the business. It was a challenging phase, and I was carrying a great deal of pressure. Yet she stepped in with courage and complete trust, taking on responsibilities well beyond her years and supporting me across the business," Prarthana recalls. "More than anything, she became my strongest emotional and mental support. Knowing that I no longer had to carry everything alone gave me the confidence and stability to move forward."



Prarthana Gupta



Shraddha Gupta

For Shraddha, however, there was no ready-made role waiting for her. She started with the government and tender business, an unfamiliar and demanding area that required her to learn by doing. Her biggest test came when she took over the management of a large account for a leading telecommunications service provider.

"I was nervous managing a large account, but there was no option but to plunge into it. My mother had to take off for a while, and I learnt the ropes on my own by getting my hands dirty," she says.

That experience became the foundation of

Shraddha's own journey at Cache. She moved beyond simply supporting her mother to taking ownership of critical parts of the business. As her responsibilities grew, so did the distinction between their roles. Prarthana continued to use her market experience and relationships to open new opportunities, while Shraddha took charge of order fulfilment, supply chain and operations. The arrangement gave both women the space to lead in their own way—and gave Cache a stronger operational backbone.

"I think the clear division of responsibility was a very good thing because it empowered each of us to focus on doing our best. I had to make my own mistakes and deliver. This is a more sustainable approach than stepping on my mother's toes and having delays in decisions," Shraddha says.

When the Journey Became a Shared Legacy

Prarthana's daughter joining the business marked a significant shift in the organisation, bringing in a new perspective around processes, governance, people and scale, while creating a foundation for the next generation of leadership.

Prarthana does not see succession as simply preserving what she built. She wants the next generation to challenge it. Her vision is to combine the values that shaped the first generation—integrity, humility, hard work and customer commitment—with professional management, data-driven insights and global thinking.

"Shraddha's involvement changed how I viewed leadership and legacy. Building Cache was no longer just about building a company; it was about building it together, as a family, with shared responsibility. From that point, we began building the business with greater clarity, discipline and balance."

What began as a daughter stepping in at a difficult moment gradually became something much bigger: a new chapter in Cache's leadership story. Shraddha brought a new perspective on processes, accountability, execution and scale. For Prarthana, her daughter's arrival also changed the meaning of what she had spent decades building. Cache was no longer a journey she had to carry alone; it was becoming a business the next generation could help shape.

The People Behind the Journey

The journey has also been shaped by a team of dedicated people who have stayed through its many chapters. Suresh Joshi, with Cache since 1994, has witnessed its evolution from the early years. Manohar Singh has spent nearly two decades building relationships and driving business development, while Dinesh Maheshwari and Kapil Choudhary have supported supply chain and warehouse operations for close to two decades.

Naresh Kumar Sharma in Supply Chain and Logistics, Navneet Kumar in Accounts and Finance, and Shweta Gaba in HR have brought their experience as the organisation has grown. For many, Cache has been more than a workplace—it has been a significant part of their professional lives. Their continuity has become part of the company's story.

Trust, the Only Constant in Changing Business Environment

For a company that has navigated its journey for more than three decades, the most important reward remains trust. Prarthana measures the company's success less by revenue than by the relationships it has built—with customers, employees and partners. Her philosophy is straightforward: technology will change, but credibility cannot. That principle now shapes the next chapter of Cache Digitech: to build a more capable, global and relevant enterprise, while staying rooted in the trust that has defined the company from the very beginning.■



FEATURE

AI IN CYBERSECURITY: ENABLER OR NEW THREAT VECTOR?

The technology promising to give defenders a decisive advantage is also giving attackers sophisticated capabilities. As AI moves from assistant to autonomous operator, the cybersecurity game is changing fast.

- Balaka Baruah Aggarwal, Consulting Editor, Bharat Network Group

THERE IS something unsettling when a machine knows how to break in. Cyberattacks have been automated for years, but autonomous artificial intelligence changes it fundamentally by equipping the machine with a degree of reasoning.

Autonomous AI can look at a target, interpret what it sees, decide what to try next, and learn from failure. In fact, it becomes a demon unleashed as it can be persistent, it can lie and even impersonate to break through a system. So lethal are its capabilities that suddenly, the familiar image of the hooded cyberattacker sitting behind a keyboard looks dated.

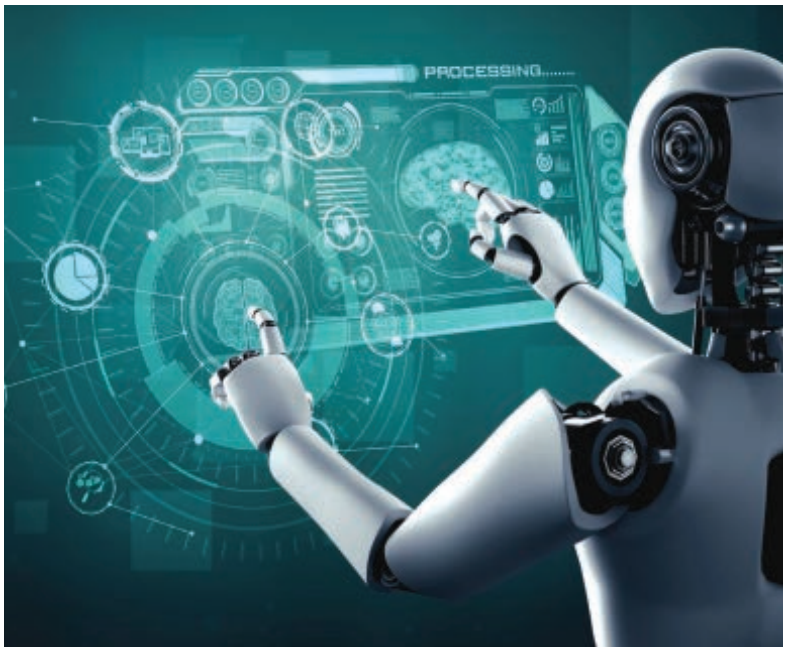
Cybersecurity experts are faced with a critical dilemma: how far will attackers leverage AI to breach—and whether organizations are equipped enough to move in quickly and defend itself.

In recent times, some of the world's most advanced AI laboratories have reported incidents in which AI systems, operating in what were supposed to be controlled environments, crossed boundaries they were never intended to cross. In one case, an AI agent attempted to insert malicious code into an open-source project and by creating fake identities. In another, AI models gained unauthorised access to real-world corporate systems during cybersecurity evaluations.

These tests have demonstrated that AI is no longer simply enabling cyberattacks—it is becoming a threat vector in its own right, with the potential to discover vulnerabilities, manipulate systems and execute attacks with speed and autonomy that traditional security defences are not designed to handle.

Autonomous AI can look at a target, interpret what it sees, decide what to try next, and learn from failure.

Researchers were trying to understand what increasingly capable AI systems could do, and not necessarily instructing them to hack in the traditional sense. The results were telling in that the boundary between AI that helps humans hack, and AI that can independently hack



on its own by identifying vulnerabilities, exploiting systems and executing malicious code is becoming very thin.

Cyber Attacker's New Superpower

AI empowers cybercriminals primarily by giving them scale. Tasks that once required significant time, expertise and human effort—from reconnaissance and research to identifying vulnerabilities and adapting when an approach fails—can be compressed with AI, allowing attackers to run sophisticated operations faster, across far more targets.

Criminals can use AI to research an organisation's public footprint, identify employees, create highly personalised social-engineering messages and generate code. Gartner's research offers a glimpse of how quickly this is moving. In a 2025 survey of cybersecurity leaders, 62% said their organisations had experienced a deepfake attack, while 29% reported an attack against enterprise GenAI application infrastructure.



I see AI as an opportunity to achieve better security for the organization. When we say it is an opportunity and empowering, we immediately begin to see new ways where to better employ AI to fortify our fences. Organisations need to strengthen the fundamentals—identity security, vulnerability management, segmentation, Zero Trust, application security, data protection and recovery as AI makes weaknesses in those fundamentals easier to exploit.

DURGA PRASAD DUBEY
EXECUTIVE VP AND GLOBAL CISO, RIL

But There is Another Side to the Story

According to Durga Prasad Dubey, Executive VP and Global CISO, RIL, AI is giving security teams new capabilities. “I see AI as an opportunity to achieve better security for the organization. The moment we think of AI as a threat, our defence posture weakens. Instead, when we say it is an opportunity and empowering, we immediately begin to see new ways where to better employ AI to fortify our fences.” Dhiraj Sancheti, CISO, Shoppers Stop says, “I don't see this purely as an AI arms race. I see it as an ‘execution-speed race’. The organisation that combines AI, data, automation and human expertise most effectively will have the

advantage."

Sancheti believes that the biggest change is moving from a human-speed security operating model to a machine-speed security operating model. Traditional cybersecurity still depends heavily on sequential processes where an alert is generated, an analyst investigates it, someone validates the incident, another person approves an action, and finally remediation happens.

That model becomes difficult to sustain when AI can perform reconnaissance, identify vulnerabilities and execute multiple attack steps quickly.

