FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

The Cyber Resilience Transformation: How AI Is Redefining Modern Cybersecurity Strategies

Neehar Pathare
CEO, CIO & MD,
63SATS Cybertech

in conversation with

Rajarshi Dhar
Associate Director, Global Security Advisory,
Frost & Sullivan, at the Cybersec India Expo 2026

In Collaboration with

Title Partner
63SATS Cybertech
Cyber Sec India Expo
powered by heise

As digital transformation accelerates across industries, cybersecurity is becoming one of the most critical priorities for enterprises, governments, and individuals alike. AI-driven attacks, growing digital identities, cloud adoption, and evolving regulatory requirements are reshaping how organizations approach cyber defense and operational resilience.

At the same time, India's fast-growing digital economy is increasing exposure to sophisticated cyber threats, driving the need for resilient and secure infrastructures. Organizations are now under pressure to defend their systems and build resilient security architectures capable of supporting uninterrupted business operations.

In this Transformational Growth Leadership discussion, Neehar Pathare shares how 63SATS Cybertech is approaching cybersecurity through AI-driven defense, cyber resilience, digital identity protection, and critical infrastructure security. Drawing on decades of experience protecting large-scale financial infrastructure, he discusses the evolving cyber threat landscape, the importance of awareness and compliance, and the need for a more holistic approach to securing organizations and individuals.

> "AI versus AI is the only way that we can block the next generation of cyber threats."
>
> — Neehar Pathare, CEO, CIO & MD, 63SATS Cybertech

Protecting Critical Infrastructure Through a New Cybersecurity Vision

Rajarshi Dhar: *Can you give us an overview of 63SATS Cybertech, including the company's vision, portfolio, and target audience?*

Neehar Pathare: 63SATS Cybertech is part of the 63 Moons Technologies group. I have personally been involved in protecting the networks and exchanges within the group for nearly eighteen years. Over the last twenty-five years, we faced many attacks, but we ensured there was no downtime across our infrastructure.

Following the COVID period, we saw cybercrime and cyberattacks increase significantly. At the same time, India emerged as one of the most targeted countries globally. Our mentor and coach, Shri Jignesh Shah, had envisioned back then that in the rapidly evolving digital world, cybersecurity will become inevitable for everyone, right from individuals to enterprises and critical infrastructure. He wanted to extend the same level of protection we built for our own infrastructure to organisations and individuals across the country. That vision culminated in the formation of 63SATS Cybertech.

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

The company's name itself comes from the concept of satellites around 63 Moons, protecting customers globally wherever they go. Today, we operate as a 360-degree cybersecurity company serving enterprises, SMEs, critical infrastructure environments, and even individual consumers. We recently launched a cybersecurity application focused on the common user, and we are already seeing strong adoption through downloads and installations.

The Three Defining Trends Reshaping Cybersecurity

Rajarshi Dhar: ***What are the biggest transformational trends you currently see shaping the cybersecurity industry, and how are they creating opportunities for 63SATS Cybertech?***

Neehar Pathare: The first and most visible trend is artificial intelligence. AI is becoming a double-edged sword. On one side, it helps organizations improve productivity and automate tasks. On the other side, cybercriminals are increasingly using AI to accelerate attacks and penetrate defenses much faster than before.

The pace at which AI-driven threats are evolving is making it difficult for human-led defense mechanisms alone to keep up. That is why we believe AI-driven cyber defense is essential. AI versus AI is becoming the only practical way to defend against the next generation of attacks.

At the same time, organizations are rapidly deploying AI across internal environments without always implementing the right security controls. We are increasingly seeing situations where poorly secured AI deployments create new risks around sensitive information exposure. As a result, one of our focus areas is building guardrails around enterprise AI implementations.

The second major trend is digital identity. As the number of connected devices continues to grow exponentially, virtually every connected entity will require a secure identity framework. Identity will become central to how organizations secure people, devices, and digital interactions.

The third trend is cyber resilience. Organizations now recognize that attacks are inevitable. The real challenge is ensuring business continuity while simultaneously defending against attacks. Whether the attack is small or large, businesses must continue operating securely without disruption. That resilience mindset will become increasingly important going forward.

Building an Innovation-Led Cybersecurity Organization

Rajarshi Dhar: ***Cybersecurity and innovation go hand in hand. How important is innovation and R&D within your organization?***

Neehar Pathare: Innovation is deeply embedded in the DNA of the 63 Moons Technologies group. Historically, we have always been an IP-led organization rather than a manpower- or services-driven company. Many of the businesses we built in the past, from exchanges to energy trading platforms, were innovation-led initiatives that transformed their sectors.

We are bringing that same innovation mindset into cybersecurity. We have a large research and development team that continuously monitors emerging cyber trends, attack vectors, and evolving risks. We actively study activity across the dark web and monitor discussions happening in various underground channels to better understand how future attacks may evolve.

In addition, we have strong capabilities in red teaming and offensive security testing. We do not just assess security posture theoretically; we actively simulate breaches and attacks to identify weaknesses and help organizations strengthen their defenses. Alongside this, we also support organizations on compliance and data privacy initiatives.

Helping Organizations Navigate India's Evolving Regulatory Environment

Rajarshi Dhar: *Regulatory compliance is becoming increasingly important across sectors. How does 63SATS Cybertech help organizations navigate evolving cybersecurity and data privacy regulations?*

Neehar Pathare: Over the last several years, cybersecurity regulations and compliance frameworks have become much more important across industries. We closely study regulatory guidelines and simplify them into actionable frameworks that organizations can implement operationally.

