SPEAKIN ASIA DIALOGUES FORUM '26
WHITE PAPER | MUMBAI

DIGITAL TRUST AT SCALE:

Cybersecurity and the Future of India's Financial Ecosystem

How India's BFSI sector can accelerate innovation while safeguarding institutions, customers, and the integrity of the nation's evolving financial landscape.

Knowledge Partner
Thapar Institute of Engineering & Technology

Foreword

India's financial sector is at an inflection point. As we race to build the world's most digitally connected economy, we are simultaneously navigating threats that are more sophisticated, faster-moving, and more systemic than at any time in our history. The question is no longer whether institutions will face cyberattacks — it is whether they are truly prepared to withstand them.

The Asia Dialogues Forum 2026 in Mumbai brought together the most consequential voices in India's BFSI landscape — from board chairs and CISOs to regulators, national security experts, and academic leaders — in a rare closed-door dialogue designed to move beyond scripted narratives. What emerged was both a diagnosis and a call to action: digital trust is not a compliance checkbox; it is the foundation on which every future financial transaction will rest.

This white paper distils the insights, debates, and imperatives that surfaced over the course of that conversation. It examines the architecture of resilience, the evolving threat landscape shaped by AI, the delicate balance between innovation and risk in banking and insurance, and the emerging regulatory frameworks that must now evolve at the speed of the threats they seek to govern.

At SpeakIn, we believe that the most important conversations happen in rooms where people can be candid. We are proud to host this forum and to share its findings with a broader audience through this white paper.

Deepshikha Kumar Anand
Founder, SpeakIn

Executive Summary

The SpeakIn Asia Dialogues Forum 2026 in Mumbai convened nineteen senior leaders from across India's banking, financial services, insurance, and technology sectors for a 90-minute structured dialogue on digital trust, cybersecurity, and the future of India's financial ecosystem.

19	90	4
Senior Leaders	**Minutes of Dialogue**	**Core Themes**
CXOs, CISOs, Board Chairs	Closed-door, unscripted	Trust, Threat, Innovation, Regulation

The forum identified four interconnected challenges defining the current moment for India's BFSI sector: the imperative to embed security into product architecture from day one; the escalating sophistication of AI-powered threats including deepfake fraud and ransomware-as-a-service; the structural vulnerability created by third-party vendor ecosystems; and the critical gap between the letter of regulatory compliance and the spirit of genuine digital trust.

Across all discussions, a single theme emerged with force: the human element — whether through board-level oversight gaps, employee training deficits, or the psychological nature of trust itself — remains both the greatest vulnerability and the greatest opportunity for India's financial institutions.

KEY FINDINGS AT A GLANCE

- 1 in 5 cyberattacks in India in 2024 targeted the BFSI sector (Economic Survey 2025)
- Average global cost of a data breach reached USD 4.4 million in 2025 (IBM)
- 60% of cybersecurity breaches involve human factors — phishing, social engineering, misconfiguration
- 90% of data breaches in India result from internal leakages, not external hacking
- India's DPDP Rules 2025 mandate full compliance by May 2027 with penalties up to ₹250 crore

Section 1: Trust by Design — Building Resilient Systems

The forum opened with a fundamental reframing: cybersecurity in India's financial sector has long been treated as a back-office function — a compliance burden managed by a technical team below the board's radar. The consensus among participants was unambiguous: this model is broken, and the cost of maintaining it grows with every new digital product, open banking integration, and AI deployment.

From Compliance Exercise to Board Imperative

Giles Castelino of LSEG offered one of the forum's most striking data points: LSEG operates infrastructure through which the majority of India's Dollar-INR foreign exchange is traded. A five-minute outage generates systemic risk for the entire country. For an organisation at that scale, cybersecurity has transitioned from a "tick-the-box" agenda item to a top-two board priority — driven, he noted, not by enlightenment but by regulatory deterrence.

"We have moved from cybersecurity being a compliance item to it being a top-two priority at our board. Regulations like the EU's DORA, which can impose fines based on a percentage of global turnover, create the deterrence that forces real budget allocation."