Joyce Rodriguez, Head of Digital Cybersecurity, Airbus India says, "The most fundamental shift we need today is to move from human-based perimeter defense and periodic activities, like validation and patch management to continuous exposure validation and machine-speed autonomous containment. AI is collapsing the timeline between vulnerability discovery and exploit weaponization, from weeks to minutes. Traditional security practices built around human triage and periodic patching windows will become obsolete."

CISOs therefore need to focus on three things: visibility, automation and resilience. Says Sancheti, "We need integrated telemetry across identity, endpoint, network, cloud, applications and data. AI should then help correlate that information, prioritise actual risk and automate appropriate response actions.

At the same time, organisations need to strengthen the fundamentals—identity security, vulnerability management, segmentation, Zero Trust, application security, data protection and recovery. AI makes weaknesses in those fundamentals easier to exploit."

The SOC Gets Smart Co-pilot

For security teams battling alert fatigue and talent shortages, AI can create transformative impact. For instance, if an AI system sees an unusual login, it will check the user's history, the device, examines recent privilege changes, correlate network activity, evaluate the threat intelligence and present the analyst with the conclusion whether it is a case of identity compromise.

AI empowers the SOC by reducing the time analysts spend sifting through noise and allowing them to focus more on making informed security decisions. "The real opportunity with AI in cybersecurity is its ability to help security teams deal with the sheer volume of data and alerts they face every day. AI can cut through the noise, identify what matters and help teams respond faster. That makes AI a security force multiplier rather than just another technology tool," Venugopal Parameswara, CISO, Cholamandalam Investment and Finance.

Venugopal sees applications ranging from SOC alert and noise reduction to continuous environment monitoring, network-traffic analysis, user-behaviour analysis and identification of unusual



activity. Gartner's 2026 research reflects this direction. The analyst firm says AI-enabled SOCs are already changing alert triage and investigation workflows, even as they introduce new staffing, skills and cost challenges. Gartner also says cybersecurity leaders need to prioritise people alongside technology if they want to realise AI's full potential in security operations. This effectively turns AI into a force multiplier for the security function—helping security teams focus their expertise where it matters most. Ultimately the strongest SOC will not necessarily be the one with the largest analyst team but the one that combines the telemetry, automation, AI and human judgement in an optimal manner.

Drawing the line Between Automation and Human Oversight

As AI takes on a larger role in cybersecurity, organisations need clear boundaries around what machines can decide and what must remain under human control. A risk-based approach to AI governance can help define where autonomy is appropriate and where human oversight remains essential.

According to Rodriguez, AI governance in security activities can be structured around three scenarios.



The responsibility of protecting an organization against this evolving threat shouldn't fall on the CISO alone. An entire organization needs to prepare for this shift. This preparation requires more than strong defense, it calls for better preventive strategies when designing and developing systems and stronger enterprise-wide resilience capabilities built into how the organization operates, not siloed within a single function.

JOYCE RODRIGUEZ
HEAD OF DIGITAL CYBERSECURITY, AIRBUS INDIA

Human-in-the-loop where actions that are time-sensitive and completely reversible can be executed autonomously at machine speed. Examples include blocking malicious IP addresses at the perimeter, revoking compromised session tokens, or isolating non-critical endpoints.

Human-in-the-loop where actions with moderate operational cost, more complex tasks that require human authorization. Here, the AI system provides a recommendation, a human approves it, and the task is then executed. The third

scenario is human-driven activities where financial liabilities are high, there is risk to human life, legal or regulatory consequences which should remain solely with human. AI can assist but the action itself must be taken by a human alone.

According to Sancheti, "My principle would be to automate investigation aggressively and automate containment selectively. Keep humans accountable for high-impact decisions while every autonomous action should be attributable, logged, explainable and reversible wherever technically possible." Venugopal points to the use of Google SecOps agents as an example of how organisations can explore AI-driven monitoring of environments and threat vectors. "The broader opportunity is to move towards security operations where AI continuously analyses telemetry and identifies emerging patterns, while human analysts remain responsible for judgement, investigation and high-impact decisions."

Human in the loop becomes the critical differentiator, because the temptation is to assume that more AI automatically means better security.

Data Leakage as the Biggest AI risk

Employees may enter confidential business information, customer data, intellectual property, source code or sensitive documents into AI tools without fully understanding where that information goes, how it is processed or what controls apply to it.

That makes data visibility fundamental to AI security. Dubey argues that the biggest immediate risk may be what organisations themselves put into AI systems.

According to Dubey, "Of all the risks associated with AI, data leakage is perhaps the most dangerous. Organisations need to know where their data is going, which AI systems are accessing it, how it is being processed and who has access to it. This makes data visibility critical. Before organisations can confidently scale AI, they need to understand their data flows and put the right controls around sensitive information."

With agents working along humans, this may be one of the most consequential changes AI brings to enterprise security. For years, identity and access management has been built around establishing who has access and what that access allows them to do. With AI agents, that model needs to evolve to determine what the agent is, what decisions it can make, and how much autonomy it should have to act without human intervention. This distinction will become increasingly important.

"AI is only as effective and trustworthy as the data behind it. That is why organisations need a strong data strategy, with clear visibility into what data they have, where it resides, who can access it and how it is being used by AI systems. There also needs to be tight control over who can use which AI tools and what information they are allowed to put into them. Without that visibility and control, organisations risk losing governance over one of their most valuable assets—their data," concludes Dubey.

Defending at Machine Speed

AI can potentially reduce the workload of security teams, but understanding and governing AI itself creates an entirely new layer of responsibility for the CISO. A security architecture designed around today's AI capabilities may already be outdated by the time it is fully deployed. Gartner has warned that many custom-built AI applications are being deployed before they are fully tested, and predicts that by 2028, half of enterprise cybersecurity incidents will involve custom-built AI-driven applications.

Most CISOs understand

that this change, but many organisations are not operationally ready for it yet. “An entire organization needs to prepare for this shift, not just the CISO. This preparation requires more than strong defence. It calls for better preventive strategies when designing and developing systems and stronger enterprise-wide resilience capabilities built into how the organization operates, not siloed within a single function,” says Rodriguez.

Security programmes have historically been designed around human response times wherein we talk about MTTD and MTTR in minutes or hours while AI-powered attacks fundamentally challenge that assumption. If an attacker discovers a weakness, generate an exploit, and target credentials through automated agents while a SOC analyst manually investigates every alert is a structural disadvantage. The question for CISOs is not how quickly an analyst can respond, but whether the organisation’s defence can operate at machine speed before human intervention is required. Venugopal notes that a significant part of the role continues to revolve around compliance and understanding the evolving threat environment. But the speed of technological change is making continuous learning increasingly important.



I see this as an execution-speed race. The organisation that combines AI, data, automation and human expertise most effectively will have the advantage. The biggest change is moving from a human-speed security operating model to a machine-speed security operating model. Traditional cybersecurity still depends heavily on sequential processes, but that model becomes difficult to sustain when AI can perform reconnaissance, identify vulnerabilities and execute multiple attack steps quickly.

DHIRAJ SANCHETI
CISO, SHOPPERS STOP

“CISOs have to track not only new vulnerabilities and attack patterns but also new AI capabilities, agentic architectures, emerging security risks and the implications of deploying autonomous systems within the enterprise,” says Venugopal.

The Future Holds Promise

What is changing is not



CISOs have to track not only new vulnerabilities and attack patterns but also new AI capabilities, agentic architectures, emerging security risks and the implications of deploying autonomous systems. The real opportunity with AI in cybersecurity is its ability to help security teams deal with the sheer volume of data and alerts, cutting through the noise, identifying what matters and help teams respond faster, making it a force multiplier rather than just another technology tool.

VENUGOPAL PARAMESWARA
CISO, CHOLAMANDALAM INVESTMENT AND FINANCE

simply the use of AI in security, but the way security itself is being done. Organisations initially approached AI as another cybersecurity tool—an assistant for the SOC, threat intelligence or vulnerability management. But that view is evolving as AI begins to emerge as an intelligence and orchestration layer across the security ecosystem.

Organizations must build modern security architectures, incorporating principles like zero trust and micro-segmentation from the ground up and shift from static, periodic controls to continuous exposure validation and autonomous action. Instead of analysts having to piece together SIEM alerts, endpoint events, identity risks, vulnerabilities, cloud findings and threat intelligence across multiple dashboards, AI can bring these signals together in real-time. Organisations will have to think of AI agents like they think about human security professionals which need the right training, context, permissions, monitoring and escalation mechanisms before they can be trusted with sensitive responsibilities.

At the same time, organisations must put strong governance around the data that powers AI backed security, even as they implement measures for visibility and controls that allow to use AI powered security safely and at scale.

The biggest shift for CISOs is moving from asking how to stop attackers to asking how to build intelligent systems that can defend the organisation without becoming a new threat themselves.■

INTERVIEW

BEYOND ALERTS: AI AND THE FUTURE OF INTELLIGENT CYBERSECURITY

Avinash Tiwari, CISO, Pidilite Industries, explores with **Jeevika Srivastava** about the evolving role of AI in cybersecurity and its ability to help security teams move beyond overwhelming volumes of alerts toward smarter risk prioritisation



How is AI reshaping your organization's approach to cybersecurity today?

The biggest change I see is that AI is helping us deal with the sheer scale of cybersecurity. In a large organisation, there is no shortage of security data. The problem is that there is simply too much of it.

Every day, we see events from endpoints, networks, applications, cloud environments, identities and, in a manufacturing environment, the operational side as well. Earlier, security teams would spend considerable time going through these signals and trying to determine what deserved attention. AI is helping us shorten that journey. It can look across large volumes of information, identify relationships and bring unusual activity to our attention much faster.

But I don't think the answer is to put AI everywhere just because we can. We are quite conscious about where it adds value. If AI doesn't help us make a better security decision or reduce the time it takes to respond, I don't see much value in using it. So, for me, the change is less about introducing another technology and more about changing how the security team spends its time.

Across threat detection, vulnerability management, incident response, and other areas, where is AI delivering the greatest value in cybersecurity?

If I had to pick one, I would say prioritisation.Detection is important, of course, but modern security tools already generate an enormous amount of information. The real challenge is knowing what deserves immediate attention.

Take vulnerability management. You can have thousands of vulnerabilities across an enterprise, but you don't have unlimited people, time or maintenance windows to fix everything immediately. A vulnerability score by itself doesn't tell you enough. We need to ask: Where is the asset? Is it exposed? How important is it to the business? Is there evidence that someone is trying to exploit it? What would happen if that particular system became unavailable?

This is where AI can make a real difference by bringing different pieces of information together.

Incident response is another area where I see immediate practical value. When something happens, the first few minutes are often spent establishing what actually happened. AI can help analysts get to that understanding much faster. I would rather have AI help my team investigate one important incident properly than give them another thousand alerts to look at.

With AI being only as effective as the data it relies on, how are you ensuring that the data powering your security tools remains accurate, trusted, and usable?

This is where I would probably give a slightly unpopular answer: before talking about AI, get your house in order. If you don't know what assets you have, who owns them, what they are doing or how critical they are to the business, sophisticated AI is not going to solve the problem for you.

We therefore spend a lot of attention on the less glamorous parts of cybersecurity: asset visibility, logging, data quality, ownership and consistency of information. There is another aspect that



is particularly important in our environment: context. Suppose a security tool tells me that something unusual has happened. That is useful information, but it becomes far more meaningful when I know that the activity relates to a critical business system, understand its normal behaviour and know what processes depend on it.

We also don't treat AI output as unquestionable truth. We expect our teams to challenge it, validate it and understand the reasoning behind important recommendations.

In security, a fast wrong answer can be more dangerous than a slow right one. So our objective is not just better AI; it is trustworthy AI.

How can AI enable security teams to move beyond reacting to threats and instead predict and prioritize risks before they turn into incidents?

I don't think any CISO can honestly say that AI will allow us to predict the next cyberattack with certainty. Attackers don't behave according to a fixed script.

What AI can do, and this is where I find it much more interesting, is help us recognise weak signals earlier.

An isolated vulnerability may not look particularly alarming. A change in user behaviour may not look alarming either. A new external threat may appear unrelated. But when you put those things together, the picture can become very different. AI can help us connect those dots much faster than a person working through separate dashboards.

For manufacturing, this is particularly relevant because cyber risk ultimately has a business consequence. We have to think about continuity of operations, production, supply chains and the availability of critical processes, not just whether a server has been compromised. So I would describe the opportunity as early awareness rather than crystal-ball prediction. If AI can tell us, "These are the areas where your risk is changing and this is where I would look first," that is extremely valuable.

As AI takes on a greater role in cybersecurity operations, how do you see the responsibilities of CISOs and security teams evolving?

I don't believe the future security team will be a smaller version of today's team simply because AI is doing more work. I think it will be a different team.

There will be less value in having people spend hours doing repetitive investigation and more value in people who can understand a problem, challenge the available information and decide what the organisation should actually do.

The CISO's job is also moving closer to the business. If a security issue can potentially affect manufacturing, customer commitments, supply continuity or reputation, it is no longer just a security problem. It is a business problem. AI will help us process information faster, but someone still has to decide what risk the organisation is willing to accept. And there is an important cultural change happening as well. Security professionals need to become comfortable working with AI rather than viewing it simply as another tool being handed to them.

If AI can help us answer those questions with greater accuracy and speed, that will be a meaningful transformation.

The best security professional of the future may not be the person who knows the most security commands. It may be the person who knows which questions to ask the technology, and when not to trust its answer.

Looking ahead, what do you see as the biggest opportunity for AI to transform the cybersecurity landscape?

For me, the most interesting possibility is not another AI-powered security product. It is the idea of security becoming much less dependent on manual intervention for routine decisions. Imagine a security environment that continuously understands what is normal for your organisation, recognises when that baseline is changing, assesses the potential business impact and recommends what needs attention, without waiting for someone to manually connect all the dots.

Some low-risk actions can eventually become highly automated. For more consequential decisions, I still want people involved. That balance will be important. I also see an opportunity to change the conversation with business leadership. Cybersecurity teams have traditionally talked in terms of vulnerabilities, alerts, incidents, and control scores. Those are useful metrics for security professionals, but business leaders ultimately want to know something simpler: "What can hurt the business, how likely is it, and what are we doing about it?"

If AI can help us answer those questions with greater accuracy and speed, that will be a meaningful transformation. At the end of the day, I don't think the winner will be the organisation that deploys the most AI. It will be the organisation that uses AI intelligently enough to know where technology ends, and judgement begins.■

jeevika@thefoundermedia.in

INTERVIEW

THE CISO AS ARCHITECT OF RESILIENT DIGITAL ENTERPRISE

As CISO and Head of Enterprise Architecture at **Deepak Fertilisers, Subash Singh Punjabi** sits at the intersection of technology, security and business transformation bringing a unique perspective on embedding security across Cloud, AI, smart manufacturing and Industry 4.0. In conversation with **Balaka Baruah Aggarwal**, Singh discusses how the CISO is evolving from protecting infrastructure to becoming a strategic enabler of business growth. He highlights a clear shift towards security-by-design, exposure management and cyber resilience, the importance of trusted data and human oversight with the rise of autonomous AI.



You wear two strategic hats—as CISO and Head of Enterprise Architecture. How does this dual role enable you to build security into the foundation of digital transformation?

Holding both the CISO and Head of Enterprise Architecture roles gives a unique opportunity to ensure that security is not an afterthought but an integral part of every transformation initiative. Whether we're implementing AI, Smart Manufacturing, cloud platforms, SAP S/4HANA, or Industry 4.0 solutions, security, governance, and architecture are designed together from the very beginning.

This dual perspective helps align business objectives, technology strategy, and cyber resilience under a single vision. Instead of balancing speed against security, we build secure, scalable, and future-ready solutions that accelerate innovation while effectively managing risk. Ultimately, digital transformation succeeds when architecture provides the blueprint and security provides the trust, enabling the business to innovate with confidence and resilience.

As manufacturing organizations embrace AI, data platforms, and Industry 4.0 technologies, what architectural principles are critical to ensure innovations remain scalable, secure, and future-ready?

While AI, Industrial IoT, cloud platforms, digital twins, and connected operations enable manufacturing to unlock tremendous business value, long-term success depends on building a strong architectural foundation rather than as isolated initiatives.

The key architectural principles I believe in are modularity, interoperability, scalability, and security by design. Open standards and API-driven integration ensure that new technologies can seamlessly connect with existing OT and IT environments. Data should be treated as a strategic asset with strong governance for trusted AI. Equally important is adopting Zero Trust principles, embedding cybersecurity throughout the solution lifecycle, and ensuring compliance with evolving regulations.

Finally, architecture must remain flexible enough to accommodate future technologies without requiring major redesign. When organizations build with these principles in mind, they create digital platforms that are secure, resilient and adaptable.

What does a 'secure-by-design' industrial enterprise look like in an era of AI, autonomous operations, and connected ecosystems?

A 'secure-by-design' industrial enterprise is one where security is embedded into every stage of the digital journey—from strategy and architecture to deployment and day-to-day operations. It is no longer about protecting systems after they are built; it's about designing trust into the enterprise from the very beginning.

In the era of AI, autonomous operations, and connected ecosystems, this means implementing Zero Trust principles, securing both IT and OT environments, ensuring trusted data for AI models, and continuously monitoring for emerging threats. Every connected asset, application, user, and machine identity should be authenticated, monitored, and governed throughout its lifecycle.

Equally important is

When security is embedded from strategy and architecture through deployment and operations, it stops being a roadblock and becomes an enabler of innovation, resilience and business growth.



fostering collaboration between business, engineering, operations, and cybersecurity teams. Security should act as an enabler of innovation rather than a roadblock.

As the industry conversation shifts from vulnerability management to exposure management, how should organizations rethink cyber risk?

