Netpoleon

BHARAT CXO DRIVE



Journey of Completing "N" on the Map.

A Stronger Netpoleon Footprint Across India's CXO Community.

Edition OND012026.
A CXJ Production

CXO® JUNCTION

BHARAT CXO DRIVE

Every organisation must defend its own digital frontier. But the future of cybersecurity cannot be secured in isolation.

As businesses embrace AI, accelerate digital transformation, and become increasingly interconnected, the responsibility of protecting the enterprise has grown far beyond technology. Cybersecurity leaders are expected to anticipate what lies ahead, make decisions amid uncertainty, and balance innovation with resilience. The challenges may differ from one organisation to another, but the underlying responsibility is shared across the industry.

And sometimes, the most valuable progress begins when leaders step beyond their own organisations to exchange ideas, share experience, and see familiar challenges through a different lens.

That is the thinking behind Bharat CXO Drive, a five-month, 12-city journey by Netpoleon India, in partnership with CXO Junction, created to bring India's cybersecurity leadership community closer.

Bringing together CISOs, CIOs, CTOs, and senior cybersecurity and technology decision-makers, the initiative creates opportunities for meaningful peer engagement through exclusive CXO roundtables, practitioner-led technical discussions, and the Red vs Blue cybersecurity challenge. Each brings a different dimension to the experience: strategic dialogue among decision-makers, practical knowledge from the field, and an opportunity to recognise the skills and thinking behind cyber defence.

For business and technology leaders, these developments demand more than awareness of emerging tools. They require an understanding of where innovation creates value, how security priorities align with business objectives, and what it takes to build capabilities that can evolve alongside the threat landscape.

Bharat CXO Drive brings these considerations into a shared forum. By connecting strategic leadership with technical expertise and industry experience, it encourages a more open exchange of perspectives, creating space for new ideas, informed debate, and learning that extends beyond organisational boundaries.

This magazine brings those people, ideas, and experiences into focus.

Within these pages, readers will discover stories and insights emerging from the Red vs Blue challenge, celebrating the expertise and achievements behind the competition. Industry perspectives and partner contributions broaden the conversation, exploring the technologies, strategic considerations, and emerging developments influencing the future of enterprise cybersecurity.

Bharat CXO Drive is helping create that momentum, connecting the people and perspectives shaping the conversation today while contributing to the vision of a more secure digital tomorrow.

Different perspectives. Collective intelligence. A stronger cyber future for India.

EDITOR'S NOTE

At CXO Junction, we believe meaningful conversations have the power to build stronger communities and shape the future of industries.

Bharat CXO Drive, in partnership with Netpoleon India, brought this belief to life through an engaging platform for India's cybersecurity and technology leaders to connect, share experiences, and explore new perspectives.

By combining exclusive roundtable discussions, technical insights, and the Red vs Blue challenge, the initiative created an experience that went beyond traditional industry events.

For us, this journey represents the value of collaboration and the importance of creating spaces where leaders can learn from one another.

I extend my sincere appreciation to Netpoleon India, the participating CXOs, and everyone who contributed to this initiative.

Here's to stronger partnerships, meaningful conversations, and a more connected cybersecurity community.

Mohinee Singh

Warm regards,

CEO, CXO Junction



TABLE OF CONTENT









The Netpoleon Story 02

History, Evolution & Future

Behavior Intelligence 08

For the Agentic Enterprise, by Exabeam

Voices of Impact 10

Red Team

Beyond the Pilot 22

Making Agentic AI Accountable, by BMC Helix

Voices of Impact 23

Blue Team

CXO JUNCTION



NETWORK.
EXPLORE.
MAKE THE CHANGE.

- 10,000+ Enterprise Leaders connected
- Strategic Tech Media & Executive PR
- Closed- Door Executive Forums
- Flagship Event Series across India

CONNECT WITH OUR TEAM

Info@cxojunction.com

+91 83 6090 9060

www.cxojunction.com

Follow us at

HISTORY OF NETPOLEON

THE NETPOLEON STORY

OUR HISTORY, EVOLUTION & VISION FOR THE FUTURE



01 THE BEGINNING IN SINGAPORE

Netpoleon's journey began in Singapore in 2000, founded by Francis Goh as a value-added systems integrator.

As the technology landscape evolved, so did the company. By 2006, Netpoleon had transformed into a Value-Added Distributor (VAD), with a growing focus on network and cybersecurity technologies.

But distribution was never just about moving products.

Netpoleon built its value around expertise technical knowledge, pre-sales capability, architecture design, proof of concepts, implementation, migration, training and post-sales support.

02 FROM SINGAPORE TO APAC

As cybersecurity became business-critical, Netpoleon expanded across Asia-Pacific, establishing operations in Singapore, Australia, India, Indonesia, Malaysia, Vietnam, Thailand, the Philippines, Cambodia, Myanmar and New Zealand.

Its role evolved into connecting global technology with local market knowledge, technical capability and channel execution.

A key milestone came in 2017, when Macnica Networks Corporation entered into an equity partnership with Netpoleon, connecting its growing APAC presence with a broader international technology ecosystem.

03 REDEFINING "VALUE ADDED"

Today, enterprises don't suffer from a lack of cybersecurity technologies. In many cases, they face the opposite problem, too many tools, too much complexity and too little clarity. That has changed what customers and partners need from a distributor. Netpoleon has evolved from providing technology availability to technology enablement, helping partners understand, position, demonstrate, implement and support technologies across cloud security, identity, SASE, OT/ICS, SIEM, data security, threat intelligence, CNAPP and observability. Throughout that evolution, one thing has remained central: the channel. Netpoleon's model is built around enabling partners with technology, expertise and services while helping global cybersecurity companies navigate diverse regional markets.

> "**The product mattered.What happened around the product mattered just as much.**

THE PHILOSOPHY REMAINED SIMPLE:

- Find strong technologies globally.
- Build capability locally.
- Enable partners.
- Solve real enterprise problems.

KEY HIGHLIGHTS & MILESTONES

A JOURNEY OF GROWTH, PARTNERSHIPS AND POSSIBILITIES



2000
THE BEGINNING
Founded in Singapore by Francis Goh, beginning its journey as a value-added systems integrator.



2006
BECOMING A VAD
Transformed into a Value-Added Distributor, sharpening its focus on network and cybersecurity technologies.



2017
GOING GLOBAL
A strategic equity partnership with Macnica Networks Corporation opens a new phase of international growth and strengthens the connection to the global technology ecosystem.



2017
ENTERPRISE RECOGNITION
Received the KPMG Enterprise 50 Award, marking its growing business presence in Singapore.



2019–2021
EXPANDING APAC FOOTPRINT
Continues its regional expansion, including Australia and New Zealand, building a broader APAC presence.



2023–2024
GROWING INDUSTRY RECOGNITION
Recognition includes Aruba's EdgeConnect Distributor of the Year for India and becoming the first Infoblox Diamond Distributor in Asia Pacific.



2025–2026
A BROADER TECHNOLOGY ECOSYSTEM
Expands across areas such as cloud-native security, Zero Trust, data observability and AI-driven IT operations through new strategic partnerships.



2026
REGIONAL EXCELLENCE
SailPoint Distributor of the Year – India 2026, Nozomi Networks' APJ Cross Border Distributor of the Year for the third consecutive year, and Exabeam's Distributor Dedication Award.



2026
A NEW LOOK, THE SAME EVOLUTION
A refreshed brand identity, marking another chapter in its growth across the region.



TODAY
FROM DISTRIBUTION TO ENABLEMENT
Operates across major APAC markets, combining global cybersecurity technologies with certified engineering, architecture, implementation, training and 24/7 technical support.

Orchestrating Symphony

of technology for Indian Enterprises

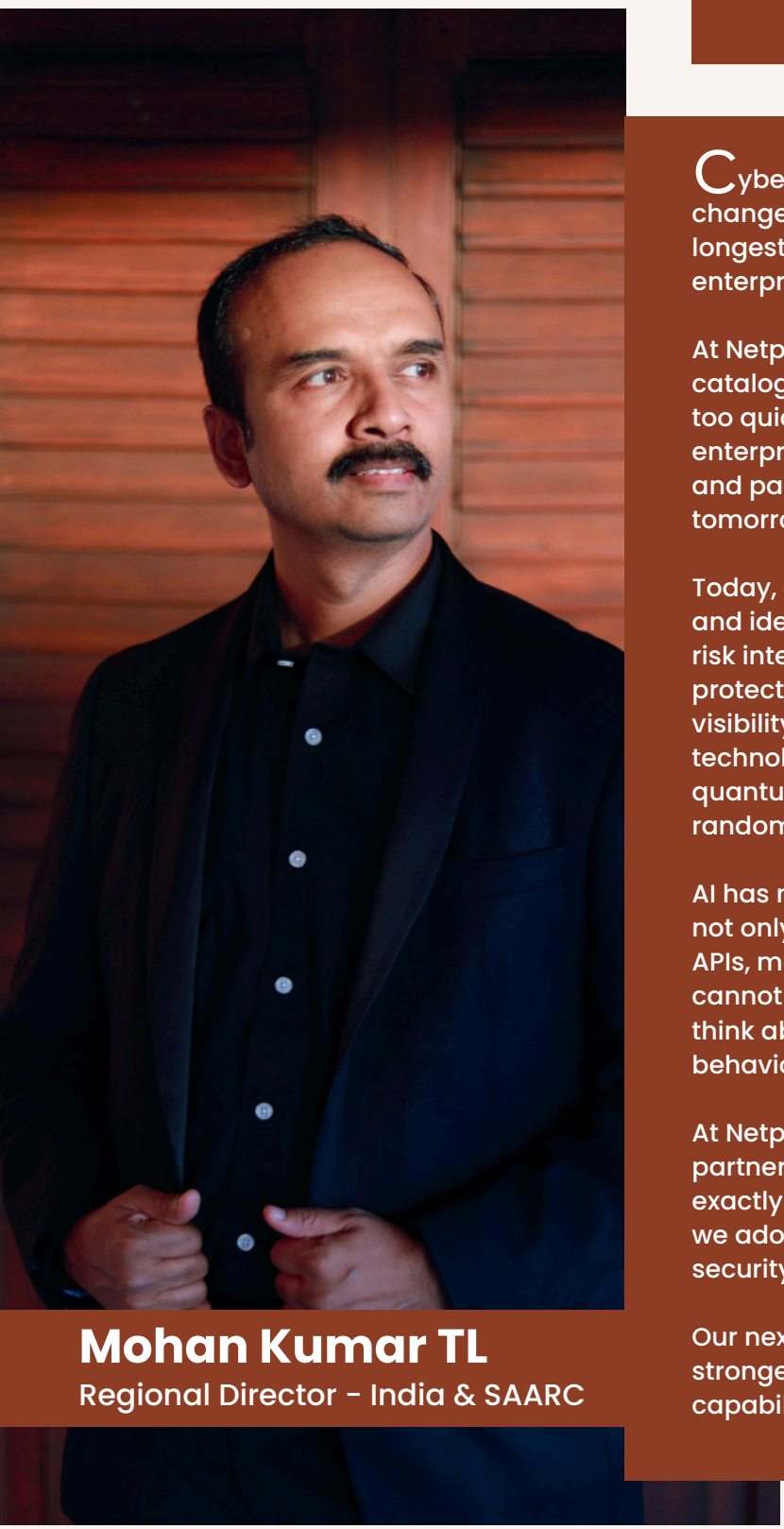


- Identity Security
- NG-SOC & Threat Intel
- Email & Data Security
- OT & IoT Security
- Monitoring, Asset Mgmt.
- Assessment
- DevSecOps & App Sec

in.sales@netpoleons.com

netpoleon

I don't think India needs another cybersecurity distributor.
*It needs a **technology translator**.*



Mohan Kumar TL
Regional Director - India & SAARC

Cybersecurity distribution has and continues to change. The winners will not be the companies with the longest product list, but the ones that understand what enterprises currently need and will need next.

At Netpoleon India, we have never wanted to become a catalogue of cybersecurity logos. Technology changes too quickly for that. Our role is to understand where enterprise risk is moving and bring the right tech, skills, and partners together before that risk becomes tomorrow's emergency.

Today, our ecosystem spans across privileged access and identity security, continuous asset assurance and risk intelligence, DNS and network security, SIEM, OT/ICS protection, cloud-native and Zero Trust security, n/w visibility, AI-driven IT operations, and quantum-safe technologies such as post-quantum cryptography, quantum key distribution and quantum-generated randomness.

AI has now changed the conversation. Enterprises are not only using AI; AI is beginning to access data, call APIs, make decisions and act. That means AI security cannot become another product checkbox. We need to think about identity, permissions, data exposure, agent behaviour, network context and governance together.

At Netpoleon India, we are building conversations, partner capability and technical expertise around exactly this shift helping customers move from "How do we adopt AI?" to "How do we adopt AI with complete security?"

Our next chapter will be about deeper engineering, stronger professional services, more AI-security capability and a sharper Centre of Excellence.

ONE NATION. SHARED MOMENTUM

STARTING FROM WEST INDIA, THE JOURNEY BEGAN....








1 PUNE

2 MUMBAI

3 AHMEDABAD

4 JAIPUR

5 DELHI

6 LUCKNOW








7 HYDERABAD

8 BENGALURU

9 CHENNAI

10 MUMBAI BFSI

11 BENGALURU 2.0

12 COCHIN

UNITED BY VISION. DRIVEN BY PROGRESS.

AFTER 6 MONTHS, THE JOURNEY IS COMPLETED IN THE SOUTH REGION.

exabeam

Behavior Intelligence for the Agentic Enterprise

Secure humans and agents. Accelerate security operations.



Security Starts with Behavior

Organizations are entering a new era where AI agents, digital assistants, and autonomous systems operate alongside human employees, transforming how work gets done. These digital workers act at machine speed — accessing data, invoking APIs, and making decisions — unlocking productivity while introducing a new class of insider risk. To keep pace, security teams need a combination of human insight and digital-speed behavior intelligence to monitor, govern, and secure this evolving workforce while simultaneously leveraging its power for accelerated security operations.

Whether it's insider threat defense for users and agents, securing AI adoption across your enterprise. or advanced threat detection, investigation, and response (TDIR) powered by AI and automation, Exabeam has you covered.

Stop insider threats — human and AI

Monitor behavior of both employees and AI agents to gain visibility into this new class of insider threat. User and entity behavioral analytics (UEBA) and Agent Behavior Analytics (ABA) automatically baseline activity, exposing anomalies that signal an actionable threat.

Outsmart AI-driven attacks

Detect, understand, and outpace AI-driven attacks with context and precision. AI-powered detections and automated timelines reveal threats in progress, while intelligent prioritization ensures teams focus on what matters most — even as attackers evolve at machine speed..

Accelerate results with human + AI teaming

Automate and accelerate threat detection, investigation and response (TDIR). An integrated team of AI agents streamlines the entire TDIR workflow, from enriching threat data to building evidence-backed timelines. Experience faster and more precise investigations, increasing team productivity.

Deliver measurable outcomes-driven security

Benchmark and prove the value of your security program against peers and quantifiable outcomes. Translate raw security data into business-relevant insights to demonstrate progress against your most strategic use cases, MITRE ATT&CK TTPs, and compliance initiatives.

Get unmatched choice and flexibility

Maximize your investment in best-of-breed security tools using the industry's most open and integrated platform. Establish a unified view of your security operation without getting locked into a proprietary scheme and control costs with advanced data pipeline management that allows you to search data in place and leverage low-cost storage. We have deployment options for every environment — in the cloud, on premises, or hybrid.

The Leading Platform for AI-Powered Security Operations

The New-Scale Security Operations and LogRhythm SIEM Platforms protect against insider threats across all identities, deliver unrivaled detection capabilities, and optimize security operations by automating TDIR workflows with AI.

New-Scale Fusion

Highly scalable and easy-to-manage cloud-native SIEM enabling AI-powered insights to automate TDIR workflows, fuel use cases, and deliver unrivaled detection capabilities. The most complete New-Scale offering.

New-Scale Analytics

Cloud-native, AI-powered analytics and automation, delivering unrivaled detection capabilities to support the most strategic use cases. Works with New-Scale SIEM and other third-party SIEM products.

New-Scale SIEM™

Highly scalable and easy to manage cloud-native SIEM.

LogRhythm Intelligence™

Hybrid delivery of machine learning-based AI to the LogRhythm SIEM Platform.

LogRhythm SIEM

Scalable, feature rich, and easy-to-use self-hosted SIEM platform delivering organizations maximum control over their data.

NetMon

Real-time visibility into network traffic that strengthens threat detection, investigation, and response against advanced attacks and provides insight into black box AI and agentic systems. Available on the New-Scale and LogRhythm SIEM Platforms.

Recognized for Leadership and Innovation

As a recognized industry leader, our continued innovation is valued by more than 3,000 enterprises worldwide. Customers rely on Exabeam as their trusted partner to modernize security operations and effectively address the new landscape of cyber threats.

Exabeam Named a Leader: 2025 Gartner® Magic Quadrant™

Exabeam is proud to be named a Leader in the 2025 Gartner® Magic Quadrant™ for Security Information and Event Management. This marks the sixth time Exabeam has been recognized as a Leader. (2018, 2020, 2021, 2022, 2024, 2025)

Gartner continues to acknowledge Exabeam strengths such as user experience, pre-built dashboards, real-time data, and alert prioritization.

Select Awards and Recognition



Gartner, Magic Quadrant for Security Information and Event Management, [Andrew Davies, Eric Ahlm, Angel Berrios, Darren Livingstone, 8 October 2025]. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. This graphic was published by Gartner, Inc. As part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Exabeam. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR).

exabeam™

Learn more at www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2026 Exabeam, LLC. All rights reserved.

RED

OFFENSIVE SECURITY



INSIDE THE CHALLENGE

CXOs simulated real-world attacks to uncover vulnerabilities and test security defences.

WHAT WAS PUT TO THE TEST?

- **Vulnerability Discovery**
  Identifying security gaps.
- **Attack-Path Analysis**
  Tracing attacker movement.
- **Privilege Escalation**
  Exposing access weaknesses.

THE RED TEAM MINDSET

Find the weakness.
Follow the attack.
Challenge the defence.

WINNERS'

VOICES OF IMPACT



Securing the Software Supply Chain:

Moving from Reactive Defence to Continuous Risk Reduction

Traditional software security is trapped in a reactive loop , treating supply chain defence as a binary pass/fail gate right before deployment. This point-in-time scanning model is fundamentally broken. It ignores "The Dependency Debt Paradox," leaving CISOs blind to downstream vulnerabilities and developers drowning in the noise of theoretical, unreachable risks.

My article challenges this status quo by introducing a practical blueprint for Continuous Risk Reduction. arbitrary severity scores. By shifting from defensive firefighting to autonomous integrity, we stop treating security as a friction-filled blocker and transform it into a high-velocity business accelerator that builds undeniable customer trust.

The era of reactive firefighting must end. As CISOs, we can no longer afford to spend our weekends chasing downstream ghosts in code we didn't write. By building hermetic, ephemeral, and self-verifying pipelines, we don't just reduce risk—we reclaim our time, restore our sanity, and turn security into a quiet, unstoppable engine of business velocity

PARTH TRIVEDI

CISO

Bosch Global Software Technologies

> ***True resilience is not achieved by building taller walls, but by establishing cryptographic code provenance, deploying hermetic and ephemeral build pipelines, & prioritizing remediation based on live exploitability rather than arbitrary severity scores.***

WINNERS'

VOICES OF IMPACT



From Data Governance to Data Security:

Turning Visibility into Action

RAJIV MEHTA

AVP Head Data Governance & Technology

Adani Enterprises Ltd.

Data is a strategic business enabler that drives innovation, powers AI, and creates competitive advantage. Do we know what data we have, where it is, who can access it, and how well it is protected?

Visibility Is Only the Beginning

Discovery, classification, and ownership build a foundation, but visibility alone does not prevent a breach. Excessive privileges, exposed files, and unauthorized data movement leave governance disconnected from security. Value appears when visibility becomes measurable action.

Governance defines how data is managed; security protects it. Connect the two across five dimensions:

1. Discover and classify: Continuously find data across cloud, SaaS, and endpoints, classifying by business impact.
2. Connect sensitivity with access (IAM, IGA, PAM): The right identity, access, purpose, and time.
3. Convert visibility into preventive controls (encryption, DLP): Findings should trigger defined responses, from restricting access to tracking remediation.
4. Integrate detection and response (SOC, SIEM): Correlating classification, identity, and behaviour exposes threats like a compromised account exfiltrating files.
5. Measure outcomes (KPIs): Track classification coverage, excessive access, remediation timelines, and time to contain incidents.

Automation and AI accelerate discovery, detection, and remediation, but errors, false positives, and AI processing of sensitive data add risk, so they need risk-based policies, human oversight, and clear ownership.

Resilience

Understand, assess, prioritize, enforce, and optimize, starting with the exposures that matter most. Data security is not solely an IT responsibility; business, technology, security, privacy, legal, risk, and audit teams must collaborate.

Plan a 12-18 month move to Optimized maturity: ownership, classification, and access (0-6 months); compliance, monitoring/DLP, and incident response (6-12); automation, Zero Trust, and real-time compliance (12-18). Also, shortlist solution partners by priority and cost-benefit, piloting to win budget.

Every insight should lead to action, every exposure should have an owner, and every intervention should reduce business risk.

WINNERS'

VOICES OF IMPACT



NARENDRA KUMAR SHARMA

CIO

Delhi Police
(Ministry of Home Affairs)

Cybersecurity at the Front Line:

Protecting Critical Public Infrastructure

As nations accelerate digital transformation, cybersecurity is vital to Critical Public Infrastructure, including power grids, healthcare platforms, and transport systems. In emergency, disaster response, and public safety operations, cyber incidents can directly threaten citizen safety and operational continuity.

Real-World Impact: The AIIMS Delhi Ransomware Attack

The November 2022 ransomware attack on AIIMS New Delhi demonstrated how a cyber incident can quickly become a patient-safety crisis. It disrupted the e-Hospital system, affecting outpatient registrations, appointments, billing, and laboratory services, forcing manual operations for nearly two weeks. Five servers containing records associated with 3–4 crore patients were affected, disrupting access to critical medical information and reportedly contributing to treatment delays and rescheduled surgeries. This incident highlights that cybersecurity is not just about data protection; it is essential for clinical continuity and human lives.

Delhi Police IT/IoT Security Case

An unusually large volume of data was transferred from the department's network to an external destination. An investigation established that attackers had infiltrated the environment and stolen sensitive information. A joint response team comprising the Security Operations Centre (SOC), IT Security, Cyber Crime, Intelligence, and Police Operations was established. An IT-based Exposure Analysis Engine and correlation service were activated to identify and address the threat. Communication between internet-facing services, corporate IT, police operational applications, investigation systems, and restricted intelligence databases was controlled to prevent unrestricted access.

Mitigating Modern Threats

As OT, cloud, and 5G networks converge, AI-driven attacks, phishing, supply-chain breaches, ransomware, SCADA manipulation, and denial-of-service threats are increasing. Protecting these systems requires asset visibility, continuous monitoring, and regular patching. A Zero Trust Architecture strengthens security through multi-facor authentication, least-privilege access, encryption, network segmentation, and immutable backups.

WINNERS'

VOICES OF IMPACT



MAKSOOD AHMAD SIDDIQI

HEAD IT & IS

MARGSOFT Technologies (P) Ltd.

Cloud, Connectivity and Control:

The Security Priorities of a Growing Technology Enterprise

There was a time when securing a company's technology was relatively straightforward. You knew where the servers were, which devices belonged to the organization, and most employees worked from an office connected to the corporate network. A firewall at the edge and a few layers of endpoint protection provided a reasonable sense of where the security boundary was. And every new connection, application or cloud service introduces another question about security.

Cloud has changed almost everything
The more useful question is: who has access to what, and why?

Strong authentication, multi-factor authentication, sensible access permissions, protection of privileged accounts and regular reviews of user access are no longer optional extras. Microsoft's 2025 Digital Defence Report found that 97% of the identity attacks it observed were password-spray attacks.

Connectivity brings opportunity, and exposure
A company's security posture is increasingly influenced by organizations it does not own. The 2025 Verizon Data Breach Investigations Report examined more than 22,000 security incidents and 12,195 confirmed breaches across 139 countries. Third-party involvement appeared in 30% of breaches, twice the previous year's level.

Trust cannot simply be assumed
The principle is actually quite practical: don't give someone broad access simply because they are connected to the corporate network. Security is not just about keeping attackers out. It is also about limiting the damage when someone gets in.

Control means knowing what is happening
It is difficult to protect systems that the organization does not know it has.

Eventually, something will get through
The real test of an organization is what happens next. The World Economic Forum's Global Cybersecurity Outlook 2026 found that only 19% of organizations surveyed said their cyber resilience exceeded their minimum requirements.

Then came AI
Cmpanies need to know what AI tools are being used, what information they can access and who remains accountable for their actions.

In the end, cybersecurity is not about protecting technology for its own sake. It is about protecting the trust, continuity and freedom to grow that technology makes possible.

WINNERS'

VOICES OF IMPACT



GIRISH KUMAR M N

BISO- SENIOR DIRECTOR CYBERSECUTIY

UNISYS

Securing Connected Engineering Environments:

The Convergence of IT, OT and Cyber Resilience

A gentle disclaimer on these views being based on 3 decades of my personal experience in IT, Information/Cyber Security at multiple layers of the Organization (System Administrator to C Level).

Rewinding 3 decades ago, Security Guard was most commonly known to be at the entry/exit gate to fast forward to have Security Leaders having a seat at the Board level meetings. This change has mainly occurred due to the everchanging technology resulting in enhanced Threat Landscape that requires Management investment and attention.

I usually state "Common Science still a priority for effective Cyber Science and now AI Science". While AI/ML and Quantum Computing are bringing digital civilizational shift that requires changes the approach from Architecture, Frameworks to all processes/controls. The Fundamentals still remain the strong factor to apply effective guard rails and continuous evolution/improvement.

Enterprise security is evolving beyond traditional cyber defence toward a resilient model. As organizations adopt artificial intelligence, cloud computing and digital services, conventional approaches struggle to address sophisticated threats.

The next generation of enterprise security will integrate Zero Trust, AI-powered security operations, cloud protection, risk governance and cyber resilience. Zero Trust strengthens identity-based access by continuously validating users, applications and AI agents. AI-enabled operations help teams detect threats, investigate incidents and automate responses. Securing AI systems, data and cloud environments is essential to protecting information and maintaining digital trust.

Ultimately, next-generation Cyber Security is not about preventing every incident. It is about

1. ***Emphasis on upskilling***
2. ***Enabling innovation with Security Guardrails***
3. ***Anticipating threats to Limit disruption***
4. ***Sustaining customer trust through accountable leadership and continuous improvement.***

WINNERS'

VOICES OF IMPACT



PARAMAGURU RAMACHANDRAN

Director – Information Security

SUTHERLAND GLOBAL

Securing Global Service Delivery:

Managing Cyber Risk Across Distributed Enterprise Operations

Global service delivery no longer has a perimeter to defend. Work now moves across capability centers around the globe, vendors in multiple time zones, SaaS platforms nobody owns end to end, and people logging in from home. Every one of those hand-offs is a place where a single compromised identity or supplier can halt delivery for clients on the other side of the world.

This paper argues that cyber risk in distributed operations is managed best not by adding more controls at each site, but by treating security as one operating system that runs the same way everywhere. It sets out where the risk concentrates, a five-pillar model for governing it, what is specific to India's position as the world's delivery hub, and a 90-day plan that a CXO can start on Monday.