Giles Castelino, Managing Director, LSEG

Amisha Vora of Prabhudas Lilladher pushed the argument further: boards do not merely need to receive security briefings — they need to own cybersecurity strategy. The rapidly evolving AI and digital landscape means the standard quarterly review cycle is insufficient. Shraddha Thacker of UnionPay International reinforced this view, arguing that as more independent directors with technical backgrounds join boards, a new standard of personal accountability for security oversight must emerge.

The Architecture of Trust: Zero-Trust and Security by Design

Vishweshwaran Ramakrishnan of Unity Small Finance Bank described a structural shift that several participants echoed: security teams are increasingly being brought into the product design stage, rather than summoned for a final approval ritual. This "secure by design" philosophy — promoted also by Anand Kumar Sinha of Tata Technologies — represents a fundamental change in how financial institutions architect their digital products.

"Adopting a zero-trust stance is not a sign of paranoia — it is actually how an organisation fulfils its promise of being trustworthy. It means no vulnerability is taken for granted."

Amisha Vora, Chairperson & MD, PL Capital Group

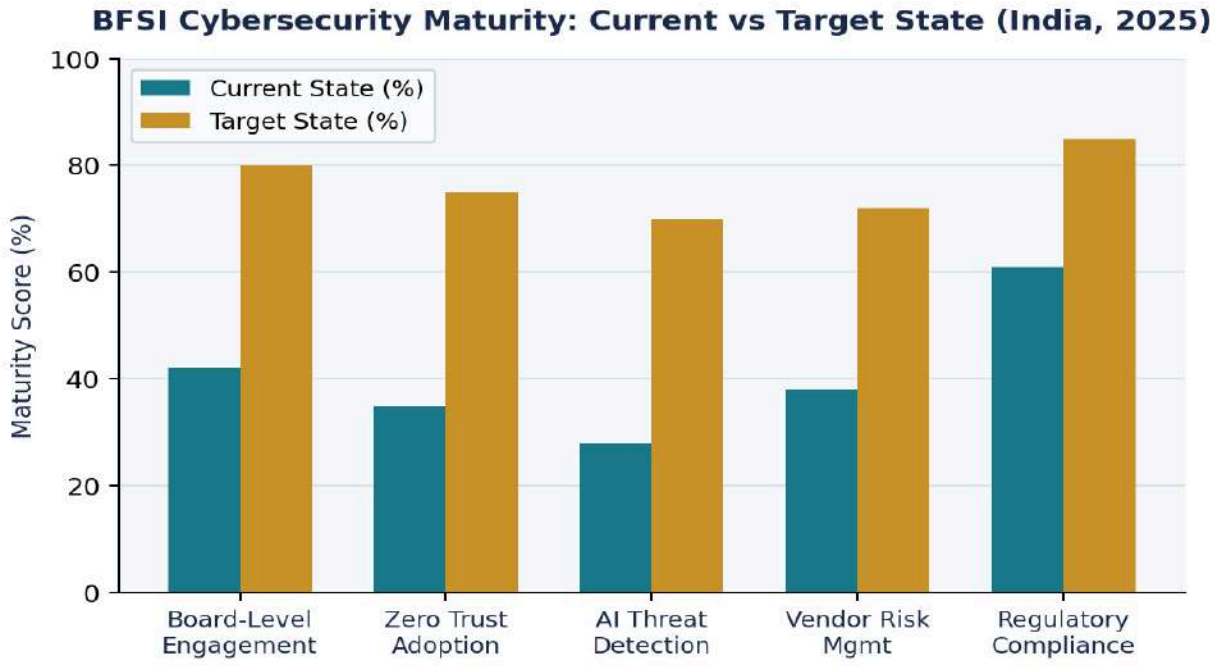
Dr. Padum Kumar Nay of Thapar Institute introduced an evolutionary lens: the human brain evolved to solve immediate, physical threats — not complex, abstract digital ones. This "evolutionary mismatch" makes humans the inherent weakest link in any security architecture. The implication for system design is clear: resilient systems cannot rely on human vigilance alone; they must be built to withstand human error.