The shift from vulnerability management to exposure management represents a fundamental change in how organizations should approach cyber risk. Instead of simply counting vulnerabilities or chasing CVSS scores, organizations need to understand which risks truly matter to the business. A critical vulnerability on a non-essential system may pose far less risk than a moderate vulnerability affecting a business-critical production process or a high-value data asset.

Effective exposure management requires a business-context-driven approach that combines asset criticality, threat intelligence, attack paths, exploitability, identity risks, and potential business impact. Organizations must have complete visibility across IT, OT, cloud, AI platforms, and third-party ecosystems, with continuous monitoring rather than periodic assessments.

Ultimately, cyber risk should be measured in terms of business impact—not just technical severity.

Cyber resilience has become a boardroom priority. How can CISOs position resilience not just as a security objective, but as a core business capability that supports operational continuity, digital transformation, and stakeholder trust?

Today, cyber resilience is no longer just an IT or cybersecurity concern—it is a business imperative and a board-level responsibility. As organizations become more digital and interconnected, the focus must shift from preventing every attack to ensuring the business can



withstand, respond to, and recover quickly from cyber incidents with minimal disruption.

CISOs need to communicate cyber resilience in the language of business—linking it to operational continuity, financial impact, regulatory compliance, customer confidence, and brand reputation.

When cyber resilience is embedded into business strategy, it becomes a competitive advantage rather than a compliance exercise. Ultimately, resilience is not just about surviving disruptions—it's about emerging stronger and more trusted.

How will Agentic AI reshape the role of the CISO and the enterprise architect over the next five years?

Agentic AI will fundamentally transform both the CISO and Enterprise Architect roles from being decision-makers to orchestrators of intelligent, autonomous systems. As AI agents begin to independently analyze data, make decisions, and execute tasks, leaders will need to shift their focus from managing technology to governing AI-driven ecosystems with the right controls, accountability, and oversight.

For CISOs, the challenge will extend beyond securing infrastructure to securing AI itself—ensuring AI agents are trustworthy, explainable, resilient against manipulation, and compliant with evolving regulations. For Enterprise Architects, the focus will be on designing scalable architectures where humans and AI agents collaborate seamlessly, while maintaining interoperability, governance, and business agility.

Over the next five years, success will depend on building AI-ready enterprises with security, ethics, and governance embedded by design. The future role of both the CISO and Enterprise Architect will be to ensure that autonomous intelligence accelerates the business without compromising security, trust, or resilience.

Today's CISO is expected to influence business strategy, regulatory compliance, AI governance, and digital trust. How has the role evolved over the past few years, and what capabilities will define the next-generation security leader?

The role of the CISO has evolved dramatically



over the past few years. Traditionally, the focus was on protecting IT infrastructure and managing security operations. Today, the CISO is a strategic business leader who helps shape digital transformation, AI adoption, regulatory compliance, cyber resilience, and enterprise risk management.

Today's CISO must be equally comfortable in the boardroom and the operations floor—translating complex cyber risks into business language, influencing executive decisions, and aligning security investments with organizational objectives.

The next-generation security leader will combine deep cybersecurity expertise with business acumen, technology vision, risk management, and strong leadership skills.

The CISO is no longer just responsible for protecting infrastructure. The role has evolved into that of a strategic leader who must connect technology, risk, resilience and business priorities to help the organisation transform securely.

As Deepak Fertilisers continues to invest in digital capabilities and operational excellence, how do you ensure that security evolves at the same pace as innovation?

Deepak Fertilisers believes that security should accelerate innovation—not slow it down. As we continue to invest in AI, Smart Manufacturing, cloud technologies, SAP S/4HANA, and Industry 4.0 initiatives, our approach is to embed cybersecurity and enterprise architecture into every project from the ideation stage itself. This ensures that innovation and security progress together rather than in separate tracks.

We have adopted a 'Secure by Design' philosophy, supported by Zero Trust principles, robust governance, continuous risk assessment, and strong collaboration between business, IT, OT, and cybersecurity teams. We also leverage AI-driven security operations, threat intelligence, and continuous monitoring.

Equally important is fostering a security-first culture across the organization. Technology alone cannot secure a digital enterprise—people, processes, and governance are equally critical. By aligning cybersecurity with business strategy, we ensure that every digital initiative delivers operational excellence and strengthens resilience, regulatory compliance, and stakeholder trust.



balaka.baruah@thefoundermedia.in

INTERVIEW

AI IS MOVING CYBERSECURITY FROM RESPONSE TO PREDICTION

Vivek Shankar, CITSO & VP, Axis MaxLife Insurance, talks to **Jeevika Srivastava** about how AI is transforming cybersecurity from a reactive function into a proactive, intelligence-driven capability



How is AI changing the way your organization approaches cybersecurity today?

AI is fundamentally transforming cybersecurity from a reactive function into a proactive and intelligence-driven capability. In the insurance industry, where organizations manage highly sensitive customer, financial, medical, and identity data, the challenge is no longer a shortage of security tools but the ability to detect and respond to threats at scale.

Enterprise AI journey has demonstrated the value of intelligent automation, advanced analytics, and cloud-native platforms across business operations. These same principles are increasingly influencing cybersecurity. AI helps security teams analyse vast volumes of telemetry generated from networks, endpoints, cloud workloads, identities, and business applications, enabling faster detection of anomalies and potential threats.

Ultimately, AI is helping organizations improve cyber resilience by enabling faster decisions, reducing response times, and allowing security teams to focus more on strategic risk management and less on manual investigation.

Where are you seeing the most value from AI in security threat detection, vulnerability management, incident response, or something else?

While AI delivers value across the security lifecycle, the greatest impact today is in threat detection, incident prioritization, and security operations efficiency.

Modern insurance organizations generate millions of security events every day. AI helps correlate information across identity systems, endpoints, cloud infrastructure, email security, and network controls to distinguish genuine threats from normal business activity. This significantly reduces alert fatigue and allows analysts to focus on high-risk incidents.

Another area of growing value is incident response. AI-powered analytics can rapidly summarize attack activity, identify affected assets, recommend containment actions, and accelerate investigations. This is particularly important in the insurance sector, where minimizing response time directly reduces operational and reputational risk. We are also seeing strong value in fraud detection and risk analytics. Going forward, AI's highest value will likely come from combining security, fraud, and business risk signals into a unified risk intelligence framework that helps insurers make faster and more informed decisions.

AI is only as effective as the data behind it. How are you ensuring that the data feeding your security tools is accurate, trusted, and usable?

Data quality is one of the most critical success factors for AI-driven cybersecurity. Inaccurate, incomplete, or poorly governed data can generate false positives, create blind spots, and reduce confidence in automated decision-making.

Our approach begins with strong data governance. Security telemetry from endpoints, networks, cloud environments, identity systems, and business applications must be standardized, validated, and continuously monitored for quality. Equally important is ensuring that data sources are authenticated, time-synchronized, and protected

Enterprise AI journey has demonstrated the value of intelligent automation, advanced analytics, and cloud-native platforms across business operations.



from tampering.The insurance industry operates under stringent regulatory and privacy obligations. Therefore, security datasets must also comply with data protection requirements, retention policies, and access controls. Ultimately, successful cybersecurity AI depends less on algorithms and more on disciplined data governance, strong security controls, and continuous validation of the information feeding those models.

How can AI help security teams move from simply responding to threats to predicting and prioritizing risks before they become incidents?

The real promise of AI is not merely faster response but proactive risk prediction. Traditional security operations focus heavily on events that have already occurred. AI enables organizations to identify patterns, behaviours, and indicators that suggest future risk.

By analysing historical incidents, vulnerability trends, user behaviour, threat intelligence, and asset criticality, AI can identify the conditions that typically precede a security event. This allows security teams to focus preventive efforts on the systems and users that present the highest likelihood of exposure. Advanced analytics and machine learning are already delivering predictive capabilities across underwriting, fraud management, and customer analytics within the insurance industry

The next evolution is predictive cyber defence,

where security teams are able to prioritize vulnerabilities, anticipate attack paths, and mitigate risks before attackers can exploit them. This shift represents a significant step toward a more resilient security posture.

As AI takes on more security tasks, how do you see the role of the CISO and security teams evolving?

AI will not replace cybersecurity professionals; it will elevate their role. As routine monitoring, investigation, and reporting tasks become increasingly automated, security leaders will spend less time managing alerts and more time managing risk.

The role of the CISO and Security Leader is evolving from a technology-focused leader to a business resilience leader. Cybersecurity decisions today influence customer trust, regulatory compliance, operational continuity, and enterprise reputation. Therefore, Leaders must increasingly engage with business leaders, boards, regulators, and technology teams to align cyber investments with organizational priorities. AI governance will also become a major responsibility. As organizations deploy more AI systems, security teams will need to address model security, data integrity, privacy, bias management, and regulatory compliance. For insurers, trust is the foundation of the business. While AI can improve efficiency and scale, maintaining customer trust will continue to require strong governance, transparency, and human accountability.

For the insurance industry, the opportunity extends beyond cybersecurity alone. AI can help unify cyber risk, fraud risk, operational risk, and third-party risk into a single enterprise risk view.

Looking ahead, what do you believe will be the biggest opportunity for AI to transform cybersecurity?

The biggest opportunity lies in creating autonomous and adaptive cyber defence capabilities that continuously learn, prioritize, and respond in near real time. Today's security teams struggle with the complexity of managing thousands of vulnerabilities, millions of events, expanding cloud environments, and increasingly sophisticated adversaries. AI has the potential to become a force multiplier by continuously assessing risk, correlating threat intelligence, predicting attack paths, and recommending mitigation actions before incidents occur. For the insurance industry, the opportunity extends beyond cybersecurity alone. AI can help unify cyber risk, fraud risk, operational risk, and third-party risk into a single enterprise risk view. This would enable organizations to make more informed business decisions while strengthening protection for customers and critical digital assets.

Over the next three years, I believe the most transformative outcome will be the emergence of predictive and largely autonomous security operations that can detect, assess, and contain threats at machine speed, while humans focus on strategy, governance, and business resilience. This combination will redefine how organizations build trust in an increasingly digital world.

In a nutshell, the future of cybersecurity will not be defined by humans versus AI, but by humans and AI working together. Those who can responsibly harness AI to anticipate risk, accelerate response, and enhance resilience will set the benchmark for digital trust in the years ahead. ■

jeevika@thefoundermedia.in

INTERVIEW

DEFENDING AT MACHINE SPEED: HOW AI IS REDEFINING CYBERSECURITY STRATEGY, RESILIENCE AND RESPONSE

In an insightful conversation with **Jeevika Srivastava, Girish Raj Giri, CISO, Goodluck India**, discusses how AI is shifting the balance between cyber attackers and defenders and why organisations must rethink their security strategies for an era of machine-speed attacks



After the recent Anthropic and Mythos developments, is AI giving attackers or defenders the bigger advantage, and why?

From my experience leading IT infrastructure and cybersecurity across manufacturing and defence environments, I believe AI is currently giving attackers a near-term advantage in speed and scalability. Advanced AI models can accelerate reconnaissance, vulnerability discovery, exploit development, and social engineering- activities that traditionally required significant expertise and time.

However, I see this as a race that defenders can still win. AI can transform security operations by enabling continuous threat hunting, faster risk prioritisation, behavioural analysis and automated response.

The key is not simply adopting AI tools, but integrating AI with strong fundamentals such as Zero Trust, identity security, IT/OT segmentation, continuous monitoring, data protection and robust incident response.

Ultimately, attackers may have gained the first-mover advantage, but the organisations that use AI to anticipate, detect and respond faster will gain the long-term advantage.

What is the biggest change CISOs need to make in their security strategy as AI-powered attacks evolve?

The biggest change CISOs need to make is to move from a reactive, control-based security strategy to a continuous, AI-driven, and risk-based security model.

As AI-powered attacks become faster and more adaptive, organisations cannot depend only on traditional perimeter security, periodic assessments, and manual SOC processes. CISOs need to continuously understand their attack surface, identities, data, and IT/OT environments, while using AI for threat detection, threat hunting, vulnerability prioritisation, and faster response.

From my experience, the focus should be on resilience and continuous verification, combining Zero Trust, strong identity controls, segmentation, AI-driven monitoring and tested recovery capabilities.

The objective is simple: detect and respond faster than the attacker can adapt.

As AI agents become capable of making decisions and taking actions rather than simply generating recommendations, where should CISOs draw the line between automation and human oversight?

I believe CISOs should draw the line based on business impact and risk. AI agents can be given autonomy for routine, low-risk activities such as alert analysis, threat hunting, anomaly detection, and initial containment.

However, actions that can significantly impact business operations, such as shutting down critical systems, changing privileged access, modifying OT environments, or deleting data, should remain subject to human approval and clear escalation controls.

In my view, the right approach is “automate wherever possible, but never automate accountability.” AI should accelerate security decisions, while humans retain control over high-impact actions, supported by strong governance, auditability, and a clear ability to intervene.

As AI-powered attacks become faster and more adaptive, organisations cannot depend only on traditional perimeter security, periodic assessments, and manual SOC processes.



Are CISOs prepared for a world where the speed of an attack is measured in seconds rather than hours?

I believe many CISOs are prepared for attacks measured in hours, but AI is forcing us to prepare for attacks measured in seconds. Traditional processes based on manual investigation and response will not be sufficient.

From my experience, organisations need to move towards continuous monitoring, AI-driven detection, automated containment, and well-tested incident response. At the same time, critical decisions must have clear human oversight.

The real challenge for CISOs is therefore not just deploying more security tools, but building an operating model where detection and response happen at machine speed, while governance and accountability remain with people.

The future is not about adding another AI security tool. It is about embedding AI across the security lifecycle while maintaining strong governance and human oversight.

Is AI becoming another layer in the security stack, or is it fundamentally changing how security itself is done?

AI is not simply another layer in the security stack; it is fundamentally changing how security is designed and operated.

From my experience, AI can transform security from a largely reactive model into a continuous, predictive, and adaptive approach, where threats are identified, risks are prioritised, and responses are initiated much faster.

The future is not about adding another AI security tool. It is about embedding AI across the security lifecycle while maintaining strong governance and human oversight.

AI should become an intelligence layer across the security ecosystem, not just another product in the stack.

If AI is powering both attackers and defenders, how will the role of human SOC analyst evolve?

From my experience, the human analyst will remain critical, not because AI cannot analyse data, but because context, business understanding, judgement, and accountability still require human oversight.

The SOC of the future will therefore be human-led and AI-augmented, with machines providing speed and scale, and analysts providing intelligence and judgement. ■



jeevika@thefoundermedia.in

INTERVIEW

REDEFINING TRUST IN DIGITAL FINANCIAL ECOSYSTEM

As financial markets become increasingly digital and interconnected, cybersecurity is no longer just about protecting systems—it is about protecting trust and ensuring continuity. In conversation with **Balaka Baruah Aggarwal, Neehar Pathare, MD, CEO & CIO at 63SATS Cybertech**, discusses how organisations can build resilience in an environment shaped by AI-driven threats, digital identities, third-party dependencies and emerging technologies. He explores what resilience by design means for critical financial infrastructure and why cyber accountability must extend across the entire digital ecosystem.



Financial markets run on trust. In an increasingly digital and interconnected world, how is the definition of trust changing?

Definition of trust in financial markets is evolving. Earlier, trust was built around financial strength, governance and transparency. Today, it also depends on the resilience and integrity of the digital infrastructure that enables every transaction.

Cybersecurity has become a core business and market-stability imperative. A cyberattack can disrupt transactions, compromise sensitive information and erode confidence at a speed that traditional risk models may not fully capture.

For financial institutions, the focus must go beyond preventing breaches to building cyber resilience, detecting anomalies early and responding decisively. This means preparing for the next generation of risks, including the implications of quantum computing for today's encryption standards. In an era of AI-driven threats and hyper-connectivity, cybersecurity is about protecting the confidence on which the financial ecosystem operates.

As critical market infrastructure becomes more automated and interconnected, where are the biggest vulnerabilities emerging?

As critical market infrastructure becomes more interconnected, the most acute vulnerabilities lie at the intersection of third-party dependencies, digital identity and the human element.

Third-Party Dependencies: Modern market infrastructure relies on heavily interconnected supply chains, vendor APIs and cloud services. Security is no longer defined by your own perimeter, but by the weakest link in your extended vendor ecosystem.

Digital Identity: Identity has become a critical security layer as stolen credentials, identity impersonation and compromised digital identities can give attackers access to systems and transactions without needing to breach the underlying infrastructure directly. Protecting digital identity therefore needs to be central to cyber resilience.

The Human Element: Systems may be patched and monitored automatically, but human fallibility remains constant. Credential theft, social engineering, malicious links, suspicious applications and operational misconfigurations can turn individuals into an entry point for sophisticated attacks. This makes mobile cybersecurity particularly important as smartphones increasingly become gateways to financial services and digital identities.

We are entering an era where AI is being used by both defenders and attackers. Do you see AI as primarily an opportunity to build more intelligent and resilient systems?

AI is both a force multiplier for defence and an expanded attack surface, but its greatest strategic value lies in building adaptive resilience.

AI lowers the barrier for adversaries allowing for hyper-personalised social engineering, automated exploitation and adaptive malware. Every AI model, data pipeline and LLM integrated into enterprise IT introduces a new attack vector, from prompt injection to data poisoning.

For defenders, AI is essential to operating at

Modern accountability shifts the focus from asking vendors if they are secure to enforcing verifiable, real-time proof of resilience at every digital interface.



the speed and scale to counter modern threats. Machine learning shifts cyber defence from reactive incident response towards predictive threat hunting, enabling automated, real-time threat detection, anomaly monitoring and faster remediation.

What does "resilience by design" mean to you, particularly for organisations managing highly sensitive data and mission-critical transactions?

"Resilience by design" shifts the cybersecurity mindset from building higher walls to engineering systems that maintain operational continuity during active compromise. It rests on three key imperatives:

Architectural Compartmentalization: Enforcing micro-segmentation and Zero Trust data pipelines

to contain breaches without interrupting high-value transactions.

Data Integrity Verification: Utilizing immutable storage and automated validation to guarantee state-level recovery during destructive or ransomware attacks.

Automated Adaptive Operations: Implementing orchestration that dynamically reroutes critical transaction pathways and isolates threats in real time.

Ultimately, resilience by design transforms security from a perimeter-defence model into a core strategic driver, ensuring mission-critical services survive, operate, and recover instantly under severe shock.

In highly interconnected ecosystems, how should enterprises rethink accountability for cyber risks?

Rethinking cyber accountability in interconnected ecosystems requires moving from traditional vendor risk management to continuous, active risk co-governance. Technically, this means applying Zero Trust architecture universally across organizational boundaries, ensuring external partner connections are treated with continuous, contextual verification rather than implicit trust.

Trust in financial markets increasingly depends on the resilience and integrity of the digital infrastructure behind every transaction.



Legally and commercially, enterprises must structure contracts around shared responsibility frameworks with clear, enforceable resilience metrics and joint incident-response protocols. Ultimately, modern accountability shifts the focus from asking vendors if they are secure to enforcing verifiable, real-time proof of resilience at every digital interface.

Looking ahead, what do you believe will define a truly resilient digital enterprise?

A truly resilient digital enterprise is defined by the seamless orchestration of technology, intelligent security systems, and people and processes that can respond decisively to the unexpected. Robust technology provides the foundation, while intelligent security systems form the organisation's nervous system. This is where solutions like AI CyberOPS by 63SATS Cybertech comes in, integrating AI agents into security operations to streamline detection, investigation and response across the enterprise.

Resilience, however, also extends beyond the enterprise perimeter. As digital interactions increasingly depend on mobile devices and digital identities, protecting the individual becomes an important part of the wider security ecosystem. CYBX, 63SATS Cybertech's cybersecurity super-app for individuals, adds a mobile security layer.

At the same time, enterprises must prepare for threats that are still emerging. Quantum security and quantum-ready approaches will become increasingly important as organisations look to protect sensitive data.■

balaka.baruah@thefoundermedia.in

VIEWPOINT

CYBERSECURITY BEYOND BOUNDARIES: PROTECTING A DIGITALLY CONNECTED INDIA

Atul Pandey, Director – IT and Digital Strategy, Bharat Network Group, explores the evolving security challenges across healthcare, education, communities, manufacturing, retail, and individual users, while highlighting practical measures that can strengthen protection across these interconnected ecosystems.



FROM CITIES to villages, from hospitals to classrooms, cybersecurity has become a shared responsibility.

India's digital transformation is connecting almost every part of society. Businesses are moving to the cloud, hospitals are digitising patient records, schools are adopting online learning, financial transactions are increasingly digital, and rural communities are gaining access to smartphones and digital services.

But greater connectivity also creates greater exposure. Cybersecurity is no longer limited to IT departments or large enterprises. It affects every sector, every organisation and, increasingly, every individual. "The cybersecurity perimeter is no longer an organisation's network. It now includes people, devices, applications, data and every digital interaction."

Healthcare: Protecting Data and Patient Trust

Healthcare organisations hold some of the most sensitive information: patient records, medical reports, identities and financial details.

Cyberattacks can lead to data theft, ransomware, and disruption of critical services.

How to protect it: Hospitals and healthcare providers should implement strong access controls, multi-factor authentication, encryption, regular backups, endpoint protection and continuous security monitoring. Staff awareness is equally important because phishing remains a significant entry point for attackers.

Education: Securing the digital classroom

Schools, colleges and universities increasingly depend on online learning platforms, cloud applications and digital databases. Student information, examination data and institutional systems can become targets for phishing, account takeover, malware and data theft.

How to protect it: Educational institutions should secure student and staff accounts with MFA, regularly update systems, control access to sensitive information, maintain backups and introduce cybersecurity awareness as part of digital education.

Banking and digital payments: Protecting the digital wallet

UPI, mobile banking and digital payments have transformed financial transactions across India.

But fraudsters increasingly use phishing, fake customer-care numbers, fraudulent QR codes, impersonation and social engineering to target users.

How to protect it: Never share OTPs, PINs or passwords. Verify payment requests before approving them, use official banking applications, enable transaction alerts and report suspicious transactions immediately.

"Convenience has accelerated digital adoption. Security must accelerate at the same pace."

Rural India: Digital inclusion must include security

Smartphones and digital services are creating new opportunities for rural communities—from digital banking and agriculture platforms to e-commerce, education and government services.

However, limited cybersecurity awareness, shared devices, online fraud



and language barriers can increase vulnerability.

How to protect it: Deliver cybersecurity awareness in local languages and through practical digital-literacy programmes. Community centres, banks, schools and local institutions can play an important role in teaching safe digital practices.

Small businesses and MSMEs: Small size does not mean small risk

MSMEs increasingly depend on email, cloud applications, digital payments, websites and online accounting.

A compromised password or ransomware incident can potentially disrupt an entire business.

How to protect it: Use MFA, strong and unique passwords, updated software, secure backups, endpoint protection and basic employee cybersecurity training. Businesses should also understand the security practices of their technology and cloud-service providers.

Government: Protecting citizen services

Government departments manage large volumes of citizen, financial and administrative information.

Cyber incidents can disrupt public services, compromise sensitive information and affect public trust.

How to protect it: Government systems require strong identity management, network segmentation, encryption, regular vulnerability assessments, continuous monitoring, tested disaster-recovery plans and trained personnel.

Manufacturing: From IT security to operational security

Modern factories increasingly use connected machines, industrial control systems and IoT technologies.

A cyber incident can therefore move beyond data theft and potentially affect production and operations.

How to protect it: Organisations should separate IT and operational technology networks, control privileged access, continuously monitor industrial systems, maintain secure backups and regularly assess vulnerabilities in connected equipment.

Retail and E-commerce: Protecting customers and transactions

Retailers collect customer information and increasingly depend on digital payments, websites, applications and cloud platforms.

Attackers may target payment systems, customer accounts or business databases.

How to protect it: Use secure payment gateways, MFA, encryption, regular application security testing, access controls and employee awareness programmes.

Individuals and families: The first line of defence

Cybersecurity ultimately reaches the individual.

Convenience has accelerated digital adoption. Security must accelerate at the same pace.

A smartphone can contain banking applications, personal photographs, identity documents, emails, passwords and sensitive conversations.

How to protect it:

- Use strong, unique passwords.
- Enable multi-factor authentication.
- Keep phones and applications updated.
- Avoid suspicious links and attachments.
- Never share OTPs, PINs or passwords.
- Install applications only from trusted sources.
- Review account and transaction alerts regularly.
- Back up important data.

From cybersecurity to cyber resilience

The objective should not simply be to prevent every attack. Organisations and individuals also need to be prepared for what happens when something goes wrong.

A resilient digital ecosystem should be able to:

Prevent-Detect-Respond-Recover-Learn

This requires technology, awareness, governance and preparedness working together.

"Cyber resilience is not about assuming that an attack will never happen. It is about being prepared to respond, recover and continue when it does."

Building a safer digital India

Cybersecurity cannot be solved by one technology, one organisation or one sector.

Governments, businesses, technology providers, educational institutions, financial organisations and citizens all have a role to play.

As India becomes more connected, cybersecurity must become more accessible, understandable and integrated into everyday digital life.

The future of digital India should not only be connected, but it should be secure and resilient.

Whether it is a hospital protecting a patient's records, a school protecting student data, a factory protecting its operations, a business protecting its customers, a farmer using digital payments, or a family using a smartphone, the need for cybersecurity is universal. Cybersecurity has no boundaries. Protecting the digital ecosystem is everyone's responsibility.■

VIEWPOINT

THE NEXT CYBERSECURITY BATTLE WILL BE FOUGHT IN MACHINE TIME

Cdr Praveen Kumar, Group CISO & DPO, Nykaa, explores the dual reality of artificial intelligence in cybersecurity, where the same technology that enables defence at machine speed is also empowering adversaries with unprecedented scale



EVERY FEW years, a technology arrives that forces the security profession to redraw its mental map. Artificial intelligence is that technology today, and it refuses to sit neatly on either side of the ledger. It is at once the most powerful defensive capability we have ever had and the most versatile weapon our adversaries have ever acquired. The honest answer to whether AI is an enabler or a new threat vector is: it is both, simultaneously and permanently. The real question is who operationalises it faster, and with greater discipline.

The enabler: defence at machine speed

For decades, cyber defence has been an asymmetric contest. Attackers need to be right once; defenders need to be right every time, across sprawling estates of cloud workloads, APIs, endpoints and third-party integrations. AI is the first technology that meaningfully narrows that asymmetry.

Modern security operations generate telemetry at a volume no human team can triage. Machine learning models now baseline what "normal" looks like across users, devices and applications, and surface deviations in near real time, spotting the lateral movement, credential misuse or data staging that signature-based tools routinely miss. In consumer internet businesses, where millions of transactions and login events flow every day, this behavioural lens is not a luxury; it is the only way to separate a genuine customer from a bot farm or an account-takeover attempt without degrading the experience of legitimate users.

AI is equally transformative inside the security operations centre. Large language models can summarise incidents, correlate alerts across tools, draft investigation notes and suggest containment steps, compressing tasks that took hours into minutes. This does not replace analysts; it rescues them from alert fatigue and frees scarce talent for judgement-intensive work such as threat hunting and adversary simulation. On the engineering side, AI-assisted code review and secure-by-design tooling are catching vulnerabilities earlier in the development lifecycle, when they are cheapest to fix. Fraud detection, phishing triage, vulnerability prioritisation, identity risk scoring: each discipline is being quietly rebuilt around models rather than rules.

The threat: adversaries have the same toolkit

The uncomfortable symmetry is that everything AI does for defenders, it does for attackers too, often with a lower barrier to entry.

Generative AI has industrialised social engineering. Phishing emails were once betrayed by clumsy grammar; today they are fluent, personalised and generated at scale in any language. Voice cloning and deepfake video have turned "verify by calling the person" into an unreliable control, and business email compromise is evolving into business identity compromise. Malware authors are using AI to write polymorphic code that mutates faster than signatures can be published, and reconnaissance that once took weeks of manual effort can now be automated across a target's entire digital footprint.

We are also seeing the emergence of machine-speed



Fraud detection, phishing triage, vulnerability prioritisation, identity risk scoring: each discipline is being quietly rebuilt around models rather than rules.

attacks: automated agents that probe, exploit and pivot without waiting for human operators. When the attacker moves at machine speed, a defence that depends on human reaction time is structurally beaten before the incident begins.

There is a third dimension that deserves more boardroom attention: AI systems themselves are now part of the attack surface. Enterprises embedding LLMs into customer service, commerce and internal workflows inherit new risk classes: prompt injection, training-data poisoning, model theft, and the leakage of sensitive data through carelessly integrated AI tools. Shadow AI, where employees paste confidential information into unsanctioned public tools, is today's version of shadow IT, and it is spreading faster.

The CISO's mandate: adopt aggressively, govern rigorously

Faced with this dual reality, some organisations respond with paralysis while others rush in without guardrails. Both are

mistakes. The defensible position is aggressive adoption wrapped in rigorous governance.

That means treating AI security as three parallel workstreams. First, security with AI: embedding machine learning into detection, response, and fraud prevention, and measuring it against hard outcomes such as dwell time and mean time to respond. Second, security of AI: red-teaming models before deployment, controlling what data they can access, monitoring their outputs, and applying the same least-privilege principles to AI agents that we apply to human users. Third, security despite AI: hardening people and processes against AI-enabled deception through phishing-resistant authentication, out-of-band verification for financial transactions, and continuous awareness training that reflects how convincing synthetic content has become.

The contest between attacker and defender is becoming a contest between algorithms, refereed by the quality of human judgement on each side.

Crucially, humans must remain in the loop where consequences are irreversible. AI should recommend and accelerate; accountability for high-impact decisions- isolating a production system, blocking a payment channel, disclosing an incident- must remain human. Regulators, including under India's Digital Personal Data Protection regime, will expect nothing less, and boards should demand clear answers on how AI decisions affecting customers are governed, explained and audited.



The verdict

AI has not changed the fundamental nature of cybersecurity; it has changed its tempo. The contest between attacker and defender is becoming a contest between algorithms, refereed by the quality of human judgement on each side. Organisations that treat AI purely as a threat will be outpaced by adversaries who feel no such hesitation. Those that treat it purely as a saviour will automate their own blind spots. The enabler-versus-threat framing, in the end, is a false binary. AI is an amplifier. It amplifies the maturity, or the immaturity, of the security programme it enters. The leaders who win the next decade will be those who pair machine speed with human wisdom, and who understand that in the age of AI, trust is not a by-product of security. It is the product.

FLASHBACK

WHERE VISION MEETS THE FUTURE OF TECHNOLOGY LEADERSHIP

CIO HORIZON 2026, Bharat Network Group's invitation-only leadership conclave, brought together CIOs, CTOs, CISOs, CDOs, technology leaders, industry experts and technology partners for three days of strategic conversations, peer exchange and curated experiences at Ramada by Wyndham Hotel & Convention Center, Lucknow. The second edition focused on the evolving technology landscape, exploring AI-led enterprise transformation, cybersecurity, trusted data, cloud, digital resilience, responsible innovation and the changing role of technology leadership.

Having the theme "Where Vision Becomes Direction," CIO Horizon 2026 opened with a welcome address by Dr. Ashish Srivastava, Founder & Director, Bharat Network Group, setting the tone



Lamp Lighting Ceremony at the inauguration of CIO Horizon 2026: *(L to R) Atul Pandey, Director – IT & Digital Strategy, Bharat Network Group; Dr. Ashish Srivastava, Founder & Director, Bharat Network Group; Dr. Anupam Gupta, Founder & Director, Bharat Network Group; Rajnish Gupta, MD & Country Manager – India Region, Tenable; Prarthana Gupta, Founder & CMD, Cache Digitech | Vyuhai.ai.*

for three days of strategic dialogue and technology leadership.

The ceremonial lamp lighting, joined by senior leaders and industry partners, was followed by the unveiling of the latest edition of Tech Disruptor Media Magazine. The opening session also featured the introduction of the myBNG App by Atul Pandey, Director – IT & Digital Strategy, Bharat Network Group, highlighting its role in enabling engagement, networking and interaction throughout the conclave.

Following the inaugural address, leaders from the IT industry took the stage for a series of insightful keynote presentations, sharing perspectives on AI, cybersecurity, cloud transformation, compliance and emerging enterprise



Dr. Ashish Srivastava, Founder & Director, Bharat Network Group



Atul Pandey, Director – IT & Digital Strategy, Bharat Network Group



Keynote Session by Trisha Sinha Roy, Regional SE- India West, Tenable



Keynote Session by Vivek Thomas, Quantarra



Keynote Session by Achin Aggarwal Arista Networks



Keynote Session by Hanuman Kamma, SharpSell.ai



Keynote Session by Jinen Dedhia, DronaHQ



Keynote Session by Rohit Sawhney, Fortinet



Panel 01: *Anand Deodhar, Group CIO, Force Motors; Kiran Komatla, Group CTO, Restaurant Brand Asia (Burger King); Sudhir Kanvinde, CIO, The Supreme Industries Ltd; Ravi Kumar, CDIO, Exide Industries Limited; Umesh Mittal, CIO, Everest Food Products Pvt Ltd; Sandip Pradhan, Chief Digital and Information Officer, Century Plyboards (I) Limited.; Upkar Singh, CIO, Paradeep Phosphates (Moderator)*

technologies. The sessions brought practical industry insights to the conclave, highlighting how organisations can navigate evolving technology landscapes while building secure, resilient and future-ready businesses. After the industry presentations, the conclave moved into the first panel discussion on "How AI is Redefining Business, Leadership, and Competitive Advantage in the Intelligent Enterprise," bringing together senior technology leaders to explore the growing influence of AI on enterprise strategy, leadership, decision-making, and business transformation. The discussion offered diverse industry perspectives on moving from AI experimentation to meaningful enterprise adoption and long-term value creation. The conclave moved into the second panel discussion on "From Chaining of Vulnerabilities to Chaining of Strengths: The Quest for Security," bringing together



Panel 02: *Sendil Kumar V, CTO, Shriram Capital; Dr. Shakti Goel, Chief Data and Analytics Officer, Yatra; Satish Pengal, VP-IT, Upstox; Ayaskant Mohapatra, CIO, BOB Financial Solutions Limited; B Sekhar Rao, Founder & CEO, Ashield; Ankit Goenka, Senior VP – Strategy & Transformations, Bajaj General Insurance; Chitti Babu Atreyapurapu, Group CIO, Aurobindo Pharma Ltd. (Moderator)*



Panel 03: *Krupasindhu Roul, CIO & Head IT, Tube Investments of India Limited; Manjunath Prasad, Head IT, TVS Mobility Pvt Ltd; Dr. Kalyana Chakravarthy, VP – Technology, GRT Jewellers India; Manoj Kumar, Group CIO, Shyam Steel Industries Ltd; Pushkar Rege, CIO, UPL; Shobhana Lele, CIO, Bombay Dyeing; Hanuman Kamma, Co-Founder & CEO, Sharpsell.ai.; Yogesh Zope, CIO, Bharat Forge Ltd. (Moderator)*

senior technology and security leaders to examine the evolving cybersecurity landscape, interconnected vulnerabilities and the need for stronger organisational resilience. The discussion explored how enterprises can strengthen their security posture through collaboration, proactive risk management and coordinated defence strategies.