A modern enterprise delivers service through a web, not a building. India alone hosts 2,117 global capability centers across 3,728 units, employing about 2.36 million people, according to the Nasscom–Zinnov GCC report released in May 2026 (source). These centers no longer run back- office tickets; they own global products, platforms and client outcomes.

Clients do not buy controls; they buy the confidence that work will arrive on time, intact and private, wherever it was done. In a distributed enterprise, that confidence is built at the seams: the vendor login, the cross-border data flow, the hand-off between teams that have never met.

The organisations that win the next decade of global delivery will be the ones that treat cyber risk the way they treat quality: one standard, measured everywhere, owned by the business. For India, which now runs a large share of the world's enterprise operations, that is not only a defensive duty.

It is a competitive edge.

WINNERS'

VOICES OF IMPACT



BHAGWATI DUBEY

CISO

Tata Capital Housing Finance Ltd.

The Resilient BFSI Enterprise:

Protecting Digital Lending & Financial Ecosystems From Emerging Threats

Digital lending is making financial services faster and easier for customers but also creates new cyber risks. BFSI companies now depend on mobile apps, APIs, cloud services, artificial intelligence, data platforms and external service providers. Each connection creates a trust dependency that led to identity theft, fraud, data breaches, ransomware, API attacks or deepfake scams. To stay resilient, BFSI organisations must protect the complete digital lending ecosystem, not just individual systems. Security should combine Zero Trust, secure design, continuous monitoring, third-party risk management, data protection, AI governance, incident response and recovery planning.

A practical resilience model can follow seven steps: Govern, Know, Prevent, Detect, Respond, Recover and Adapt.

These steps help organisations understand risks, protect important assets, detect attacks early, respond quickly, restore services safely and learn from incidents. This approach can strengthen customer trust, business continuity and long-term cyber resilience across the financial ecosystem against rapidly changing digital threats.

WINNERS'

VOICES OF IMPACT



VENKATESH PS

Global Director – Global Business Resilience Practice

Cognizant Technology Solutions

Resilience at Global Scale:

Why DNS-Layer Visibility Is the First Line of Offense

In today's hyperconnected economy, resilience means anticipating risks, detecting threats early, and sustaining operations at global scale. For a global services leader like Cognizant, this requires visibility beyond network and endpoint controls. One critical but underestimated layer is the Domain Name System (DNS).

Why DNS Visibility Matters

DNS translates domain names into the destinations applications, users, and services need, so almost every digital interaction depends on it. Threat actors exploit it for command-and-control, phishing, malware delivery, and data exfiltration, while DNS failures can disrupt availability and continuity. What we cannot see, we cannot protect, and what we cannot detect early, we may struggle to contain.

Proactive Resilience

- **Early Threat Detection:** Spot suspicious domains, unusual patterns, and command-and-control activity.
- **Global Threat Intelligence:** Correlate DNS telemetry across regions to reveal isolated attack patterns.
- **Faster Incident Response:** Give security teams context to investigate, prioritize, and contain threats.
- **Business Continuity:** Detect DNS anomalies affecting critical applications.
- **Third-Party Risk Awareness:** Improve visibility into malicious domains across the ecosystem.

What This Means for Leaders

Resilience must be built into how technology is designed, secured, and operated. DNS-layer visibility should be a foundational capability within a broader cyber resilience strategy, integrated with SIEM, EDR, network detection, threat intelligence, identity controls, and incident response. Its value lies in turning DNS intelligence into actionable insights, measurable risk reduction, and faster decisions. This takes collaboration across security, infrastructure, cloud, application, and continuity teams, and leaders who treat resilience as a business outcome.

The Leadership Imperative

The question is no longer whether controls exist, but whether the organization can recognize threats before they become business-impacting. DNS-layer visibility is not the whole strategy, but it can be a powerful first line of offense. At global scale, resilience is about maintaining trust, protecting business value, and enabling digital transformation with confidence.

WINNERS'

VOICES OF IMPACT



PRAJEESH KG

CISO

Muthoot Capital Services Ltd.

Trust, Compliance and Digital Finance:

Building Security Into Every Customer Interaction

As digital ecosystems evolve, cybersecurity and privacy must work together to protect sensitive data. In cloud-first and AI-enabled environments, the focus must shift from securing networks alone to protecting data wherever it resides, moves or is processed.

A data-centric security approach integrates privacy into every stage of the technology lifecycle. Data discovery, classification and flow mapping help organizations understand what information they collect, where it is stored, who can access it and how long it should be retained.

Extending Zero Trust to the data layer ensures that access is governed by least privilege, continuous monitoring, encryption, masking and data-loss prevention. Data minimization further reduces exposure by limiting unnecessary collection and retention of sensitive information.

Privacy by design must also become an engineering priority, embedding data protection into application development, testing, logging and deletion processes rather than treating it as a post-deployment compliance requirement.

Ultimately, integrating cybersecurity, privacy and resilience enables organizations to reduce exposure, contain incidents, strengthen regulatory readiness and build stakeholder trust.

Protecting data by design is not merely a compliance obligation; it is a foundation for secure innovation and sustainable business value.

Organizations must also ensure that third-party partners and AI systems handle sensitive information responsibly through clear access controls, defined retention policies, continuous monitoring and accountability. This integrated approach helps maintain data protection across the extended enterprise while enabling innovation without compromising privacy or security.

bmc helix

Agentic AI for ServiceOps that scales with your business

helixops.ai



Deepak Singla

Area VP India & ASEAN, BMC Helix

Cybersecurity distribution has and continues to change.

The winners will not be the companies with the longest product list, but the ones that understand what enterprises currently need and will need next.



BEYOND THE PILOT

Making Agentic AI Accountable for Operational Outcomes

Enterprises do not lack AI insight. They lack the ability to act on it with speed, control and accountability. The next stage of enterprise AI is connecting intelligence to governed measurable operational action. That separates experimentation from advantage, and it is why Agentic AI belongs to the boardroom agenda now.

The Bharat CXO Drive reinforced this view. The five-month, 12-city roundtable series was led by our distributor Netpoleon India and ran from Ahmedabad on 12 June to Cochin on 9 October 2026.

BMC Helix presented at eight of the twelve roundtables. We spoke with CXOs, IT infrastructure leaders and security leaders across Tier 1 and Tier 2 markets, spanning Banking, Public Sector, Manufacturing, Pharma and Conglomerates. Partners build trust in the markets they know best, and together we reach the right rooms.

Across sectors, the question was the same: how do we let AI act on operations without losing control? Agentic AI is not one team's topic. It changes how the whole enterprise runs, secures and services its technology.

BMC Helix answers with an Agentic AI ServiceOps platform. For agents to deliver value, three conditions must hold: shared context, clear guardrails and measurable outcomes. Enterprise Service Management brings consistent, AI-enabled service delivery.

AIOps turns operational signals into event correlation and proactive remediation. ServiceOps unites the two on an open platform, so agents act on shared service context, within governance, from detection to resolution.

The result is faster resolution, lower operational overhead and a service-centric view of IT aligned to business goals. As a focused, AI-first ServiceOps company, this is our core business, not an add-on.

Our channel partners make this real with local delivery expertise and managed services that speed adoption and time to value.

My recommendation to every CXO: Start with the outcome, whether MTTR, service availability or resolution quality. Define the guardrails before scaling agents. Agentic AI earns its place when it is accountable for results.

BLUE

DEFENSIVE SECURITY



INSIDE THE CHALLENGE

CXOs took on the defender's role, working through scenarios to detect threats, respond under pressure, and protect critical assets.

WHAT WAS PUT TO THE TEST?

- **Threat Detection**
  Recognising suspicious activity.
- **Incident Response**
  Containing threats effectively.
- **Recovery & Resilience**
  Strengthening security readiness.

THE BLUE TEAM MINDSET

Detect the threat.
Contain the damage.
Protect the business.

WINNERS'

VOICES OF IMPACT



Cybersecurity Meets Privacy:

Building Security Architecture that Protects Data by Design

As digital ecosystems evolve, cybersecurity and privacy must work together to protect sensitive data. In cloud-first and AI-enabled environments, the focus must shift from securing networks alone to protecting data wherever it resides, moves or is processed.

A data-centric security approach integrates privacy into every stage of the technology lifecycle. Data discovery, classification and flow mapping help organizations understand what information they collect, where it is stored, who can access it and how long it should be retained.

Extending Zero Trust to the data layer ensures that access is governed by least privilege, continuous monitoring, encryption, masking and data-loss prevention. Data minimization further reduces exposure by limiting unnecessary collection and retention of sensitive information.

Privacy by design must also become an engineering priority, embedding data protection into application development, testing, logging and deletion processes rather than treating it as a post-deployment compliance requirement.

Ultimately, integrating cybersecurity, privacy and resilience enables organizations to reduce exposure, contain incidents, strengthen regulatory readiness and build stakeholder trust.

Protecting data by design is not merely a compliance obligation; it is a foundation for secure innovation and sustainable business value.

Organizations must also ensure that third-party partners and AI systems handle sensitive information responsibly through clear access controls, defined retention policies, continuous monitoring and accountability. This integrated approach helps maintain data protection across the extended enterprise while enabling innovation without compromising privacy or security.

VISHWAS PITRE

CISO & DPO

Zensar Technologies Ltd.

WINNERS'

VOICES OF IMPACT



Securing the Modern

Financial Enterprise: From Perimeter Security to Continuous Protection

SAMEER PRAMOD KHAKHAR

Deputy CISO

Shriram Finance Ltd.

As financial services become increasingly interconnected, real-time and autonomous, cybersecurity must evolve beyond protecting infrastructure to preserving institutional trust. In a world of cloud platforms, APIs, third-party dependencies and AI-driven operations, security must continuously verify authority, preserve integrity and ensure resilience.The traditional perimeter-based model is no longer sufficient. Financial transactions span customers, institutions, fintech partners and external service providers, making identity governance, transaction security and supply-chain risk management essential. Zero Trust principles must therefore extend beyond authentication to verify what each user, application or AI agent is authorised to do.Regulatory frameworks, including NIST Cybersecurity Framework 2.0, the European Union's Digital Operational Resilience Act and India's evolving financial-sector cybersecurity requirements, reinforce the importance of governance, accountability and demonstrable control effectiveness. Compliance alone is insufficient; institutions must prove that their controls work and that critical services can recover securely.

Artificial intelligence presents both opportunity and risk. While AI can strengthen fraud detection, threat intelligence and incident response, it can also enable sophisticated impersonation, autonomous attacks and correlated failures. AI agents must consequently be governed as privileged identities, with limited permissions, continuous monitoring, defined operating boundaries and immediate revocation capabilities. Human accountability must remain central.Looking ahead, autonomous financial ecosystems will require verifiable identities, authenticated instructions, traceable decisions and clearly defined machine authority. Quantum readiness will also demand cryptographic inventories, agile security architectures and planned migration towards post-quantum cryptography.Ultimately, cyber resilience is measured not by the absence of incidents but by an institution's ability to detect threats, contain disruption, maintain critical services and recover to a demonstrably trusted state.The future of financial cybersecurity lies in continuous verification of authority, preservation of integrity and resilience of critical services. Finance may become autonomous, but trust must remain verifiable.

WINNERS'

VOICES OF IMPACT



MANDAR KULKARNI

CISO, Head of Cybersecurity

Adani Power

Defending the Enterprise Behind the Perimeter:

A CISO's Playbook for Modern Infrastructure

The most dangerous assumption in cybersecurity is that what lies inside the perimeter can be trusted. Cloud, SaaS, APIs, operational technology, acquisitions and third parties mean the boundary moves with every partner, deployment or identity. Adversaries needn't breach the front gate; a stolen credential, exposed API or compromised supplier is enough. Enterprises must be designed to detect, contain and survive that inevitable foothold.

The stakes are higher for National Critical Information Infrastructure, where an attack can interrupt services, affect safety, disrupt revenue and invite regulatory scrutiny. As conglomerates grow through acquisitions and partnerships, security must make growth safer and more trustworthy, not slower. Cyber due diligence should begin before a transaction and continue through integration, guided by criticality, IT/OT connectivity, regulatory exposure and brand impact.

Zero Trust (verify explicitly, enforce least privilege, assume breach) is the foundation, supported by SASE, DLP, PAM and micro-segmentation to limit lateral movement, while EDR, XDR, SIEM and OT-aware detection contain threats.

Yet technology is only as effective as the people who run it. Role-based learning, realistic simulations and clear accountability build a workforce that can recognize risk and decide under pressure. People competency matters as much as the tools.

Every investment must show which critical service it protects, what loss it reduces and how quickly operations recover. The strongest enterprise is not the one that promises to keep every adversary out, but the one with the skilled workforce, resilient architecture and operational discipline to leave them nowhere to move and no ability to stop the business.

WINNERS'

VOICES OF IMPACT



The New IT Security Baseline for Financial Services

While working on industry-level web projects, I noticed that good engineering already practises what security teams keep asking for.

A login token that expires in minutes and can be cancelled by the server. A review that happens every month, not just before an audit.

A GitHub pipeline where no change reaches production unseen. I use these as a simple lens for NBFCs. Seeing, acting and recovering matter more than the number of tools bought.

My view: the weak spot is rarely technology. It is that nobody knows who is allowed to pull the plug on a loan system at midnight.

It closes with three engineering habits any NBFC can adopt this quarter.

SHAILESH TRIPATHI

GM IT

Laxmi India Finance Ltd.

WINNERS'

VOICES OF IMPACT



Protecting the Beverage Enterprise:

Building Security Across Distributed Operations and Digital Workflows

NISHANT KANDPAL

Information Security Manager

Varun Beverages

"**Protecting the Beverage Enterprise:**
The beverage industry operates on scale, speed and continuity. From manufacturing plants and warehouses to distribution networks, corporate offices and digital platforms, every part of the business is increasingly connected. This connectivity **creates efficiency**, but it also expands the organisation's security exposure.