For example, we help organizations understand what activities need to be performed daily, monthly, and quarterly from a cybersecurity and compliance standpoint. We also developed assessment models where organizations can answer a set of questions and evaluate their cybersecurity posture through a measurable scoring system.

The Digital Personal Data Protection Act (DPDP) is especially important because it introduces both implementation requirements and legal implications, including significant financial penalties. To support customers more comprehensively, we have partnered with legal experts who can help address the legal side of compliance while we focus on implementation, assessment, and operational readiness.

Aspirations for Securing India's Digital Infrastructure

Rajarshi Dhar: *Looking ahead over the next five years, where do you see 63SATS Cybertech positioning itself in the market?*

Neehar Pathare: One advantage we have as a relatively young company is that we approach the market with a very fresh mindset. We also work closely with Israeli cybersecurity partners and leverage some of the latest cybersecurity technologies available globally.

Our aspiration is to become one of the most critical pillars supporting the nation's cybersecurity ecosystem. We want to help protect enterprises, individuals, and critical infrastructure environments across the country. Over the next five years, we believe we can play a leading role in strengthening India's cyber resilience and protecting critical national infrastructure.

Addressing the Industry's Biggest Cybersecurity Challenges

Rajarshi Dhar: *What do you see as the biggest roadblocks or challenges currently facing the Indian cybersecurity market?*

Neehar Pathare: One of the biggest challenges is still awareness. Many organizations continue to believe cyber incidents will happen to someone else but not to them. While awareness is improving, there is still a significant gap in how seriously cybersecurity is treated across many environments.

Another major challenge is ineffective implementation. Many organizations deploy cybersecurity solutions such as firewalls but only utilize a small percentage of their actual capabilities. Security technologies should not simply be installed as check-box solutions. They need to be fully configured, continuously optimized, and integrated into the broader security posture of the organization.

We often see significant gaps during security assessments and red team exercises. In many cases, organizations are not maximizing the value of the cybersecurity investments they have already made.

At the same time, the regulatory landscape is evolving rapidly. AI regulations, data privacy regulations, and cybersecurity frameworks are continuously changing. Organizations will need to invest more aggressively in both cybersecurity and AI governance going forward.

Why Cybersecurity Requires a 360-degree Approach

Rajarshi Dhar: *What advice would you give organizations that are currently modernizing their IT environments and moving toward hybrid cloud infrastructures?*

Neehar Pathare: Organizations should avoid looking at cybersecurity challenges in isolation. Security posture must be evaluated holistically across the entire organization rather than department by department.

For example, as companies adopt cloud environments and hybrid architectures, security decisions made by one department can affect the broader enterprise environment. That is why organizations need a complete 360-degree view of their cybersecurity posture.

Our approach is focused on helping customers identify gaps, fine-tune their existing environments, and apply the right security controls where needed. We do not simply recommend purchasing additional solutions. Instead, we help organizations ensure the technologies they already use are implemented correctly and optimized effectively. That is ultimately how organizations, and the country as a whole, will become more secure.

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

Neehar Pathare is the Managing Director, CEO, and CIO of 63SATS Cybertech, with over two decades of experience in technology leadership, information security, and cyber resilience. An alumnus of Indian Institute of Management Ahmedabad, he is recognized for integrating AI-driven intelligence into cybersecurity strategies to enable proactive and predictive defense models. His expertise spans advanced threat detection, digital forensics, cybersecurity governance, and risk management.

Before leading 63SATS Cybertech, Pathare held leadership roles at 63 Moons Technologies Ltd., Financial Technologies, and Robert Bosch, where he managed global information security and IT operations. He also serves as Vice President on the Management Committee of the CIO Association and continues to drive 63SATS Cybertech's mission of delivering scalable and affordable cybersecurity solutions for India's MSME sector.

Rajarshi Dhar | Associate Director, Global Security Advisory, Frost & Sullivan

Rajarshi Dhar serves as Associate Director for Global Security Advisory at Frost & Sullivan and is the subject matter expert for the Security Advisory practice across the Middle East, Africa, and South Asia. He specializes in cybersecurity, cloud technologies, and digital transformation, with expertise spanning growth consulting, market intelligence, and strategic advisory. Rajarshi holds an MBA in Marketing from the New Delhi Institute of Management and a Bachelor's degree in Electronics & Communication Engineering from North Maharashtra University.

Ready to Lead the Transformation?

- **Book a Growth Strategy Session:** Align your growth roadmap with Frost & Sullivan's Visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts:** Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Share Your Transformation Story:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council:** Collaborate with industry leaders shaping the future of your ecosystem.
- **Nominate for Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Demonstrate Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Activate Brand & Demand Growth:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Annexure: Strengthening Cyber Resilience in the Age of AI

AI adoption is accelerating across enterprises, but so are cyber risks. Intelligent attacks, expanding digital identities, hybrid infrastructures, and evolving regulations are reshaping how organizations approach cybersecurity, resilience, and governance.

To support organizations navigating this transformation, Frost & Sullivan provides forward-looking insights and strategic analysis across AI-driven cybersecurity, cyber resilience, digital identity, and critical infrastructure protection, including:

- Top 10 Growth Opportunities in Cybersecurity, 2025
- Managed Detection and Response, Global, 2025-2028
- Zero Trust Architecture: Next-Generation Cybersecurity Framework for Digital Enterprises
- Growth Opportunities in AI-Driven Threat Detection & Response
- Zero-Trust Browser Security Market, Global, 2025–2030

Together, these analyses reinforce the central themes explored in this Transformational Growth Leadership discussion: AI-driven cyber defense, operational resilience, digital trust, regulatory readiness, and the future of holistic cybersecurity transformation.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN