OPINION PG 16

From Threats to Tools

Mahammad Shafi Shaikh, Senior Manager Information System Administration, Agro Tech Foods

JULY 2025
SUPPLEMENT OF CIO&LEADER

CISOFORUM

Security For Growth And Governance

From Chaos to Control
How India's CISOs Are Rewriting the Security Playbook

PG 10

A 9.9 GROUP PUBLICATION
www.csoforum.in
csoforum-in csoforum-in

studiotalks
AI
studiotalks

Securing trust in a hyperconnected era

AS INDIA accelerates into a digital-first economy, managing identity has never been more complex—or urgent. The explosion of apps, APIs, AI-driven services, machine-to-machine interactions, and ubiquitous cloud adoption has redefined enterprise security perimeters. For Indian CISOs, identity is now the first—and often,the lastline of defense.

Today's identity ecosystem is sprawling. Employees, contractors, partners, bots, and devices all demand access—often from outside traditional corporate boundaries. APIs expose sensitive data to third parties. AI-powered automation enables machines to act independently. In an economy where digital transformation is accelerated by initiatives like Digital India and Aadhaar, the stakes are even higher.

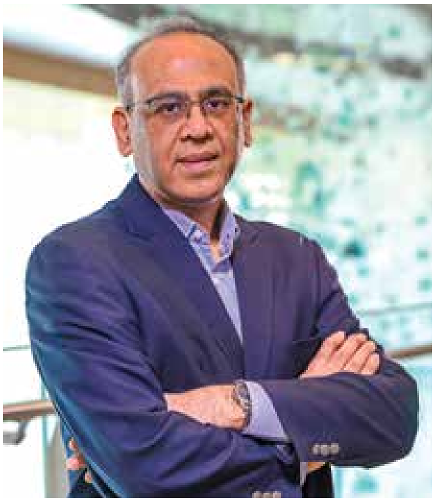
The challenges are multifaceted. Fragmented identities plague organizations, with users juggling multiple credentials across platforms, increasing the risk of weak passwords. APIs have become attack surfaces, with poorly secured endpoints exploited for breaches. AI and automation require new governance models for non-human identities like service accounts and IoT devices. Multi-cloud complexity leads to inconsistent policies and shadow IT.

Adding urgency is the looming quantum computing threat. Within a decade, quantum computers could render current encryption obsolete, fundamentally impacting identity authentication. Meanwhile, evolving Indian data protection laws require balancing user convenience with compliance.

Critically, identity failures can directly impact business continuity. When identity systems fail, operations halt, remote work vanishes, customer services become inaccessible, and supply chains disconnect. For Indian enterprises, identity resilience increasingly equals business resilience.

The solution demands fundamental change. Zero Trust approaches—where every user, device, and API is rigorously verified—are essential. Organizations must invest in unified identity platforms centralizing access management across cloud and on-premises assets. Continuous, adaptive authentication must replace static credentials. Robust API security is non-negotiable. Strong governance for machine identities—tracking, auditing, and reviewing—is equally critical.

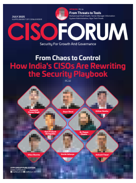
India's digital ambitions hinge on trust. For CISOs, mastering identity management isn't just a technical challenge—it's foundational for secure, resilient enterprises. So, start your Zero Trust identity transformation today—your organization's future may well hinge on it. ∎



"Zero Trust isn't a buzzword anymore. It's the blueprint for business continuity in the digital age."

R. Giridhar
Group Editor, B2B Tech
r.giridhar@9dot9.in

CONTENTS JULY 2025


JULY 2025
From Threats to Tools
CISOFORUM
Security For Growth And Governance
From Chaos to Control
How India's CISOs Are Rewriting the Security Playbook

Cover Design by:
Manish Kumar

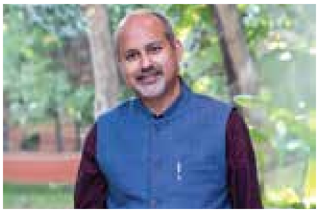
NEWS & VIEWS

OPINION

INTERVIEW

INSIGHTS

FEATURE



CISOFORUM
Security For Growth And Governance
www.cisoforum.in

MANAGEMENT
Managing Director: **Dr Pramath Raj Sinha**
Printer & Publisher / CEO & Editorial Director (B2B Tech):
Vikas Gupta
COO & Associate Publisher (B2B Tech):
Sachin Nandkishor Mhashilkar (+91 99203 48755)

EDITORIAL
Group Editor: **R Giridhar**
Executive Editor: **Jatinder Singh**
Correspondent & Editorial Coordinator - CISO Forum:
Jagrati Rakheja
Principal Correspondent: **Musharrat Shahin**

DESIGN
Creative Director: **Shokeen Saifi**
Assistant Manager- Graphic Designer: **Manish Kumar**

SALES & MARKETING
Director - B2B Tech:
Vandana Chauhan (+91 99589 84581)
National Sales Head - B2B Tech:
Hafeez Shaikh (+91 98331 03611)
Head - Brand & Strategy:
Rajiv Pathak (+91 80107 57100)

COMMUNITY ENGAGEMENT & DEVELOPMENT
Head - Community Relations: **Dipanjan Mitra**
Head - Databases: **Neelam Adhangale**
Community Manager: **Vaishali Banerjee**
Community Manager: **Snehal Thosar**
Community Manager: **Reetu Pande**
Community Manager: **Nitika Karyet**
Assistant Manager - Community Development:
Shabana Shariff

OPERATIONS
General Manager - Events & Conferences:
Himanshu Kumar
Senior Manager - Digital Operations:
Jagdish Bhainsora
Assistant Manager - Events & Conferences:
Sampath Kumar
Video Editor: **Sunil Kumar**

PRODUCTION & LOGISTICS
Senior Manager - Operations: **Mahendra Kumar Singh**

OFFICE ADDRESS
9.9 GROUP PVT. LTD.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published and Printed by Vikas Gupta for and on behalf of the owners, 9.9 Group Pvt Ltd (formerly known as Nine Dot Nine Mediaworx Pvt Ltd). Published at 121, Patparganj, Mayur Vihar Phase-1, Near Mandir Masjid, Delhi-110091 and printed at G. H. Prints Private Limited, A-256 Okhla Industrial Area, Phase-I, New Delhi - 110020.

Editor: **Vikas Gupta**

9.9 GROUP

Deepak Rana joins Evalueserve as Global CISO

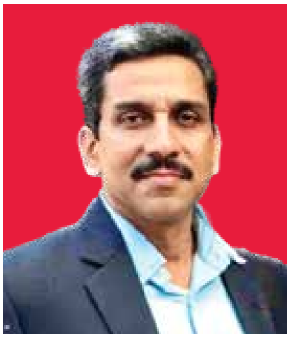
Deepak Rana has been appointed Global Chief Information Security Officer at Evalueserve. With over 20 years of experience in cybersecurity, compliance, and governance across telecom, BFSI, and IT, he brings deep expertise from prominent companies such as BT Group and Tech Mahindra, among others. He will lead Evalueserve's global security strategy, enhancing its cybersecurity posture and aligning it with industry best practices and regulatory standards.

K V Dinesh Babu joins Veritas Finance as CISO

K V Dinesh Babu has been appointed Chief Information Security Officer at Veritas Finance Limited. With over a decade of experience in cybersecurity and infrastructure, he will lead the company's security strategy. Previously, he held key roles at Equitas, Mphasis, and Standard Chartered, bringing deep BFSI expertise to strengthen Veritas Finance's digital security and risk management frameworks.

Kavitha Ayappan joins Neurealm as Vice President – Cyber Security and CISO

Kavitha Ayappan has been appointed Vice President – Cyber Security and CISO at Neurealm. With 20+ years of experience in cybersecurity leadership, risk management, and IT strategy, she will strengthen Neurealm's cyber defense. She has held key roles at Cholamandalam, Aspire Systems, and Cognizant, bringing deep expertise in regulatory compliance, cloud security, and cybersecurity transformation



Sachchidanand Muchandi elevated to Executive Director & Group CISO at JM Financial

Sachchidanand Muchandi has been promoted to Executive Director & Group CISO at JM Financial Ltd. With nearly 30 years of experience in cybersecurity and IT infrastructure, he will lead group-wide security governance. A 16-year veteran at JM Financial, he brings deep expertise in enterprise risk and cyber architecture, driving the company's mission of trust and resilience in a dynamic threat landscape.

Prof. Sandeep K. Shukla appointed Director of IIT Kanpur

Prof. Sandeep K. Shukla an IEEE Fellow and globally recognized expert in cybersecurity, embedded systems, and formal methods, has been appointed Director of IIT Kanpur. A recipient of the US PECASE and Humboldt Bessel Awards, he has led key national cybersecurity initiatives and brings deep academic, policy, and technical expertise to guide the institute into its next phase.

Ajaya Kumar K R appointed as General Manager & Group Information Security Officer at Bank of Baroda

Ajayakumar K R has been appointed General Manager & Group Information Security Officer at Bank of Baroda. With over 20 years in banking cybersecurity, he now leads global security operations across 18 countries. His leadership has driven enterprise-wide architecture, regulatory compliance, and secure   digital innovation, positioning him to advance the bank's cybersecurity posture and digital transformation agenda.

Security operations overwhelmed by maintenance tasks

Organizations spend more time maintaining security tools than defending against mounting cyber threats.

By **CISO Forum** | editor@cisoforum.com

SECURITY OPERATIONS centers globally are overwhelmed by tool maintenance while cyber threats grow more advanced, according to Splunk Inc.'s State of Security 2025 report.

The study, which surveyed security professionals worldwide, found that 46% of organizations spend more time maintaining security tools than actively defending their operations.

Only 11% of organizations trust AI completely for mission-critical security tasks

Cyberattacks have grown in scale and complexity, with two-thirds of respondents reporting data breaches in the past year—making them the most frequent security incident. Despite rising adoption of AI, only 11% of organizations fully trust AI for mission-critical tasks, highlighting a reliance on human oversight. "Human oversight remains central to effective cybersecurity, and AI is used to enhance human capabilities," said Michael Fanning, CISO at Splunk.

Operational inefficiencies are rampant: 60% of respondents cite tool maintenance as the top inefficiency, while 78% say their tools operate in silos, creating barriers for 69% of teams. Security analysts are also overwhelmed by alerts—59% report alert fatigue and 55% deal with excessive false positives. Alarmingly, 52% are considering leaving cybersecurity, and the same number say their teams are overworked.

AI is showing potential: 59% of organizations have seen efficiency gains and over half have prioritized AI in their 2025 plans, particularly in threat analysis, data queries, and policy development.

Those using unified security platforms report substantial benefits: 78% detect incidents faster and 66% achieve quicker remediation. The findings emphasize the urgent need to balance advanced technology and skilled personnel in today's escalating threat environment. ■

AI vs AI: The ultimate cyber showdown begins

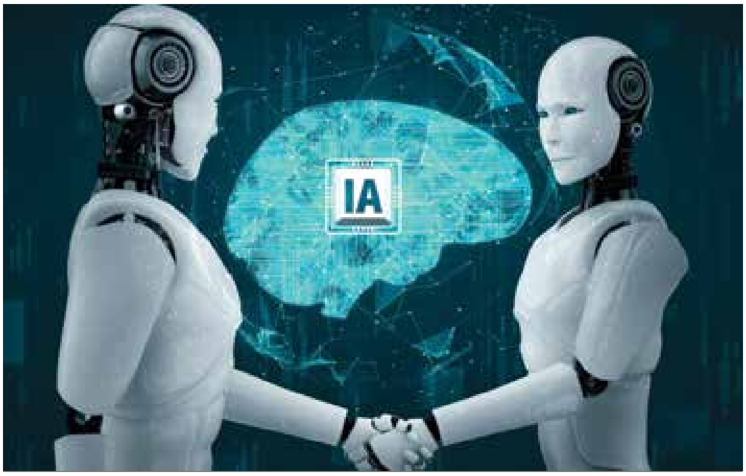
As AI-powered attacks surge, Fortinet launches an AI-driven defense suite—asserting that the only way to fight AI is with AI.

By **CISO Forum** | editor@cisoforum.com

THE BATTLEFIELD has shifted. Gone are the days when a poorly spelled phishing email was the biggest worry. Today's cybercriminals utilize sophisticated AI tools, such as FraudGPT and BlackmailerV3, to create attacks that are so convincing they could even deceive security experts. But Fortinet isn't backing down—they're meeting AI with AI.

The new threat reality

Recent data paints an alarming picture: voice phishing attacks surged 442% between the first and second halves of 2024. Meanwhile, cybercriminals are now using AI to power some of the most convincing and scalable attacks we've ever seen, from deepfake video calls to AI-generated phishing emails. Traditional email filters are struggling to keep up with this new breed of intelligent threats.



"We're not just blocking threats—we're predicting them,"

Nirav Shah, Senior Vice President, Fortinet

Fortinet's counter-strike

Fortinet has unveiled its answer: the FortiMail Workspace Security suite, powered by artificial intelligence. This isn't just another security update—it's a complete reimagining of workplace protection.

The new suite goes far beyond email, safeguarding browsers and collaboration tools like Microsoft Teams, Google Workspace, and Slack. Think of it as a digital bodyguard that follows users wherever they work, detecting malicious links in chat apps and hidden malware in shared files

Full workspace shield

What makes this solution unique is its unified approach. The enhanced FortiDLP (Data Loss Prevention) system tracks sensitive data from source to destination, monitoring how employees handle confidential information and automatically flagging risky behavior.

"We're not just blocking threats—we're predicting them," explains Nirav Shah, Fortinet's Senior Vice President. The system uses data lineage tracking to understand how information flows through an organization, providing security teams with unprecedented visibility.

The bottom line

As AI-generated cyberattacks become the most feared threat by IT professionals in 2025, Fortinet's new suite represents a crucial evolution in cybersecurity. In this high-stakes game of digital chess, the company is betting that the best defense against artificial intelligence is artificial intelligence itself. ■

Government cracks down on mobile fraud with new verification system

India's government introduces mobile number verification to curb digital fraud and enhance transaction-level security.

By **CISO Forum** | editor@cisoforum.com

IN A country where scammers steal billions through fake phone numbers and fraudulent calls, India's telecom watchdog is fighting back with a powerful new weapon: a nationwide mobile number verification system.

With cyber fraud cases increasing more than fourfold in fiscal 2024—resulting in losses of ₹175 crore—the Department of Telecommunications (DoT) has proposed sweeping changes to cybersecurity rules that could transform how mobile numbers are used across the country.

New platform to stop phone number misuse

The DoT's draft rules, published on June 24, introduce a Mobile Number Validation (MNV) platform that will act like a digital bouncer for phone numbers. Banks, payment companies, and other businesses will be able to instantly check if a mobile number is genuine before processing transactions. This system targets a growing problem: fraudsters using fake or invalid numbers to trick people into sending money. The platform will verify numbers against authorized telecom operator's databases to ensure legitimacy and prevent fraud.

The DoT's draft rules introduce a Mobile Number Validation platform that will act like a digital bouncer for phone numbers.

Who pays and how much

Under the proposed rules, organizations using phone numbers to identify customers—now called "Telecommunication Identifier User Entities" (TIUE)—will pay different rates for verification:

- Government-authorized entities: ₹1.50 per number check
- Private companies: ₹3 per number check

Banks and financial institutions, which process millions of UPI transactions daily using mobile nubers, are expected to be the biggest users of this service.

Cooling period for fraud numbers

The most striking feature is the automatic punishment system, already being tested. One majorbank is piloting a program where mobile numbers involved in fraud are flagged and deactivated for 90 days. After this cooling period, the number's fraud history is automatically deleted, ensuring that innocent people who later receive the same number aren't affected by previous misuse.

Broader powers for law enforcement

The new rules give government agencies andpolice broader access to transaction details fromnon telecom companies, enabling easier tracking of fraudulent activities across platforms. The DoT has invited public feedback within 30 days, signaling imminent implementation. As digital payments grow in India, these measures mark the government's most comprehensive effort yet to combat mobile-based fraud.■

The cloud security puzzle: Why protection is harder now

Cloud security is increasingly complex, with human error, poor encryption, and credential theft being key vulnerabilities.

By **CISO Forum** | editor@cisoforum.com

AS ORGANIZATIONS accelerate their digital transformation journeys, cloud adoption has become not just an option but a necessity for modern business operations. However, this shift brings unprecedented security challenges that are testing the limits of traditional cybersecurity approaches.

Where once companies managed security through a single, controlled environment, they now face the daunting task of protecting assets across multiple cloud platforms, countless applications, and hybrid infrastructures—creating complexities even seasoned IT professionals struggle to navigate in today's distributed computing landscape.

Cloud security takes the top spot

Despite years of investment and attention, cloud security remains the biggest headache for organizations worldwide. The Thales 2025 Cloud Security Study, surveying over 3,000 professionals across 20 countries, found cloud security topped concerns for the second year running. Companies now juggle 2.1 public cloud providers, traditional on-premises systems, and 85 software applications—creating a complex security nightmare that keeps IT teams awake at night.

Human error remains the leading cause of actual security breaches. It's like being afraid of burglars while leaving your keys in the front door.

The human factor: Our weakest link

Here's a surprising finding: while companies worry most about external hackers and cybercriminals, human error remains the leading cause of actual security breaches. It's like being afraid of burglars while leaving your keys in the front door. This disconnect between perception and reality shows organizations need to focus more on training their people and simplifying security processes. Even more concerning, 68% of respondents reported a rise in attacks using stolen credentials—often successful due to human mistakes.

Data at risk: The encryption gap

The study reveals a troubling reality about data protection. While 85% of cloud data is considered sensitive, many organizations still aren't encrypting enough of it. Only 65% use multi-factor authentication for cloud access. This, despite credential theft being the fastest-growing attack method, leaves their most valuable information unprotected and critically vulnerable.

The path forward

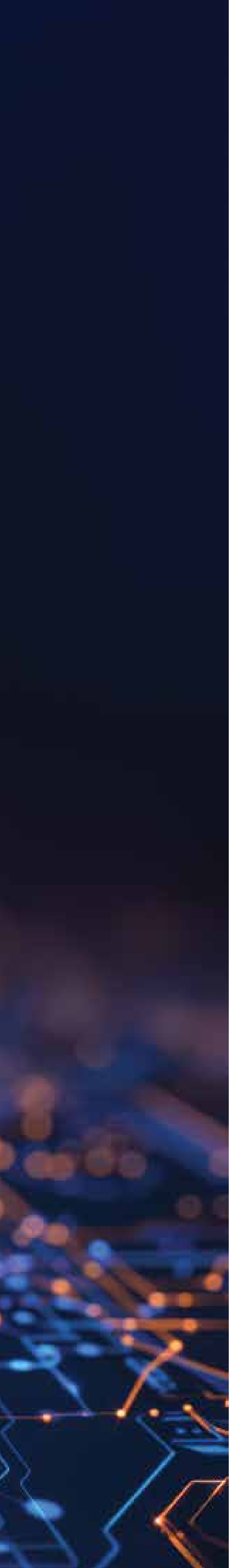
The good news? There are clear steps organizations can take. Simplifying security tools, implementing stronger encryption, and creating unified management systems across all cloud platforms can significantly improve protection. As artificial intelligence demands grow and place additional pressure on cloud security, businesses must act now to build stronger, more manageable defenses. The cloud isn't going anywhere—it'ss time to secure it properly. ■

From Chaos to Control

How India's CISOs are rewriting the security playbook

CISOs shift from gatekeepers to enablers, embedding security, resilience, and AI governance into business strategy for digital trust.

By **Jagrati Rakheja** | jagrati.rakheja@9dot9.in



IN A hyper-digitized enterprise landscape where technology evolves faster than governance models can catch up, cybersecurity is no longer the back-office function it once was. It has become the operating principle that underpins digital trust, business resilience, and brand integrity. The modern Chief Information Security Officer (CISO) has transitioned from an enforcer of controls to a strategic partner enabling the enterprise to grow responsibly.

This shift, however, hasn't been linear or frictionless. As organizations grapple with increasingly complex IT ecosystems, AI adoption, compliance pressures, and rising board expectations, CISOs are being asked to deliver more—with greater clarity, alignment, and accountability.

According to Gartner, nearly 60% of CISOs admit their security programs remain reactive, unable to keep pace with evolving enterprise demands. The challenge now is not just about responding to threats—but architecting security as a foundational layer of business transformation.

Security still in catch-up mode

Cybersecurity often finds itself reacting to the aftershocks of innovation rather than anticipating them. "Cybersecurity has always been a catch-up game," said Kishan Kendre, Global Head of Information Security. "When cloud technologies emerged, it took years to standardize the right security frameworks. Today, with AI, we're seeing the same lag. There are countless AI platforms being deployed across enterprises—but very few secure AI-native environments."

This growing disparity between technological advancement and security readiness is cause for serious concern. According to a CISO Forum study, by 2027, around 50% of organizations are projected to experience cyberattacks aimed specifically at AI-powered decision systems. As businesses quickly adopt AI in areas like customer service and analytics, security measures often lag behind or are missing altogether.

Amrish Kumar Singh, CISO at Godrej Industries, warns of the growing risks of this imbalance. "Digital transformation and cybersecurity are two sides of the same coin," he said. "If you move too fast without aligning your cyber posture, the damage can be irreversible—legal setbacks, brand erosion, even operational paralysis."

"Security should never be an obstacle to innovation — it must be the foundation that allows innovation to scale safely and sustainably."

Dr. Pawan Chawla
CISO & DPPO
Tata AIA Life Insurance

"A proactive security approach that anticipates risks is key to staying ahead of cyber threats."

Avinash Tiwari
Group CISO
Pidilite Industries

In this evolving landscape, the question is no longer whether cyber teams can keep up with innovation, but whether they can embed security deeply enough to prevent becoming its unintended casualty.

Cybersecurity as a business function, not an obstacle

In the modern enterprise, cybersecurity has moved from the server room to the boardroom. Yet despite growing awareness and budget allocations, many organizations continue to view cyber risk primarily as a technical problem—isolated from strategic decision-making. This siloed approach is no longer tenable.

"Security teams are often seen as blockers," said Amrish Kumar Singh, CISO at Godrej Industries. "But when CISOs understand the business context and communicate risks in the language of outcomes—impact on operations, customers, compliance—they become enablers of transformation. That shift in perception is absolutely critical."

The need for business-aligned security leadership is only intensifying. Gartner's 2025 recommendation stresses that security leaders must "demonstrate business acumen"to influence enterprise strategy. Thismeans being able to tie every risk, control, and investment to measurable business value—whether it's maintaining uptime, protecting brand trust, or enabling compliance-driven market expansion.

Keyur Desai, Head – IT at Prince Pipes, offered a compelling analogy: "CISOs need to start thinking like CEOs. If you own the business narrative, it becomes easier to set the right security priorities and gain executive alignment."

The transformation of cybersecurity into a core business function demands not just better tools but better communicators—CISOs who speak the language of growth, agility, and customer experience. In a world where digital risk can derail business momentum overnight, cybersecurity can no longer be a checkbox—it must be a business value multiplier.

"The DPDP Act is going to change the way we collect, store, share, archive, and delete digital personal data."

Ambarish Kumar Singh
CISO, Godrej Enterprises Group

"Embedding resilience is now a central pillar of our cybersecurity strategy — not just about prevention, but about readiness, recovery, and adaptability."

Ravi Prakash V Burlagadda
Sr Vice President - Information Security
Jio Platforms

Compliance beyond checklists: making security part of the DNA

India's upcoming enforcement of the Digital Personal Data Protection (DPDP) Act marks a pivotal moment in the evolution of enterprise data governance. As the Act pushes organizations to tighten controls over personal data collection, processing, and storage, regulatory compliance is becoming a top boardroom priority. However, seasoned CISOs warn that viewing compliance as a checklist-driven exercise could undermine its intent.

"Checklists are made for others. Real compliance needs to go into your DNA," asserted Vikas Sharma, Head – IT and CISO at Aditya Birla Group.

"If your organization views compliance as a quarterly chore, you've already lost the bigger battle. It should be like brushing your teeth—part of your routine, not a response to an external trigger."

This perspective calls for a cultural shift—from reactive to proactive, from periodic audits to continuous assurance. Organizations must move beyond document-driven reporting and embed compliance principles directly into business workflows, product development, and customer engagement strategies.

At the 2024 Gartner Security & Risk Management Summit, analysts emphasized that embedding cybersecurity into day-to-day operations—from software development to third-party engagements—is far more effective than enforcing compliance through top-down mandates. As summarized by a cybersecurity solutions provider, Gartner advocates for integrating security into business workflows to enable agility and resilience, rather than treating it as an external governance overlay.

The DPDP Act is a regulatory push in the right direction, but its success will depend on how deeply organizations internalize its principles. True compliance is not about ticking boxes—it's about building trust, by design.

Boardroom conversations: simpler, sharper, strategic

As cybersecurity cements its place on the boardroom agenda, CISOs are learning to tailor their messaging—not for technical peers, but for business leaders and directors. The language of cybersecurity is evolving from packets and endpoints to risk exposure, financial impact, and operational resilience.

"In a board meeting, you have 10 minutes," said Keyur Desai, Head – IT at Prince Pipes.

"You don't get into jargon or endpoint telemetry. You talk about risk exposure, how it'll be mitigated, and what it'll cost. The board wants clarity: What are the top risks? How do we respond? How prepared are we?"

This shift requires a more strategic, data-informed approach to communication. Frameworks like the NIST Cybersecurity Framework (CSF), FAIR (Factor Analysis of Information Risk), and Value-at-Risk (VaR) models have become instrumental in helping security leaders quantify threats in business terms. These frameworks allow organizations to assign dollar values to cyber risk—facilitating more transparent decision-making and budget alignment.

Boards are no longer content with vague threat levels or red/yellow/green dashboards. They expect concrete answers on potential losses, likelihoods, and return on investment for security initiatives. This expectation is being reinforced by regulators as well.

According to Gartner, by 2027, more than 50% of large enterprises will adopt formal cyber risk quantification frameworks, up from just 10% in 2022. This trend highlights a new era in cyber governance—one where risk visibility and strategic clarity are as important as technical controls.

Cybersecurity, once an IT concern, is now a shared executive priority.

"Cybersecurity has moved from reactive defense to proactive resilience — thinking out of the box is no longer optional."

Kishan Kendre
Global Head - Information Security
Blue Star

"Cybersecurity isn't a checklist — it must be embedded in your organization's DNA to truly drive transformation."

Vikas Sharma
Head IT & CISO
Aditya Birla Group

Budgets are bigger — but scrutiny is sharper

In the post-pandemic digital economy, cybersecurity budgets have grown significantly. Remote work, accelerated cloud adoption, and rising cyber threats have pushed boards to invest more in cyber defense. But along with this financial support comes heightened scrutiny. Today, security investments are expected to deliver tangible business outcomes—not just visibility dashboards or compliance checkmarks.

"Earlier, cybersecurity was viewed as a support function," said Kishan Kendre, Global Head of Information Security. "Today, it's a core enabler. Ironically, ransomware has been the best teacher—it put cybersecurity into the top five enterprise risks."

Executives are now asking tougher questions: What's the return on security investment (ROSI)? Are we better protected today than last quarter? Can this spend reduce breach recovery time, or enhance customer trust and brand resilience?

Anthony Basera, India Director – Enterprise Sales & Risk at Rubrik, emphasizes that this shift demands a new kind of narrative from security leaders. "Security tooling is one part of the puzzle. But CISOs need support in presenting these tools in terms of business value. The board doesn't care how many endpoints you've patched—they care about risk mitigation and business continuity."

This evolution calls for better cost-justification models, metrics that reflect business risk, and clearer alignment between cybersecurity spend and strategic priorities. According to Gartner, 75% of cybersecurity programs will be routinely assessed by their ability to deliver measurable value to the enterprise by 2026. The age of blind spending is over—every rupee must now earn its place in the resilience roadmap.

AI disruption: innovation meets uncertainty

Artificial Intelligence (AI) is rapidly transforming the cybersecurity landscape, but with it comes a paradox: the very tool that promises faster threat detection and response may also become one of the most complex risks to manage. AI-driven tools are revolutionizing how enterprises detect anomalies, automate incident response, and optimize threat intelligence. However, the speed of AI adoption is also exposing new vulnerabilities—especially when governance can't keep pace.

"AI adoption is happening faster than we anticipated," noted Amrish Kumar Singh, CISO at Godrej Industries.

"Employees are already using tools that IT doesn't know about—this is the rise of 'shadow AI.' We need to be proactive about governance before misuse becomes mainstream."

This hidden usage of AI tools outside formal IT oversight mirrors the earlier surge in shadow IT, but the stakes are arguably higher due to AI's potential to process and leak sensitive data, make autonomous decisions, or amplify bias. Compounding this is a widespread misunderstanding of what AI really is.

"We asked a team for their AI use cases," Singh added. "Out of five, only one was genuinely AI. The rest were glorified Excel formulas."

Gartner forecasts that by 2026, over 50% of cybersecurity incidents will be attributed to poor management of AI systems—making talent and governance just as critical as the technology itself. As organizations embrace AI-driven innovation, they must pair it with robust risk frameworks, clear usage policies, and upskilling programs to ensure AI becomes a force for resilience, not disruption.

"A CISO must think like a CEO — aligning security with business ensures faster, smarter digital transformation."

Keyur Desai
Head-IT
Prince Pipes and Fittings Ltd.

"When the CEO asks, 'Are we secure today?' — your only answer should be backed by a tested framework."

Urvish Acharya
Head-IT Governance, Risk &, CISO
Birla Carbon

Recent findings from Capgemini reinforce this duality. In 2024, 90% of organizations reported a cybersecurity breach, a significant jump from just 51% in 2021. Nearly half estimate financial losses exceeding $50 million in the last three years alone. What's more alarming is that 97% of enterprises faced security incidents involving Generative AI—ranging from malware generation and phishing to insider misuse and prompt injection vulnerabilities.

The report warns that Gen AI introduces a broader attack surface, demanding security across the entire lifecycle—from enterprise data ingestion and model customization to deployment and ongoing usage. Yet, three in five security leaders believe AI is essential for effective threat detection and response, and over 60% are optimistic about its long-term contribution to cyber defense.

As organizations increasingly experiment with Gen AI for threat intelligence and automation, the message is clear: AI must be governed as rigorously as it is adopted. Without this balance, enterprises risk turning a defensive advantage into a blind spot.

The talent gap: A strategic vulnerability

As cyber threats grow more sophisticated and AI compounds the complexity of enterprise security environments, the shortage of skilled cybersecurity professionals has emerged as one of the most critical vulnerabilities facing organizations today. The challenge is no longer just about hiring more people—it's about cultivating the right capabilities: strategic alignment, technical depth, and business fluency.

"There's no straight answer," said Urvish Acharya, Head – IT Governance, Risk, and CSO at Birla Carbon. "CXOs understand the risk now. They're ready to invest in people, but the talent must also be aligned with

Leadership blind spots in the modern CISO journey

This journey from chaos to control is not without its challenges, and CISOs must remain vigilant to avoid common pitfalls:

- **The strategy mirage**: Beware of high-level strategy discussions that lack actionable steps. Clear outcomes and defined implementation paths are essential.
- **The innovation paradox:** Balance the adoption of new technologies with robust risk management to ensure safe and impactful innovation.
- **The lone wolf syndrome:** Cybersecurity is a team sport. Cultivate a team with diverse skills to build a strong and resilient security posture.
- **The hindsight hang-up:** Don't dwell on past incidents alone—stay proactive by monitoring emerging threats and trends.
- **The echo chamber effect:** Step beyond like-minded discussions. Engage with varied perspectives to foster critical thinking and avoid complacency.

Source: How the CISO's Role Has Evolved from Gatekeeper to Strategic Visionary
By: Jaco Benadie, EY ASEAN Cybersecurity Energy Leader and OT Cybersecurity Competency Lead

> **"If you move too fast without aligning your cyber posture, the damage can be irreversible—legal setbacks, brand erosion, even operational paralysis."**
>
> **Ambarish Kumar Singh**
> CISO, Godrej Enterprises Group

frameworks, outcomes, and communication skills."

Acharya shared a candid moment of reckoning: "My CEO once asked me, 'If we're attacked today, how secure are we?' I didn't have a ready answer. That moment made us double down on NIST, measure across all six pillars, and build executive confidence."

This exchange underlines a core issue—cybersecurity teams must not only defend systems but also communicate assurance. A technically sound team that cannot translate risk in business terms risks being overlooked in key decisions.

The growing prevalence of AI only deepens the urgency. As Gartner warns, without qualified professionals to guide implementation, AI can create blind spots rather than visibility. This means future-ready security talent must be fluent in AI governance, risk quantification, and incident response playbooks.

Organizations must invest in structured learning, cross-functional exposure, and ongoing simulations. Cybersecurity can no longer be a siloed technical function. It requires multidisciplinary teams that can think tactically, act operationally, and communicate strategically.

The war for talent is no longer about roles—it's about readiness.

From reactive to resilient: the new CISO playbook

So what does the journey from "chaos to control" look like for India Inc.? For today's CISOs, it's not about being gatekeepers of IT or responders to the latest breach—it's about leading the organization through complexity with foresight, adaptability, and strategic clarity. The modern CISO is not just a technical defender, but a navigator of digital risk and an enabler of innovation.

This transformation demands a new playbook—one grounded in proactive resilience rather than reactive control. First, compliance must become embedded in business DNA, not relegated to quarterly checklists. As Vikas Sharma of Aditya Birla Group pointed out, true governance is habitual—"like brushing your teeth"—not a tick-box exercise.

Second, risk must be quantified in business terms. Frameworks like NIST, FAIR, and Value-at-Risk are helping CISOs articulate cyber exposure in language the board understands—impact, cost, and likelihood—making security funding easier to justify and align with business goals.

Third, talent transformation is critical. As Urvish Acharya emphasized, it's not just about hiring more hands but cultivating professionals who understand frameworks, think in outcomes, and communicate with clarity.

Fourth, AI governance must move ahead of usage. The rise of shadow AI is real, and without clear guidelines, enterprises may find themselves innovating into blind spots.

Fifth, resilience must be continuously tested. Anthony Basera, India Director at Rubrik, summed it up best: "Your greatest strength isn't the number of tools deployed—it's how often you test your resilience plan."

Lastly, CISOs must build partnerships, not just controls. Those who speak the language of business, align with digital transformation goals, and manage perceptions effectively will be seen as enablers—not blockers.

Cybersecurity today is more than a safeguard—it's a strategic function that underpins trust, accelerates innovation, and protects brand equity. In an AI-driven world, resilience is not just a capability—it's a competitive advantage. And trust? That remains the most valuable currency of all. ■

From threats to tools: How CISOs can harness AI for cyber defense

AI is reshaping cybersecurity, arming defenders and attackers alike. CISOs must navigate this double-edged sword with strategy, agility, and foresight.

By **Mahammad Shafi Shaikh** | editor@cisoforum.com

ARTIFICIAL INTELLIGENCE (AI) is transforming the cybersecurity landscape, providing both powerful defense mechanisms and sophisticated attack vectors. For CISOs, understanding how to leverage AI while mitigating emerging AI-driven threats is crucial. The intersection of Artificial Intelligence (AI) and cybersecurity presents a paradox. While AI significantly enhances threat detection and response capabilities, it simultaneously empowers threat actors with new tools to launch more sophisticated attacks. Chief Information Security Officers (CISOs) now face a dual challenge—leveraging AI to strengthen security postures while anticipating and countering AI-driven threats.

This article examines the latest AI trends in cybersecurity, including AI-powered threat detection, predictive analysis, and autonomous response capabilities. It highlights real-world examples of AI-based attacks and defenses, examines ethical and regulatory implications, and provides strategic best practices for building resilient cybersecurity frameworks. It further delves into the evolving landscape of AI and cybersecurity, exploring current trends, real-world applications, future scenarios, and strategic approaches that CISOs can adopt to navigate this complex domain. The goal is to equip CISOs with practical insights to harness the potential of AI while safeguarding their organizations against evolving threats.

1. AI-Driven threat detection and prevention

Traditional security systems rely on static rule-based models, which struggle to keep up with dynamic threats. AI introduces adaptive learning models that continuously evolve based on real-time data.

- **Machine learning (ML) for anomaly detection** – AI models analyze vast datasets to identify deviations from normal behavior, flagging potential intrusions.
- **Natural language processing (NLP) for phishing detection** – AI detects subtle language patterns indicative of phishing attempts, improving accuracy in identifying social engineering attacks.
- **Automated incident response** –AI-driven systems can isolate affected endpoints and neutralize threats autonomously, reducing response time from hours to seconds.

Example: Microsoft's AI-based Defender XDR platform identifies anomalies across endpoints and automatically responds to threats without requiring human intervention.

2. Generative AI and the rise of deepfakes

Generative AI has created new attack vectors, including deepfakes and AI-generated phishing. Threat actors utilize AI to impersonate executives in business email compromise (BEC) schemes or create synthetic identities for fraudulent purposes.

- **Deepfake audio and video manipulation** – AI-generated voices and video footage create convincing impersonations, bypassing traditional authentication mechanisms.
- **Synthetic identity fraud** – AI-generated identities are used to bypass Know Your Customer (KYC) checks and facilitate financial fraud.

Example: In early 2024, a Hong Kong-based company lost $25 million after cybercriminals used an AI-generated deepfake video to impersonate an executive and authorize a fraudulent transaction.

Mahammad Shafi Shaikh
Senior Manager Information System Administration,
Agro Tech Foods Limited

3. AI-Augmented malware and adversarial AI

AI is no longer just a defense mechanism - it is also a weapon in the hands of attackers.

- **AI-Powered malware** – Malware equipped with AI can evade detection by adapting to its environment and learning from security measures implemented by security systems.
- **Adversarial AI attackers** –Attackers use AI to generate misleading data, confuse machine learning models, and bypass AI-based security controls.onds.

Example: In 2024, a major cybersecurity firm discovered malware that utilized AI to dynamically modify its code dynamically, thereby evading detection across multiple platforms.

Future scenarios and strategic implications

1. Autonomous threat response and self-healing networks

Future AI systems will move from reactive to proactive defense, where networks autonomously detect and neutralize threats before they materialize.

- AI-driven Security Orchestration, Automation, and Response (SOAR) platforms will enable real-time threat containment and automated patching, allowing for swift and effective response to threats.

2. Zero trust architecture enhanced by AI

Zero Trust frameworks are increasingly integrating AI to strengthen identity verification and anomaly detection.

- AI will monitor user behavior and continuously evaluate access permissions based on contextual factors.
- AI-enhanced identity and access management (IAM) will reduce insider threats and unauthorized access.

Example: Google's BeyondCorp framework integrates AI for continuous verification, enhancing the effectiveness of Zero Trust models.

3. AI for supply chain tisk management

AI will play a critical role in identifying vulnerabilities within complex supply chains.

- Predictive AI models will assess supplier risk and detect early signs of compromise.
- AI-driven simulations will help model and mitigate supply chain disruptions.

Challenges and risks of AI in cybersecurity

1. Data privacy and ethical concerns

AI models require vast datasets to train effectively, raising concerns about data privacy and regulatory compliance.

- Unauthorized data collection can lead to legal and reputational risks.
- Bias in AI models can result in discriminatory outcomes.

2. Model poisoning and data manipulation

Threat actors are increasingly targeting AI training datasets.

- Poisoned data can corrupt AI models, resulting in false positives or a failure to detect threats.
- CISOs must implement robust data integrity checks and model validation protocols to ensure data accuracy and integrity.

3. Lack of explainability and transparency

AI models often function as "black boxes," making it difficult for security teams to understand decision-making processes.

- Regulatory bodies are pushing for greater transparency in AI-based security tools.
- CISOs must strike a balance between the complexity of AI models and operational clarity.

Best practices to secure AI-based systems

1. Integrate AI into a holistic cybersecurity strategy

AI should complement, not replace, existing security frameworks.

- Adopt a layered defense strategy combining AI with traditional threat detection.
- Continuously update AI models with real-time threat intelligence to enhance their accuracy and effectiveness.

2. Implement AI governance and ethical oversight

Establish a governance framework for AI deployment:

> "AI is no longer just a tool in cybersecurity—it's the battleground. The question is: who's wielding it smarter?"

- Define accountability for AI-based security decisions.
- Ensure AI models comply with industry standards and regulations

3. Invest in AI-driven threat-hunting and red-teaming

Deploy AI to simulate attacks and test network resilience:

- Use AI-based red teaming to identify vulnerabilities.
- AI-driven threat-hunting models can predict attacker behavior and recommend countermeasures.

4. Strengthen AI supply chain security

Secure AI model supply chains from data poisoning and model manipulation:

- Vet AI vendors for security compliance.
- Monitor third-party AI models for anomalies and suspicious behavior.

Conclusion

AI is revolutionizing the cybersecurity landscape, offering unprecedented capabilities in threat detection, automation, and response. However, it also introduces complex risks that demand strategic oversight. For CISOs, the key lies in harnessing AI's strengths while mitigating its vulnerabilities through proactive governance, layered defense strategies, and continuous monitoring. The future of cybersecurity will be shaped by those who can master the AI-cybersecurity nexus - turning AI from a double-edged sword into a strategic advantage. ■

"Exposure is the new frontline in India's battle for AI and cloud security"

Indian enterprises must shift from vulnerability management to secure evolving digital ecosystems.

By **Jagrati Rakheja** | jagrati.rakheja@9dot9.in

AS INDIA digital economy accelerates, so do its cybersecurity challenges. From AI adoption to hybrid cloud complexity, organizations are grappling with an ever-expanding attack surface. In this exclusive interview with CISO Forum, Rajnish Gupta, Managing Director and Country Manager at Tenable India, discusses how Indian enterprises must shift from traditional vulnerability management to exposure management—a proactive approach to identifying, prioritizing, and mitigating cyber risks. He also shares insights into Tenable's latest innovations, sector-specific trends, and how CISOs can better translate technical risks into boardroom language. For security leaders navigating AI, cloud, and compliance, this conversation offers timely and practical perspectives.