Anand Kumar Sinha outlined three structural pillars for building organisational trust: People (security awareness and cultural embedding), Process (integrated and auditable data flows), and Technology (layered

perimeter and internal security). Participants were clear that most BFSI organisations remain strong on the technology pillar while underinvesting significantly in people and process.

"Trust is not a rational act — it is an evolutionary and biological one. Institutions that consistently meet expectations will maintain it. You cannot engineer trust without understanding its nature."

Dr. Padmakumar Nair , Vice Chancellor, Thapar Institute of Engineering & Technology



Source: Forum discussion synthesis, industry benchmarks (2025)

Section 2: Innovation vs Risk — Navigating BFSI's Digital Transformation

India's financial sector is undergoing a transformation without precedent in its history. The UPI ecosystem now processes billions of transactions monthly. Digital lending, neo-banking, and open finance are reshaping how credit, savings, and insurance are distributed. The forum's second major theme examined a tension that sits at the heart of every product roadmap and risk committee: how do institutions accelerate digital innovation without generating systemic vulnerability?

The Financialisation of Digital Life

R. Kalyanaraman of BlinkX by JM Financial situated the current moment in a longer arc. Over 25 years, the industry has witnessed two compounding trends: the digitisation of financial services and the financialisation of savings — a shift away from gold and real estate toward financial instruments, accelerated sharply by COVID-19. The consumer expectation that emerged — seamless, real-time, mobile-first — now sets the baseline against which all security trade-offs are measured.

"The AI revolution is comparable to the discovery of fire or the invention of the internet. Those with the willingness — more than the ability — to reskill and upskill will always remain relevant."

R. Kalyanaraman, Managing Director, BlinkX by JM Financial

Ajay Thakur of TGI SME Capital Advisors grounded this in the primal economics of finance: trust precedes transaction. No individual will entrust capital to an institution — digital or physical — without it. But trust in capital markets is uniquely fragile. A single poorly performing stock recommendation or a compromised account can shatter years of relationship-building. The SME Exchange processes billions of transactions daily and faces continuous cyberattacks — yet has never experienced a forced shutdown. That resilience, he argued, is the product of relentless investment, not luck.

The Vendor and Supply Chain Paradox

One of the most urgent vulnerabilities discussed at the forum: third-party vendor risk. Amisha Vora described a series of cyberattacks in late 2024 and early 2025 that originated from a single shared operations vendor and cascaded across multiple brokerage and mutual fund firms. The attacks did not target individual institutions — they targeted the shared infrastructure beneath them.

"Internal security is not enough. Many of our organisations are deeply dependent on third-party vendors integrated through APIs. These are not peripheral — they are entry points, and they must be governed as such."

Amisha Vora, Chairperson & MD, PL Capital Group

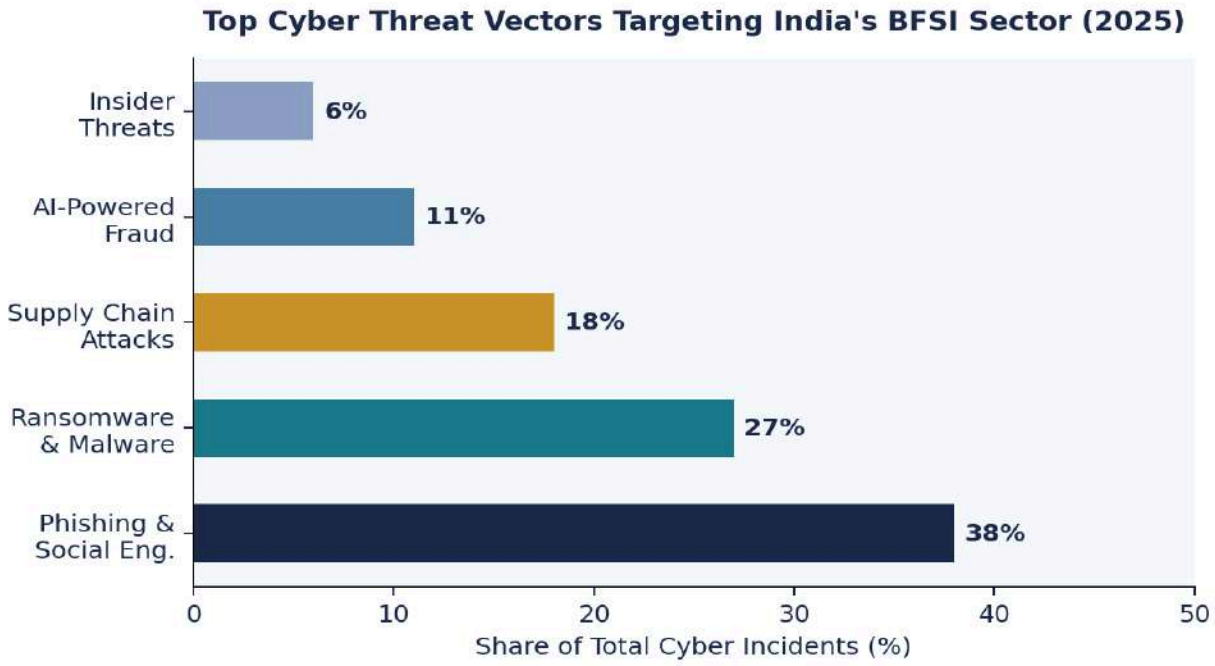
Atul Garg of SIDBI captured the dilemma succinctly: every new technology introduced for innovation simultaneously introduces an enhanced risk surface. The security posture of an institution must be continuously recalibrated to match the risk level of each new capability deployed.

Insurance as a Strategic Risk Management Tool

Sandeep Dadia and Sepia of Lockton Insurance brought an underwriting perspective that reframed the conversation: the financial value of data is, in effect, infinite. A physical office building has a quantifiable replacement cost. The value of lost data — customer records, trading positions, audit trails — cannot be bounded. This asymmetry makes traditional enterprise risk frameworks inadequate.

"We must stop treating cyber losses as black swan events. They are not. Every organisation will face a breach — the question is only when. The organisations that survive are the ones that have already planned for consequence management."

Sandeep Dadia, CEO & Country Head, Lockton Insurance



Source: DSCI-Seqrite India Cyber Threat Report 2025; SOCRadar BFSI Threat Landscape Report 2025

Section 3: The Threat Landscape — AI, Fraud & Nation-State Risk

The forum's third theme examined what BFSI institutions are actually up against. The picture that emerged was one of asymmetric warfare: adversaries who are nimble, AI-augmented, and in some cases motivated by ideology rather than financial return, operating against institutions whose security postures were built for an earlier generation of threats.

AI-Powered Attacks: The New Normal

Amit Dubey, a National Security and Cyber Intelligence Expert, described criminal syndicates operating sophisticated AI-driven operations: bot networks that engage potential victims across multiple social media platforms over weeks, building credibility before executing a final attack. The patience and sophistication of these operations — enabled by AI tools accessible at minimal cost — represents a fundamental shift from the opportunistic phishing campaigns of a decade ago.

"Criminals are now innovators. They use AI to create bot-driven illusions that build victim trust across multiple platforms before the final attack. The tools they use are accessible and cheap. The damage they cause is not."

Amit Dubey, National Security & Cyber Intelligence Expert

Ranjan Bhattacharya of HSBC India introduced the spectre of deepfake attacks as an existential challenge for financial institutions. "Whaling attacks" — in which a fraudster replicates a CEO's voice and facial presence in a live video call — are no longer theoretical. They target the human element directly, exploiting the trust networks that financial institutions have spent years building. His three-part framework — prevention ("unbreakable locks"), real-time response ("firefighting"), and recovery ("consequence management") — was widely endorsed as a useful operating model.

"As AI takes over technical productivity, the value of emotional intelligence — the human capacity for judgment and empathy — has gone through the roof. The machines handle the computation. The humans must handle the judgment."

Ranjan Bhattacharya, MD, Head of Strategy India & Middle East, HSBC India

The Persistence Problem: What Goes Undetected

Arnab Biswas of Axis Direct offered a technically grounded contribution that reshaped the forum's understanding of detection gaps. He described a case at a large private sector bank where a small piece of malware sat undetected on a decommissioned, unpatched UAT server for eighteen months before propagating into production systems. The failure was not one of perimeter security — it was one of internal vigilance, asset management, and legacy estate complexity.

"I have deep respect for hackers. They are great teachers. They consistently demonstrate that the measures we consider adequate are not. And unlike us, they sometimes operate purely for glory — with no budget constraints."

Arnab Biswas, CISO, Axis Direct

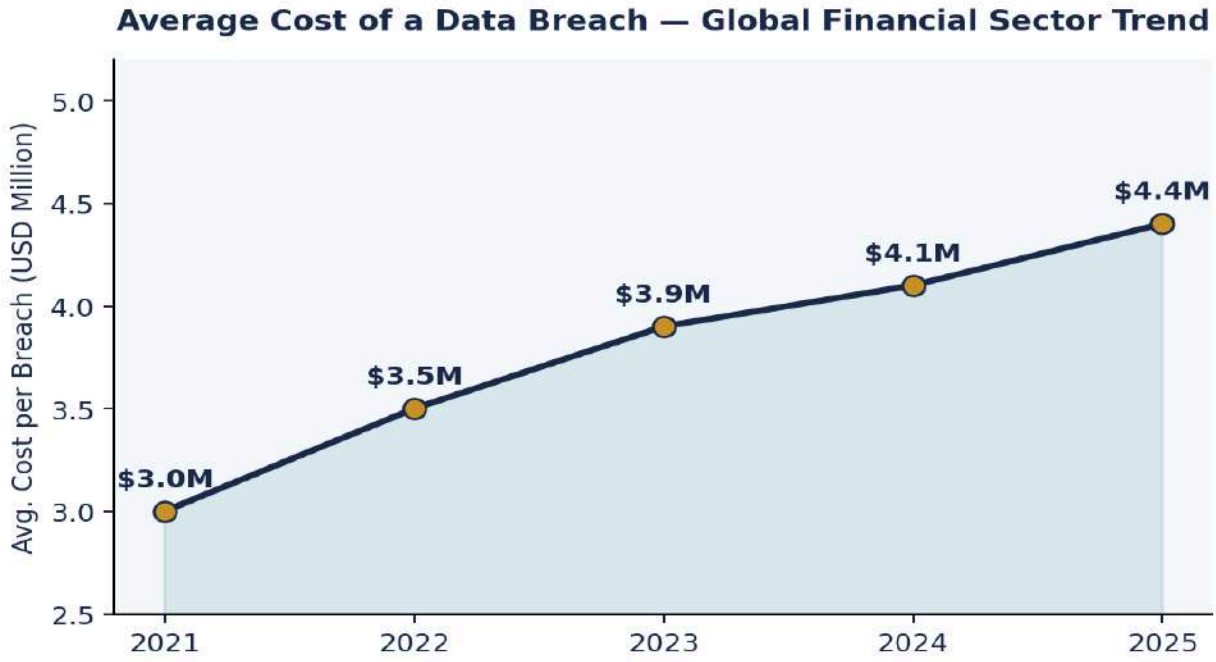
His broader argument — that security is fundamentally a data analytics problem, requiring the mining of millions of records to find a single malicious indicator — has significant implications for how CISOs communicate with boards. The question boards rarely ask, he noted, is not "how much have we spent?" but "how many black swan events have we successfully evaded?" Shifting the conversation toward efficacy, rather than expenditure, is one of the sector's most important unfinished tasks.

AI vs AI: The New Warfare at Blitz Speed

Vishweshwaran Ramakrishnan of Unity Small Finance Bank introduced one of the forum's most evocative framings: modern cybersecurity is AI versus AI warfare, happening at blitz speed. Automated tools scan for network vulnerabilities faster than any human team can respond. The implication is not merely that defences must be automated — it is that human-in-the-loop response is becoming structurally obsolete for the fastest class of attacks.

"When bots fight bots, the human cost is still felt by the common person — their account compromised, their access denied. We are building AI defences, but we must remember what we are defending."

Vishweshwaran Ramakrishnan, SVP & Head – Core IT Applications, Unity Small Finance Bank



Source: IBM Cost of a Data Breach Report 2025; global financial sector benchmarks

The Ransomware-as-a-Service Economy

Hina Kamra of Neo Wealth and Asset Management articulated the sense of structural helplessness that many participants acknowledged privately: the emergence of Ransomware-as-a-Service (RaaS) — a commoditised criminal model that lowers the barrier for sophisticated attacks to near zero — means the asymmetry between attacker and defender has grown qualitatively, not merely quantitatively. Her observation that the world is now effectively divided into those whose data has already been breached and those whose data is about to be was met with knowing acknowledgement across the room.

Section 4: Regulation, Compliance & The Path to Digital Trust

The forum's final thematic arc examined the regulatory architecture within which India's financial sector must build its cybersecurity posture — and the considerable distance between compliance and genuine trust. The consensus was clear: regulation is a necessary but insufficient condition. Institutions that treat the DPDP Act as a ceiling, or reduce the RBI's guidelines to a checklist, are building brittle defences.

The DPDP Act: A Landmark with Gaps

India's Digital Personal Data Protection (DPDP) Rules 2025, notified in November 2025, represent the country's most significant data governance legislation. The Rules operationalise the DPDP Act 2023 through a phased compliance timeline, with full substantive obligations effective by May 2027. For BFSI, the implications are material: granular consent requirements, mandatory breach notification, vendor oversight obligations, and penalties up to ₹250 crore for failure to maintain reasonable security safeguards.

"The DPDP Act is a step in the right direction. But if we benchmark it against the GDPR, it needs further refinement. The intent is right. The execution and enforcement mechanisms must now match the ambition."

Hina Kamra, Managing Director, Neo Wealth & Asset Management

Participants noted a constructive tension: the DPDP framework must balance robust data protection with India's innovation imperatives. BFSI organisations that have already invested in GDPR-aligned architectures are well positioned to extend those frameworks to the Indian market. For those starting from a lower baseline, the 18-month compliance runway — while generous — demands immediate action.

Global Standards and Local Realities

Giles Castelino offered the EU's DORA as a model worth studying: by tying penalties to a percentage of global turnover rather than fixed amounts, DORA creates incentives that scale with institutional size and complexity. The RBI's existing guidelines represent a strong domestic foundation, but several participants argued that India's regulatory frameworks have not yet fully reckoned with the systemic nature of cyber risk — the way a breach at one institution or vendor can cascade across the entire sector.

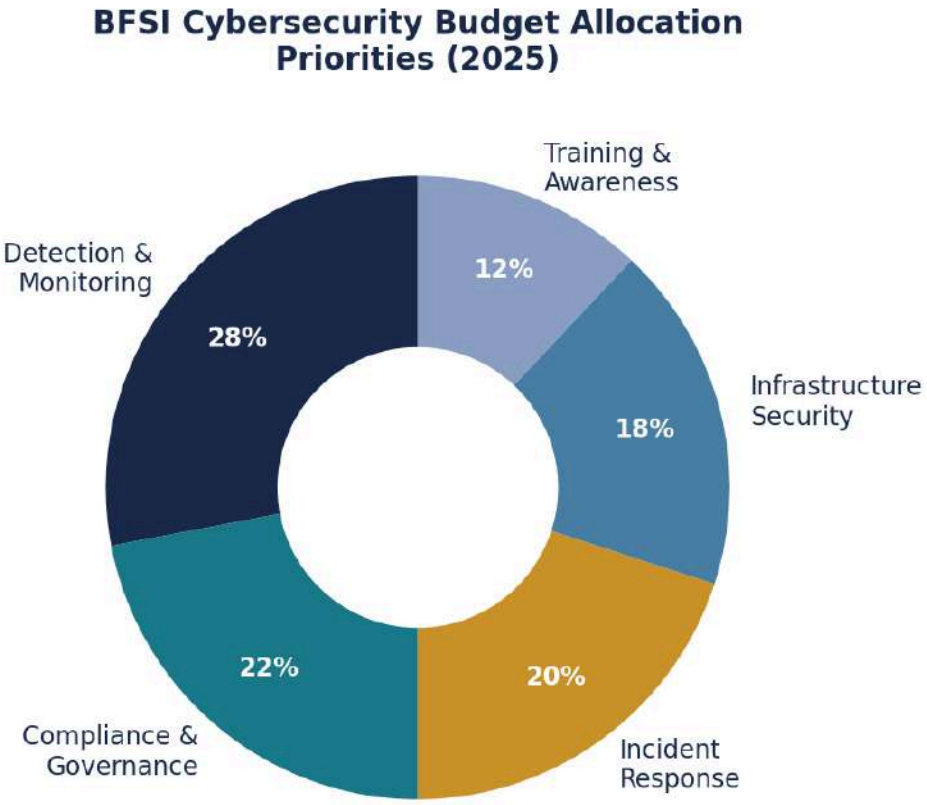
"Regulations like DORA work because the penalties are existential. They force institutions to allocate real budget to security rather than treating it as a line item to be optimised. India's regulators should take note."

Giles Castelino, Managing Director, LSEG

Compliance vs Trust: The Critical Distinction

Suresh Mahalingam, who moderated the forum, framed the session's central tension with precision: the question for India's financial sector is not whether to comply with the DPDP Act, RBI guidelines, or SEBI regulations — it is whether compliance is being used as a substitute for genuine security. An organisation that passes every audit but has not tested its incident response playbooks, has not trained its workforce on social engineering, and has not stress-tested its vendor dependencies is technically compliant but operationally vulnerable.

Dr. Mukesh Mehta advocated for a structural solution: remove human discretion from core security frameworks entirely, replacing it with rigid policies, processes, and technology protocols. The existence of detailed runbooks and playbooks for every scenario — down to how a printer reconnects to the network after a security incident — is the only way to ensure resilience when human judgment is most unreliable.



Source: Forum discussion synthesis; BFSI industry security investment surveys (2025)

Strategic Imperatives for India's BFSI Sector

The forum's discussions converged on six actionable imperatives for leaders, boards, and regulators in India's financial ecosystem:

01

Elevate Cybersecurity to a Board-Level Agenda

Security must transition from a CTO or CISO reporting function to a full board priority. Independent directors with technical literacy should be recruited, and security effectiveness — not merely compliance status — must be a standing board metric.

02

Adopt Secure-by-Design as an Organisational Default

Security and risk teams must be integrated into product design from day one. The zero-trust model — continuous validation of every digital identity and access request — should be the architectural baseline, not an aspiration.

03

Govern Vendor and Third-Party Risk as Strategic Risk

The supply chain is the sector's most under-governed attack surface. Institutions must conduct rigorous security due diligence on all third-party vendors, mandate contractual security standards, and stress-test their entire API ecosystem regularly.

04

Invest in AI-Powered Defence as AI-Powered Attacks Escalate

The era of manual threat detection is effectively over for sophisticated attacks. Financial institutions must invest in AI-driven monitoring, anomaly detection, and automated response — and must continuously update these systems as adversarial AI evolves.

05

Treat DPDP Compliance as a Trust-Building Opportunity

The DPDP Rules 2025 establish a floor — not a ceiling. Institutions that move early, exceed minimum requirements, and communicate transparently with customers about data governance will build a durable competitive advantage in the trust economy.

06

Close the Board Communication Gap on Cybersecurity

Security professionals must develop frameworks to translate technical risk into board-level comprehension. Quantifying cyber risk in financial terms — potential P&L impact, insurance liability, reputational cost — is the essential bridge between the CISO and the boardroom.

Additional Voices from the Forum

"Digital trust must be treated as a core enterprise risk, not a technical function. Boards need to move beyond surface-level comfort and develop real accountability for cybersecurity outcomes."

Suresh Mahalingam, Chairperson of the Board, Aviva India

"Future-ready talent requires more than theoretical learning. Deep integration between academia and industry, combined with experiential education, is critical to building real-world technological capability."

Dr. Maninder Singh, Professor & Head, Thapar Institute of Engineering & Technology

"Trust is the starting point of every financial transaction, yet it can be broken instantly. Institutions must continuously invest in resilience to ensure credibility is never compromised."

Ajay Thakur, CEO & Managing Partner, TGI SME Capital Advisors LLP

"The financial ecosystem constantly balances growth with control. Strong governance, independent compliance structures, and accountable leadership are essential to ensure innovation does not create systemic risk."

Shraddha Thacker, Country Manager, UnionPay International

"In a zero-trust environment, identity and access must be constantly validated. Long-term success will depend on adaptability and the ability to evolve continuously alongside rapidly changing technologies."

Anuj Gupta, Managing Director, Hitachi Systems India

"Cybersecurity frameworks must minimise dependence on human judgment. Resilience comes from clearly defined processes, automation, and detailed playbooks that ensure consistent responses during high-pressure incidents."

Dr. Mukesh Mehta, Chief Technology Officer

"Trust at scale is built through the alignment of people, process, and technology. Organisations that neglect awareness and process integration will struggle to achieve true, sustainable security."

Anand Kumar Sinha, Chief Digital & Information Officer, Tata Technologies

About the Forum

SpeakIn Asia Dialogues Forum '26

The Asia Dialogues Forum is SpeakIn's flagship multi-city thought leadership series, bringing together C-suite leaders, domain experts, and policy voices for structured closed-door conversations on the most consequential issues facing Asian business and society.

The 2026 series features the theme of Digital Trust at Scale across three cities in India, producing individual city white papers and a combined India report.

Knowledge Partner

Thapar Institute of Engineering & Technology

Thapar Institute is one of India's premier technical universities, recognised for its contributions to research, industry-academia collaboration, and experiential learning. It served as Knowledge Partner for the Asia Dialogues Forum 2026, contributing academic rigour to the forum discussions.

Forum Participants — Mumbai

Participant	Designation	Organisation
Suresh Mahalingam (Moderator)	Chairperson of the Board	Aviva India
Dr. Manindra Singh	Professor	Thapar Institute of Engineering & Technology
Dr. PadmaKumar Nair	Vice Chancellor	Thapar Institute of Engineering & Technology
Giles Castelino	Managing Director	LSEG
R. Kalyanaraman	Managing Director	BlinkX by JM Financial
Amisha Vora	Chairperson & MD	PL Capital Group
Ranjan Bhattacharya	MD, Head of Strategy India & ME	HSBC India
Sandeep Dadia	CEO & Country Head, Asia Executive Committee Member	Lockton
Ajay Thakur	CEO & Managing Partner	TGI SME Capital Advisors LLP
Shraddha Thacker	Country Manager	UnionPay International
Vishweshwaran Ramakrishnan	SVP, Head – Core IT Applications	Unity Small Finance Bank
Atul Garg	CTO	SIDBI
Hina Kamra	Managing Director	Neo Wealth & Asset Management
Anuj Gupta	Managing Director	Hitachi Systems India
Arnab Biswas	CISO	Axis Direct
Amit Dubey	National Security & Cyber Intelligence Expert	—
Dr. Mukesh Mehta	CTO	—

Anand Kumar Sinha	Chief Digital & Information Officer	Tata Technologies