Over the years, one lesson has become increasingly clear: security is strongest when it is
built into the way the business operates, rather than added after the business has been
built.
Protecting a modern beverage enterprise therefore cannot be limited to securing laptops, servers or the corporate network. Security must extend across IT infrastructure, operational technology, cloud environments, applications, identities, data and third-party ecosystems. The real challenge is achieving this security **without creating friction** for the business. Manufacturing and distribution cannot afford prolonged disruptions because of security controls. The objective should be to build security into business processes rather than trat it as an additional layer of compliance.
A mature approach starts with visibility and accountability (which is the foundation of Control). Organisations need to know what assets they have, who owns them, what access they have, how they are connected and what business processes depend on them. From there, continuous monitoring, vulnerability management, strong identity controls, endpoint protection, network segmentation and third-party risk management become practical risk reduction measures rather than isolated security initiatives.
Digital transformation also requires a stronger focus on data and workflows. As businesses adopt cloud applications, automation, APIs, AI and digital collaboration, sensitive information moves through more systems and more stakeholders. Security controls must therefore follow the data and the business process, not just the physical infrastructure.
.
For a distributed beverage enterprise, cybersecurity is ultimately about protecting more than technology. It is about protecting production, supply chains, customer trust and business continuity. The strongest security model is one that remains effective across every **plant, platform, partner and digital workflow**, while allowing the business to continue

WINNERS'

VOICES OF IMPACT



SANJAY K SRIVASTAVA

SENIOR DIRECTOR (IT)

NATIONAL INFORMATICS CENTER

Cloud, Connectivity and Control:
The Security Priorities of a Growing Technology Enterprise

Significance of Cybersecurity in E-Governance

Cybersecurity protects devices, networks, and data from unauthorized access, cyberattacks, and other harmful threats. In e-governance, this protection works in layers: firewalls, intrusion detection systems, encryption protocols, and access controls. Because these systems serve citizens daily, they must stay vigilant, respond quickly when threats appear, and cover every possible attack point, including people, cloud infrastructure, and mobile devices.

Securing e-governance requires a multilayered approach that combines strong technical measures, best practices, and strategic policies. This safeguards sensitive data, keeps systems available, and maintains public trust. As systems become more interconnected, the attack surface grows, demanding stronger frameworks. Modernization should prioritize high-risk systems handling sensitive data, citizen-facing applications, critical infrastructure platforms, unsupported software and hardware, and systems with significant compliance exposure.

E-governance systems worldwide have faced heavy cyberattacks in recent years, exposing vulnerabilities and underlining the need for robust protection. Governments are responding by prioritizing cybersecurity investments, adopting advanced technologies, and training staff continuously.

Central to this response is cyber-resilience: the capacity to anticipate, withstand, recover from, and adapt to adverse cyber events, going beyond prevention to include continuity and learning. It rests on cyber risk assessments, vulnerability assessments, penetration testing that simulates real attacks, and configuration reviews of critical assets. It is a multi-dimensional construct spanning technology, governance, and human factors.

Several modern approaches support it. Zero Trust Architecture follows "never trust, always verify," using continuous authentication, least privilege, and resource-level policy enforcement instead of perimeter defenses. AI assurance ensures AI systems are robust, safe, and aligned with policy objectives. Data sovereignty keeps sensitive data within specified jurisdictions, shaping cloud architecture choices. Federated learning trains machine learning models across parties without centralizing raw data, protecting privacy. Adversarial ML, finally, reminds us that attackers can manipulate inputs or training processes to cause erroneous model behavior.

WINNERS'

VOICES OF IMPACT



The CISO's Cloud Security Blueprint:

Protecting Digital Businesses Without Creating Silos

The isolated plant network is mostly a myth now. On shop floor, CNC controllers pull programs from PLM, test rigs push data to ERP, and OEM engineers log in remotely to fix machines, sometimes on laptops we have never seen. Production needs this connectivity, so security has to start from that reality.

In sensitive manufacturing industry, the worry isn't only stolen drawings. A modified toolpath could produce a part that passes inspection and still shouldn't fly. That makes OT security product integrity issue as much as an IT one.

Start with an asset inventory, even if it takes longer than expected. Then segment, tighten vendor access, and run joint drills with IT and plant teams in the same room.

Disclaimer: The views expressed here are my personal views and do not represent those of my organisation.

AHSAN K.

CISO

Tata AdvancedSystems Ltd.

WINNERS'

VOICES OF IMPACT



K V DINESH BABU

CISO

Veritas Finance Ltd.

Trust, Compliance and Digital Finance: Building Security Into Every Customer Interaction

India's digital finance revolution will not be measured by the speed of transactions, but by our ability to protect the trust behind every transaction.

As a CISO, I see a universal challenge: technology is evolving faster than our ability to secure it, while cybercriminals exploit every gap between innovation, governance, and accountability. Identity theft, digital fraud, compromised APIs, data exposure, third-party vulnerabilities, and AI-powered attacks are no longer merely technical incidents; they threaten livelihoods, institutional credibility, and public confidence.

I strongly believe our greatest cybersecurity failure is not always a data breach, it is the moment a customer loses confidence in the digital system they depend on. Every API, mobile application, loan approval, digital consent, and customer record represents a promise to protect someone's identity, livelihood, and financial future.

The solution is not simply another security tool or compliance checklist. We must move beyond reactive, audit-driven and checkbox security towards continuous, intelligence-led protection, embedding security by design, Zero Trust, AI-driven threat detection, privacy by default, cyber resilience, and shared accountability into every customer interaction.

Compliance is the minimum standard; trust is the ultimate responsibility.

My message to Digital India: "Innovation without security creates exposure. Compliance without accountability creates blind spots. Digital trust must be engineered, tested, and protected every day."

Cybersecurity is not the responsibility of the CISO alone; it is a collective commitment to protecting every identity, every transaction, and India's digital future.

WINNERS'

VOICES OF IMPACT



Cyber Resilience in Banking:
Preparing for the Threats You Cannot Predict

When I began my banking career more than three decades ago, banking operations were almost entirely manual. Ledgers were written and balanced by hand. During annual closing, we sometimes remained in the branch for two consecutive days, working continuously without rest or sleep until the accounts were balanced and the closing process was completed.

Today, these calculations can be completed centrally across the entire bank within a few hours. This transformation illustrates the extraordinary power of technology in banking. Yet it has also changed the nature of dependency. When thousands of manual calculations are replaced by a centralised system, the integrity of that system, its data, configurations and processing logic becomes critical to the entire institution.

However, every stage of convenience has also introduced a new dimension of risk.
A cyberattack is no longer merely a technology problem. It can quickly become a fraud event, an operational disruption, a regulatory concern and a crisis of customer confidence.

For a bank, cyber resilience must therefore deliver four outcomes:
Protect money. Preserve data integrity. Sustain critical services. Maintain trust.
Artificial intelligence is increasing the speed, scale and sophistication of this change. Technology can block an attack, but only an institution can absorb one. Resilience emerges when secure architecture, disciplined operations, informed people, accountable leadership and tested recovery arrangements work as one system.
The most important measure of cyber resilience is not how many security products a bank has deployed. It is the bank's demonstrated ability to detect, contain, recover and learn.

Modern banking reilience cannot stop at the organisational boundary. In an interconnected financial system, collective defence is not optional; it is essential to protecting public confidence.
After more than three decades in banking, my conclusion is simple:
We cannot predict every cyber threat. But we can decide, before it arrives, whether it will become a contained event or an institutional crisis.
That decision is made through the resilience we build today.

K. VENKATA SAI KUMAR

CISO

NABARD - National Bank for Agriculture and Rural Development

WINNERS'

VOICES OF IMPACT



AMIT SUBHANJE

CYBERSECURITY LEADER

RTX

Detecting the Undetectable: Behavioral Analytics as the Backbone of Defense in Aerospace

Cyber operations are employed to enhance traditional warfare. In aerospace and defense industries, such a situation means there is one more factor to consider—the trusted human access route that links with the strategic power.

Let's consider the following situation: a propulsion data engineer starts working outside his normal area of operations and inspects satellite, avionics, and flight-testing data. He does not perform any hacking actions and has no stolen passwords.

What is unusual is the context in which he operates, which may not be recognizable using standard security procedures.

Thanks to AI-powered behavioral analysis, it would be possible to create a dynamic benchmark of behavior in terms of identity, system, and data so that deviations are detected in time and corrections can be introduced.

This allows us to change the focus of security from "Is this user authorized to act?" to "Does that behavior make sense?"

In the case of airlines, it makes a crucial difference that might save years of engineering, mission readiness, strategic intellectual property, and competitive advantage.

Most dangerous cyber actions may not be unauthorized access.

Instead, they might be actions that are authorized.

WINNERS'

VOICES OF IMPACT



Thinking Like an Attacker in Gold Loan Finance:

Why DNS-Layer Visibility Is the Smartest First Move

As digital ecosystems evolve, cybersecurity and privacy must work together to protect sensitive data. In cloud-first and AI-enabled environments, the focus must shift from securing networks alone to protecting data wherever it resides, moves or is processed.

A data-centric security approach integrates privacy into every stage of the technology lifecycle. Data discovery, classification and flow mapping help organizations understand what information they collect, where it is stored, who can access it and how long it should be retained.

Extending Zero Trust to the data layer ensures that access is governed by least privilege, continuous monitoring, encryption, masking and data-loss prevention. Data minimization further reduces exposure by limiting unnecessary collection and retention of sensitive information.

Privacy by design must also become an engineering priority, embedding data protection into application development, testing, logging and deletion processes rather than treating it as a post-deployment compliance requirement.

Ultimately, integrating cybersecurity, privacy and resilience enables organizations to reduce exposure, contain incidents, strengthen regulatory readiness and build stakeholder trust.

Protecting data by design is not merely a compliance obligation; it is a foundation for secure innovation and sustainable business value.

Organizations must also ensure that third-party partners and AI systems handle sensitive information responsibly through clear access controls, defined retention policies, continuous monitoring and accountability. This integrated approach helps maintain data protection across the extended enterprise while enabling innovation without compromising privacy or security.

VINODHKUMAR C

CTO

Muthoottu Mini Financiers Limited

THE CONCLUSION.

Six months, twelve cities, and one long road. The Netpoleon Bharat CXO Drive began as an idea to bring India's security leaders around the same table, away from slide decks and sales pitches, for honest conversations about what is really happening in their world.

From Kochi to Delhi, Pune to Chennai, Bengaluru to Lucknow, every city brought its own energy, its own questions and its own way of looking at risk. CISOs, CTOs and CIOs shared what keeps them up at night, argued about what works and what doesn't, and took sides as Red Team and Blue Team with plenty of spirit. In every chapter, the finalists showed us how sharp, generous and driven this community is. Their stories and perspectives fill the pages of this magazine.

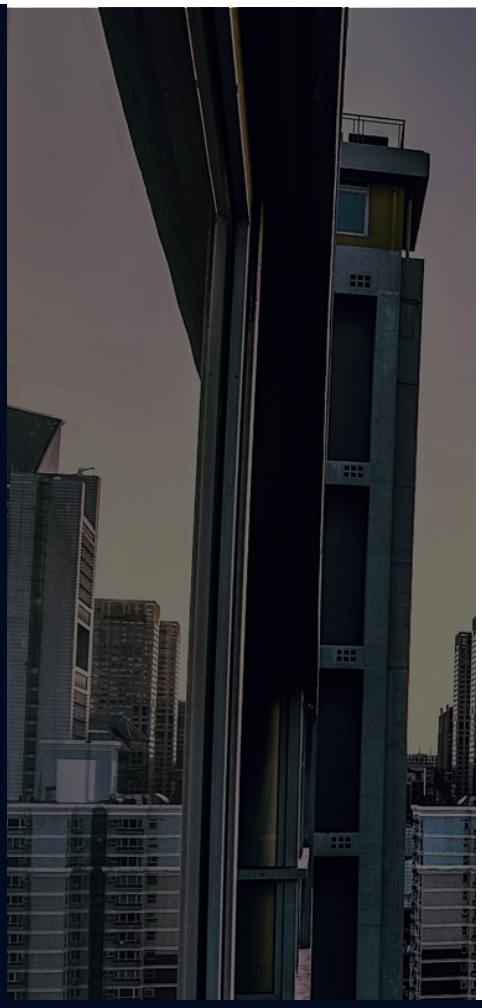
Behind all of this stood our partners. Netpoleon India, along with Infoblox, BMC Helix and Exabeam, backed this drive from the first city to the last. This collaboration made it possible to build a pan-India movement, and their expertise shaped many of the discussions you will read about here.

And then there were the Harleys. Two Harley Davidson X440s, one for the Offensive champion and one for the Defensive champion, gave the drive its finish line. The Grand Finale had the energy we hoped for, and the Wheel of Fortune kept everyone on the edge of their seats. Congratulations to the winners who rode home with the keys. We are glad we got to be part of that moment.

To every CXO who made time, took a seat at the table and brought an opinion with them: thank you. The leaderboard has a final result, but the conversations, the collaborations and the friendships will carry on well beyond it.

The drive ends here, and the community it built keeps going. We'll see you on the next road.

- Team CXO Junction



NETWORK.

EXPLORE.

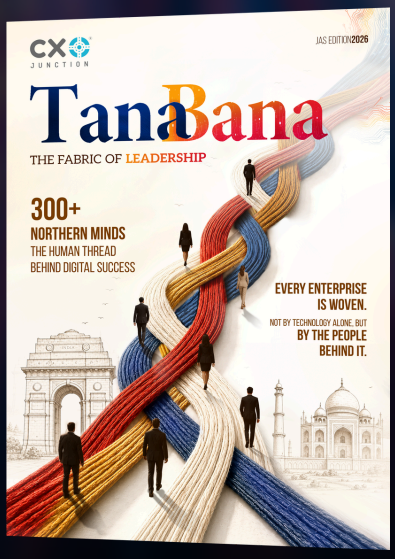
MAKE THE CHANGE.

CXO JUNCTION

A glimpse into our previous thoughtfully curated editions







www.cxojunction.com

Scan to find your digital edition here