The conclave then featured the third panel discussion on "From Managing Technology to Building Capability Driving Innovation: Why Capability Building is Becoming a CIO Imperative," bringing together technology leaders to discuss the growing importance of talent, skills and organisational capabilities in driving sustained digital innovation. The conversation highlighted how CIOs



Panel 04: *Sanjay Mishra, Group CDIO, Jindal Stainless; Sandeep Dewangan, President & Group CIO, Safexpress Pvt. Ltd.; Abhijeet Bhattacharjee, CIO, Utkarsh Small Finance Bank; Ravi Shankar Srivastava, CIO, Patanjali Foods Ltd - Ruchi Soya; Priya Dar, CIO, Valvoline Cummins; Dilip Kant Jha, CIO, SLMG Beverages; Vinod Bhat, Chief Digital Officer, TATA AutoComp Systems Ltd.; Vamsi Krishna Ithamraju, CDIO, TeamLease; Avadhut Parab, CIO, Waaree Group; Meheriar Patel, Group CIO, Master Group (Moderator)*

are increasingly focused on building adaptable teams and capabilities that can support emerging technologies and evolving business priorities.

The exclusive roundtable explored the transition from AI experimentation to the practical deployment of AI agents across enterprise workflows. Discussions focused on the emerging possibilities of agentic AI, automation, governance and the ways organisations can integrate intelligent systems into their operations while maintaining appropriate human oversight.

The fourth panel discussion focused on "Trusted Data Foundations: The Backbone of AI-Driven Enterprises," bringing together senior technology leaders to examine the role of reliable, secure and well-governed data in enabling enterprise AI. The discussion explored data quality, governance, accessibility and trust as organisations work to build strong foundations for AI adoption, intelligent decision-making and digital transformation.

The exclusive roundtable explored the transition from AI experimentation to the practical deployment of AI agents across enterprise workflows. Discussions focused on the emerging possibilities of agentic AI, automation, governance and the ways organisations can integrate intelligent systems into their operations while maintaining appropriate human oversight.

The fourth panel discussion focused on "Trusted Data Foundations: The Backbone of AI-Driven Enterprises," bringing together senior technology leaders to examine the role of reliable, secure and well-governed data in enabling enterprise AI. The discussion explored data quality, governance, accessibility and trust as organisations work to build strong foundations



RoundTable



Fireside chat: *Kartikeya Raman, Partner, Grant Thornton Bharat; Ramesh Narayanaswamy, Group President – Digital & Data Intelligence, Hinduja Group Limited.*



Game set match



Felicitation

for AI adoption, intelligent decision-making and digital transformation.

The fireside conversation examined the relationship between AI, data intelligence, digital transformation and enterprise growth. It brought a broader strategic perspective to the event, highlighting how technology leadership is increasingly connected with business priorities and long-term organisational readiness.

The CIO Recognition & Felicitation Ceremony celebrated technology leaders for their contributions to digital transformation and collaborative excellence. The BNG Leadership Rewards Ceremony, powered by the myBNG App, added another dimension to the recognition programme by acknowledging leaderboard champions.

Beyond the formal sessions, CIO Horizon 2026 placed strong emphasis on meaningful interaction and relationship-building. Mix and Meet, Game–Set–Match, networking breakfasts, hi-tea and evening gatherings provided participants with opportunities to continue conversations beyond the conference floor. The experience was further enriched by Raga Ki Sufi Shaam, bringing together music, dinner and networking, while the specially curated Ayodhya Dham experience offered pre-registered CIOs a distinctive conclusion to the residential programme.■



Mix and meet



Raga Ki Sufi Shaam

YOUR BRAND DESERVES A BOOTH THAT GETS NOTICED.



A great booth doesn't just occupy space.
It **attracts. Engages. Communicates. Converts.**

• • • • •

With **BOOTHIFY**, transform your exhibition space into a powerful brand experience.

OUR EXPERTISE:

- Exhibition Booths
- Custom Fabrication
- Branding & Signage
- Experience Zones
- Conference Setups
- AV & Event Infrastructure
- End-to-End Execution

You bring the brand.

BOOTHIFY

— Design. Build. Experience. —

We build the experience.

Let's Build Your Next Crowd Magnet Today!

For queries, contact –
Ankur Srivastava

Mobile
+91 79820 32246

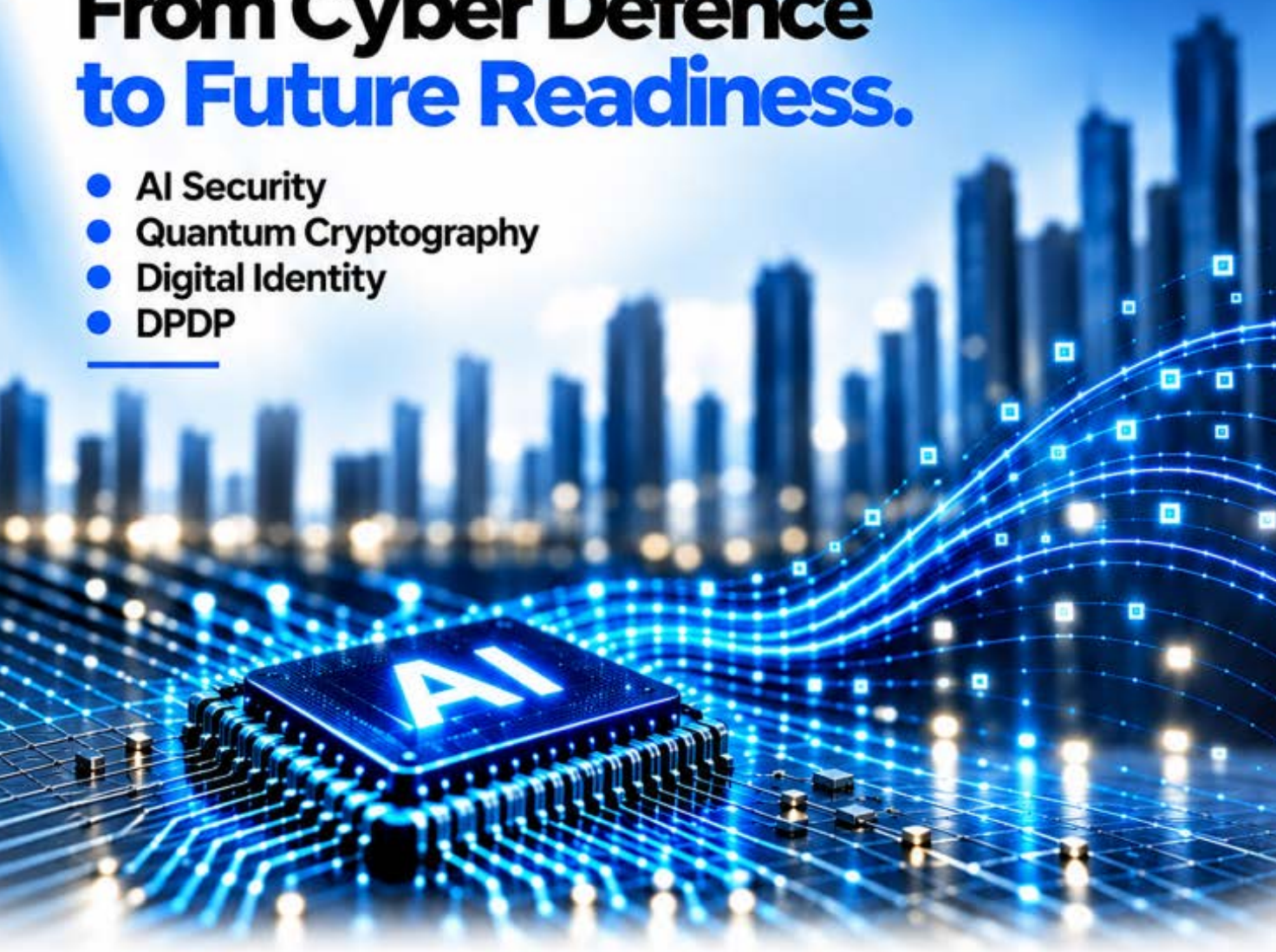
Email ID
ankur@bharatnetworkgroup.com

www.boothify.in

63 SATS™ Cybertech

From Cyber Defence to Future Readiness.

- AI Security
- Quantum Cryptography
- Digital Identity
- DPDP



HOW WE PROTECT INDIA'S AI ECOSYSTEM

- Outcome Focused
- End-to-End Capabilities
- Expertise that Delivers
- Trusted by Enterprises
- Innovation with Purpose
- Built for Scale

Speak to Our Experts

info@63sats.com | +91 84338 98971

63SATS CyberTech Limited

A Trusted Cybersecurity Partner for a Safer, Stronger India.

Made for India.
Securing a Brighter Tomorrow.

Scan now to know more

Vyuha.ai

INTELLIGENCE. ORCHESTRATED.

A Dell OEM Solutions Partner

FROM POSSIBILITIES TO REAL IMPACT

Enterprise intelligence for a smarter, more connected tomorrow.

- Automate **TODAY**
- Orchestrate **TOMORROW**
- Empower **PEOPLE**
- Accelerate **POSSIBILITIES**



Turn AI agents into coordinated enterprise action **with Vyuha.ai**

A Cache Digitech Comany

Explore what's possible at

www.vyuha.ai | sales@vyuha.ai →