CISO Forum: What are Tenable's strategic priorities for the Indian market over the next few years, especially in light of the region's rapid digital transformation?
Rajnish Gupta: As Indian organizations accelerate their digital transformation initiatives and prepare for increased regulatory pressures, there's a need to transition from traditional vulnerability management to exposure management, gaining context to make more informed decisions and proactively secure their expanding attack surfaces.

Following Tenable's acquisition of Vulcan Cyber, to reinforce its commitment to leading the exposure management market, Tenable announced powerful new enhancements to its flagship platform, Tenable One, with the introduction of Tenable One Connectors and customizable risk dashboards.

CISO Forum: With India's data protection laws evolving, how should organizations adapt their cloud and data security strategies to remain compliant while staying agile?
Rajnish Gupta: Data remains central to today's business operations, especially with the widespread adoption of AI technologies, which is leading organizations to store exponentially greater volumes of data in the cloud.

While cloud providers offer significant security features, these may not always be optimally suited to every customer's specific security requirements. Furthermore, the connectivity between cloud environments and a company's on-premises IT systems can create an attractive entry point, allowing hackers to access the entire organizational infrastructure.

Organizations should introduce a well-designed 'exposure management' approach to cybersecurity, that is, identifying, assessing, and then addressing the security risks they are exposed to. Tenable sums this up in three words: 'Know, expose, and close.'

The "know" phase involves understanding cloud resources to pinpoint potential security vulnerabilities. To deliver tangible value, the "expose" phase assesses, prioritizes, and aggregates cyber risks, enabling organizations to concentrate on their most critical issues. Finally, the "close" phase offers the necessary tools and processes to address, mitigate, and resolve identified security problems. This approach goes beyond mere knowledge provision, enabling organizations to address their security challenges efficiently.

CISO Forum: From your conversations with enterprise CIOs and CISOs, what are the most pressing cybersecurity challenges they are grappling with today?
Rajnish Gupta: One of the biggest concerns for CIOs and CISOs today is the widening gap between adopting new technologies and having the proper security measures in place to protect them. Technologies like AI and cloud computing are transforming how businesses operate, delivering unmatched speed and efficiency; however, security is struggling to keep pace with this evolution.

Tenable's Cloud AI Risk Report 2025 found that cloud-based AI is especially vulnerable to misconfigurations that can expose sensitive data, models, and services to manipulation or leakage. As AI tools become more integrated into everyday business operations, these weaknesses can trigger cascading risks across an organization. What is particularly alarming is that most businesses have only addressed a fraction of their AI-related vulnerabilities, leaving critical assets exposed, as the report highlights.

Security teams are also dealing with fragmented visibility due to the rise of multiple siloed tools, making cloud detection and response more difficult than ever. That is why CIOs and CISOs are now shifting focus toward exposure management strategies—ones that go beyond traditional vulnerability management. They're looking for approaches that help them proactively identify, understand, and mitigate risks, not just in cloud infrastructure but also in the AI systems that increasingly power innovation and decision-making.

CISO Forum: In the context of AI-driven environments, what are some of the most underestimated or overlooked cloud security risks that SaaS enterprises should be aware of?
Rajnish Gupta: Cloud and AI are undeniably transforming the way businesses operate for the better. But they also introduce complex cyber risks when combined. The most overlooked aspect of the cloud is the toxic trilogy of critically vulnerable, overly privileged, and publicly exposed cloud assets. Nearly 4 in 10 organizations have toxic combinations in their environments. Tenable's recent report found that approximately 70% of cloud AI workloads contain at least one unremediated vulnerability. Adding to the complexity are JENGA®-style cloud misconfigurations in managed AI services.

"Vulnerability management is no longer enough to defend against the modern attack surface."

With 77% of organizations having the overprivileged default Compute Engine service account configured in Google Vertex AI Notebooks, all services built on it are at risk. Organizations also overlook blocking public access to AI training buckets. Overly permissive buckets are an open invitation for threat actors to poison AI training data.

The shared responsibility model in the cloud requires organizations to secure cloud workloads. Yet, many still don't change default configurations. This means that publicly exposed and overly permissive accounts can be easily compromised, granting unauthorized access, which could result in the potential modification of all files on it.

CISO Forum: How do you see the role of AI and automation evolving in the context of vulnerability management and threat detection?
Rajnish Gupta: Vulnerability management is no longer enough to defend against the modern attack surface. With thousands of vulnerabilities emerging daily and rated as critical, it's challenging to remediate every one. AI and automation are pivotal in cutting through the noise to help security teams understand the context behind risk relationships and prioritize remediation of vulnerabilities that pose the most significant risk to business continuity. This is exposure management, and Tenable is already leveraging AI and automation, enabling organizations to proactively address cyber risk.

Tenable One now features a vast and rapidly expanding ecosystem of out-of-the-box Connectors, enabling seamless integration with widely used third-party tools for endpoint detection and response (EDR), cloud security, vulnerability management, operational technology security, ticketing systems, and more. With new Connectors launching throughout Q2 2025 and beyond, Tenable unifies security data across the enterprise, delivering a comprehensive and actionable view of organizational risk.

At the core of the platform is the Tenable Exposure Data Fabric, a scalable, cloud-native architecture that ingests, normalizes, and connects data across the security ecosystem. This foundation powers Tenable ExposureAI, the platform's machine-learning engine, which surfaces toxic risk combinations and hidden attack paths and prioritizes actions based on their potential business impact.

New unified risk dashboards further elevate the platform's impact. Designed to eliminate time-consuming manual reporting, these dashboards offer fully customizable views that align with specific business roles and priorities. With flexible report configurations and powerful visualization options, security teams can deliver insights and communicate risks faster and with greater business impact.

"Security leaders must translate technical risks into business impact, focusing on revenue, operations, and reputation."

CISO Forum: What industries or sectors in India are showing the most maturity or urgency when it comes to adopting advanced cybersecurity solutions?

Rajnish Gupta: In India, the BFSI sector leads in adopting advanced cybersecurity solutions driven by stringent regulations such as RBI mandates and the sensitive nature of financial data. The healthcare sector follows closely, driven by a surge in ransomware attacks, with a 21.82% share of cyber incidents expected in 2025. IT and telecom also show urgency, as the expansion of 5G, cloud adoption, and IoT significantly increases attack surfaces. The rising threat from nation-state actors has led the government and defense sectors to prioritize cybersecurity, with initiatives such as the National Cybersecurity Strategy enhancing resilience.

Manufacturing is maturing rapidly in India, with organizations integrating IoT security to protect supply chains. These sectors are leveraging AI-driven threat detection and automation to address vulnerabilities proactively. But there's still work to be done. Despite adopting advanced security tools, many organizations struggle with tool sprawl and data silos, leaving security teams to crunch spreadsheets instead of proactively addressing security gaps that pose the most significant risk. This approach must change if India's critical infrastructure organizations want to get ahead of threat actors.

CISO Forum: As cybersecurity becomes a board-level priority, how can security leaders better communicate risk in business terms to the C-suite and board members?

Rajnish Gupta: To effectively communicate cybersecurity risks to the C-suite and board, security leaders must translate technical risks into business impact, focusing on revenue, operations, and reputation. Tenable found that only 3% of vulnerabilities pose significant business risk, reiterating that high-impact exposures need prioritization. Using exposure management, security leaders can unify data from siloed tools, providing a clear view of critical risks and their potential financial or operational consequences. Contextualizing risks in terms of business metrics enhances decision-making. Security leaders should use clear KPIs, such as Vulnerability Priority ratings, to benchmark progress and align with business goals. By speaking in terms of financial impact, CISOs can better communicate risk and secure board support. ■

Small businesses living in a false paradise: Major cybersecurity gaps exposed

Overconfident yet underprepared, small businesses face mounting cyber threats. 2025 should be the year they act—not just believe.

By **Jagrati Rakheja** | jagrati.rakheja@9dot9.in

IN BOARDROOMS across the country, small business owners are nodding confidently during cybersecurity briefings. But in the server rooms below, their IT teams are frantically patching holes with digital duct tape. A startling new report reveals that while 43% of cyberattacks now target small businesses, most companies are dangerously overconfident about their defenses.

The confidence trap: Feeling safe while under fire

In the 2025 State of IT Security Report, Devolutions surveyed 445 small and medium business professionals and uncovered a troubling reality: 71% of SMBs feel confident handling major cyber incidents, yet only 22% have advanced cybersecurity systems in place. This dangerous gap between perception and reality leaves businesses vulnerable when they believe they're secure.

The problem worsens when you consider who is most confident. Company executives report the highest confidence levels, while IT staff – the individuals responsible for managing daily security threats – exhibit the lowest confidence and preparedness. It's like having the captain confident about the ship while the crew sees water rushing in below deck.

Still using spreadsheets to guard the crown jewels

Perhaps most shocking is how businesses manage their most sensitive access credentials. A staggering 52% of SMBs still rely on manual methods, such as spreadsheets or shared password vaults, to control access to critical systems. This means that when hackers want to steal company secrets, they often find the keys conveniently organized in an Excel file.

Recent data indicate that 55% of ransomware attacks target businesses with fewer than 100 employees, underscoring the importance of proper access management for business survival. Yet the report found that cost concerns and lack of awareness keep many companies stuck with these risky manual systems.

The AI promise vs. reality gap

While 71% of SMBs plan to increase their use of artificial intelligence for cybersecurity, 40% aren't currently using any AI tools. The enthusiasm is there, but implementation remains elusive. Many businesses worry about cyberattacks on AI systems themselves (49%) or fear becoming too dependent on automated tools (46%).

Confidence without capability is a liability—especially when your business survival depends on getting cybersecurity right.

This hesitation is understandable, but it could be potentially costly. Industry experts predict that by 2025, 45% of organizations worldwide will experience attacks on their software supply chains, representing a 300% increase from 2021.

Money talks, but not loud enough

The good news? Nearly two-thirds (63%) of SMBs increased their cybersecurity spending in 2024. The bad news? Almost 30% still spend less than 5% of their IT budget on security, and 55% say lack of funding remains their biggest obstacle.
It's like buying a more expensive lock for your front door while leaving the windows wide open.

Training falls behind

The report reveals that only 39% of businesses offer continuous cybersecurity training, while 17% provide no training at all. This is particularly concerning, as most successful attacks still rely on tricking employees into clicking on malicious links or sharing passwords.

Wake-up call for 2025

With 75% of SMBs unable to continue operating if hit with ransomware, the stakes couldn't be higher. The report suggests that 2025 must be the year SMBs move from awareness to action.

The solution isn't perfection – it's building practical, consistent security habits that match real-world risks. As cyber threats continue to evolve, small businesses that bridge the gap between confidence and capability will be the ones still standing when the digital dust settles. ■

The digital battlefield: What's keeping security leaders awake in 2025?

AI tops the list of cybersecurity fears in 2025, but outdated tools and missing basics still keep leaders up at night.

By **Jagrati Rakheja** | jagrati.rakheja@9dot9.in

IT'S 3 AM, and somewhere around the world, a cybersecurity professional gets an alert. Another potential breach. Another sleepless night. This scenario plays out thousands of times daily, as revealed in Arctic Wolf's comprehensive 2025 Trends Report, which surveyed 1,200 IT and security decision-makers across multiple countries.

AI takes the crown as top security concern

For the first time in four years, artificial intelligence has overtaken ransomware as the #1 cybersecurity worry. Nearly 29% of security leaders now rank AI-related threats as their primary concern, pushing ransomware down to second place at 21%. This shift reflects growing worries about AI-powered attacks that can craft more convincing phishing emails and identify system vulnerabilities more quickly than ever before.

However, experts warn against getting too distracted by AI hype. Traditional threats, such as malware, business email compromise, and ransomware, remain everyday realities that cause significant damage to organizations.

The sobering reality of cyber attacks

The numbers paint a concerning picture: 70% of organizations experienced at least one "significant cyber attack" in 2024. Even more alarming, only 25% of security leaders can confidently say their organization has not been breached – a sharp drop from 35% the previous year.

When attacks do succeed, the consequences are severe. Nearly two-thirds of significant cyberattacks resulted in productivity losses lasting at least three months, with some organizations experiencing disruptions for six months or longer.

The ransomware puzzle: Mixed signals

While reported ransomware attacks decreased from 45% to 23% year-over-year, the threat remains serious for those affected. Surprisingly, 76% of ransomware victims still chose to pay the ransom, despite 90% working with professional negotiators who successfully reduced payments in 52% of cases.

What are the main reasons for paying? Preventing stolen data release (50%), speeding up recovery (49%), and having no alternative recovery method (48%).

AI may be the new threat, but poor fundamentals remain the real enemy.

Technology gaps persist despite heavy investment

Despite 84% of organizations investing heavily in cybersecurity, significant challenges remain. A quarter of security leaders report outright dissatisfaction with their security tools, citing high false favorable rates (34%) and a lack of effectiveness (33%) as their top frustrations.

Surprisingly, AI security devices – despite the hype – deliver the least value, according to 18% of respondents, often generating more noise than useful alerts.

The incident response revolution

One notable improvement: incident response (IR) preparedness has significantly enhanced. An impressive 88% of organizations now maintain IR retainers (up from 64% the previous year), and 81% have had to use them. This shows organizations are taking proactive steps to prepare for inevitable security incidents.

However, only 60% maintain current incident response plans, with just 35% having truly up-to-date documentation—a concerning gap in crisis preparedness.

Looking ahead: Balancing hype with reality

As organizations navigate 2025's cybersecurity landscape, the key lesson is clear: while AI represents both opportunity and threat, fundamental security practices remain crucial. Multi-factor authentication, employee training, proper backups, and comprehensive incident response planning still form the backbone of effective cybersecurity.

The organizations that will thrive are those that embrace innovation while maintaining strong security fundamentals – because, in cybersecurity, yesterday's basics are today's lifelines. ■

The AI security tightrope: Business leaders race to innovate, security chiefs hit the brakes

As CEOs accelerate AI adoption, CISOs raise red flags—highlighting a growing divide between innovation ambition and cybersecurity readiness.

By **Jagrati Rakheja** | jagrati.rakheja@9dot9.in

IN CORPORATE boardrooms around the world, a fascinating drama is unfolding. On one side, CEOs are rushing to embrace artificial intelligence, viewing it as the golden key to future profits. On the other side, CISOs are waving red flags, warning that the AI revolution could become a cybersecurity nightmare.

New research from NTT DATA reveals just how wide this gap has become, with business leaders and security chiefs operating in almost parallel universes when it comes to AI adoption.

CEOs betting big on AI revolution

Business leaders are placing massive bets on artificial intelligence, with 89% of CEOs identifying AI as the top technology needed to stay competitive. Nearly all organizations (99%) plan to continue investing in generative AI through 2026.

AI is revolutionizing industries from healthcare—where it analyzes medical data to predict patient outcomes—to manufacturing, where it streamlines production. Financial services use AI for fraud detection and intelligent customer service.

Security chiefs sound the alarm

However, CISOs are putting the brakes on. While 94% of business leaders plan to increase security spending due to the adoption of AI, 88% of organizations express serious concerns about AI-related security risks.

The disconnect is stark: only 38% of CISOs agree their organization's AI and cybersecurity strategies are correctly aligned, compared to 51% of CEOs. Nearly half (45%) of security chiefs feel "pressured, threatened, or overwhelmed" by AI adoption—a sentiment shared by only 19% of other executives.

The growing threat landscape

Security experts have good reason to be concerned. Cybercriminals are leveraging AI to craft sophisticated phishing emails and automate the discovery of software vulnerabilities. AI systems face unique threats, including adversarial attacks that manipulate input data, data poisoning that corrupts training information, and algorithmic bias that undermines system reliability.

Only 44% of executives believe their organizations can manage privacy risks from data poisoning attacks.

The skills gap challenge

Adding to security leaders' concerns, 69% admit their teams lack the skills to work with rapidly evolving AI technology. Meanwhile, 72% of organizations still lack formal policies for AI usage, and 82% find government AI regulations unclear.

We can't secure what we don't fully understand—and with AI, that gap is growing faster than ever.

Finding the balance

The report reveals that only 39% of businesses offer continuous cybersecurity training, while 17% provide no training at all. This is particularly concerning, as most successful attacks still rely on tricking employees into clicking on malicious links or sharing passwords.

Wake-up call for 2025

Security experts recommend enhancing AI visibility across organizations, developing comprehensive security policies, embedding security by design, prioritizing data protection, conducting rigorous testing, and maintaining continuous monitoring.

The challenge ahead is clear—organizations must harness AI's transformative power while building robust defenses against emerging risks. Success requires bridging the gap between innovation-focused executives and security-minded CISOs. ■

The looming quantum threat: Why we must act now to secure cryptography

Quantum computing won't wait. With encryption at risk, organizations must migrate to post-quantum cryptography now—or risk future exposure.

By **Dr. Sandeep K. Shukla** | editor@cioandleader.com

FOR YEARS, IBM and other global technology leaders have been making steady progress toward the realization of quantum computing. Alongside them, countries such as China have also claimed moderate success in developing quantum capabilities. While these advancements represent a significant milestone in computing, they also pose a critical security threat that cannot be ignored.

The quantum computing security challenge

Much of today's cryptographic security infrastructure relies on the hardness of certain mathematical problems. These include integer factorization (which underpins RSA encryption) and the discrete logarithm problem (used in Diffie-Hellman key exchange). The security of these cryptographic systems is based on the assumption that no efficient algorithm exists to solve these problems in polynomial time. If quantum computing reaches a level where these problems can be solved efficiently, most of our existing public-key cryptography will become obsolete.

The ramifications are severe. The entire security framework used to protect financial transactions, government communications, and personal data would be at risk. We have become deeply dependent on these cryptographic methods, and without viable replacements, our ability to secure digital information would be in jeopardy.

The state of quantum computing

Some experts argue that practical quantum computing capable of breaking encryption is still 10 to 20 years away. Even Google's recent announcement of its Willow quantum processor, which boasts 123 qubits, is still far from the threshold needed to break modern asymmetric cryptographic systems. Experts estimate that to pose a real threat, quantum computers would need thousands of stable qubits. However, the possibility of a "quantum surprise"—a sudden breakthrough in secrecy—remains a major concern.

Even without an immediate threat, the long-term implications demand urgent action. Many governments and enterprises need their confidential data to remain secure for decades. If an adversary intercepts encrypted communications today, they could store the data and decrypt it later when quantum computing reaches maturity. This is known as the "record now, decrypt later" strategy, and it presents a significant threat to national security, banking, and sensitive corporate information.

Preparing for the quantum threat

The U.S. National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) have already issued guidelines urging federal agencies to prepare for quantum-safe cryptography. India's Ministry of Electronics and Information Technology has circulated similar documents, though they have yet to be mandated. Enterprises and governments must begin transitioning to quantum-resistant cryptographic methods now, rather than waiting until quantum computers become a clear and present danger.

> "We're not just preparing for the future—we're defending the present from the possibility of a quantum surprise."

The first step in quantum preparedness is identifying all instances where vulnerable cryptography is being used. This includes software, embedded systems, secure communication protocols, and digital certificates. Organizations must create a comprehensive cryptographic inventory—often referred to as a cryptographic bill of materials (CBOM)—to understand their exposure.

Once vulnerabilities are identified, organizations need to assess the risk associated with each use case. Some legacy systems may be decommissioned before quantum threats materialize, while others may need urgent upgrades. The next crucial step is achieving cryptographic agility, which allows organizations to swiftly replace existing cryptographic algorithms with quantum-safe alternatives without requiring extensive system overhauls.

The role of post-quantum cryptography (PQC)

NIST has been leading a global effort to standardize post-quantum cryptographic algorithms since 2015. The process has involved multiple rounds of rigorous evaluation and testing. In 2024, NIST finalized its selection of three quantum-safe algorithms:

- **Crystal Kyber –** A key encapsulation algorithm based on lattice-based cryptography.
- **Crystal Dilithium –** A digital signature algorithm that is also lattice-based.

- **SPHINCS+ –** A stateless hash-based signature scheme.

Lattice-based cryptography is believed to be quantum-resistant due to its reliance on complex geometric problems that quantum algorithms struggle to solve efficiently. However, these algorithms are not mathematically proven to be quantum-safe; they have merely withstood all known quantum attacks so far. This underscores the need for continued monitoring and adaptability in cryptographic implementations.

Challenges in implementing PQC

Transitioning to PQC is not as simple as swapping out one algorithm for another. Public key infrastructure (PKI) systems, which issue digital certificates, will need to be updated to support these new algorithms. Given that the current PKI ecosystem took decades to establish, integrating quantum-safe alternatives will require significant effort and time.

Moreover, real-world implementation poses challenges. Cryptographic algorithms often have vulnerabilities not in their theoretical design but in their software and hardware implementations. The infamous OpenSSL Heartbleed vulnerability in 2014 serves as a reminder that flawed implementations can render even the strongest algorithms ineffective. Side-channel attacks, where adversaries extract cryptographic keys by analyzing system behavior, remain a pressing concern. Ongoing research is needed to develop hardened implementations resistant to these threats.

India's role in quantum security

India has recently launched a national quantum mission aimed at fostering indigenous quantum technology development. As part of this initiative, research institutions such as IIT Kanpur are actively working on implementing and testing PQC algorithms. While India currently follows NIST's guidelines, there is a possibility that it will develop its own quantum-safe standards tailored to its unique security needs.

Dr. Sandeep K. Shukla
Chair Professor in Cybersecurity at IIT Kanpur

For Indian enterprises and government agencies, waiting for a government mandate may be too late. The financial sector, in particular, should start planning its quantum transition now. The Reserve Bank of India (RBI) and other regulatory bodies must issue clear directives on PQC adoption timelines, mirroring efforts by NIST and DHS.

The urgency of quantum preparedness

Despite the 10- to 20-year horizon for large-scale quantum computing, organizations cannot afford to delay. The process of migrating to quantum-safe cryptography will take years, and the threat of retrospective decryption is real. The Moskowitz Theorem underscores this urgency: if the time required to deploy quantum-safe algorithms (Y) plus the number of years data must remain confidential (X) exceeds the estimated time to practical quantum computing (Z), then organizations are at risk.

Governments and enterprises must take proactive steps now:

- **Identify quantum-vulnerable cryptography –** Conduct a cryptographic inventory to locate weak algorithms in use.
- **Assess risks and prioritize migration –** Determine which systems need immediate transition to quantum-safe alternatives.
- **Achieve cryptographic agility –** Develop flexible cryptographic frameworks that allow for seamless algorithm replacement.
- **Adopt PQC algorithms –** Begin implementing NIST-approved quantum-resistant cryptography.
- **Upgrade PKI infrastructure –** Ensure that digital certificates support quantum-safe key exchanges and signatures.
- **Monitor cryptographic advances –** Stay informed about new vulnerabilities and advancements in PQC.

Conclusion

The threat of quantum computing to modern cryptography is no longer theoretical—it is a matter of when, not if. Organizations must start planning their transition to quantum-safe cryptography today. Regulatory bodies must enforce mandates to accelerate migration, and enterprises must embrace cryptographic agility to future-proof their security frameworks. Waiting until quantum computers become powerful enough to break today's encryption will be too late. The time to act is now.

(This article summarizes a talk given by Dr. Sandeep K. Shukla, Chair Professor in Cybersecurity at IIT Kanpur, at the CISO Forum in December 2024. Some content has been edited for brevity.) ■

Why CISOs must think like CEOs!

TECHNOLOGY NO longer just supports business—it defines it. From startups to global giants, every organization is swept up in the tide of digital transformation.

As a leading cybersecurity expert remarked during a panel discussion I moderated, the pace of change has created a "FOMO effect"—falling behind is no longer an option. Yet, while digital acceleration is shaping core business strategies, cybersecurity often lags behind. This disconnect must be addressed, and the shift begins with a new mindset:

CISOs must think like CEOs. That means aligning cybersecurity with business priorities, owning the enterprise risk narrative, and positioning security not as a cost center or a roadblock, but as a strategic business enabler. In today's hyperconnected world, digital trust is the foundation upon which innovation, resilience, and long-term value are built. Without it, even the most advanced technologies can falter.

Of course, cybersecurity maturity varies—some organizations are still plugging gaps, while others are re-architecting from the ground up. But transformation doesn't require perfection; it demands awareness, intent, and agility.

Regulations, operating models, and budget constraints all shape this journey. Still, forward-looking organizations evolve incrementally by identifying risks early and adapting continuously. At the same time, CISOs must recognize that jargon has no place in the boardroom. Boards don't need a technical deep dive, they need clarity on business risk, potential impact, and the associated costs.

With only a few minutes to make their case, CISOs must speak the language of business—connecting cybersecurity to continuity, competitiveness, and measurable outcomes. The pandemic, followed by a surge in ransomware and systemic attacks, has elevated cybersecurity from a top-10 concern to a top-3 boardroom issue.

Cybersecurity is no longer just an IT responsibility—it's an enterprise-wide imperative. That's why today's CISOs must evolve from being guardians of infrastructure to becoming leaders of business resilience. ■

While digital acceleration is shaping core business strategies, cybersecurity often remains a step behind. This disconnect must be addressed, and the shift begins with a new mindset.

Jatinder Singh
Executive Editor, CISO Forum
jatinder.singh@9dot9.in

CISOFORUM

Security For Growth And Governance

Where CISOs Connect, Innovation Ignites

Join the **CISO Forum LinkedIn Group** - a dynamic community where top security leaders like YOU connect, collaborate, and exchange insights. With active engagement, it's the ultimate platform to stay informed, inspired, and ahead in the fast-evolving cybersecurity landscape.

Acquaint with curated content, expert perspectives, and thought leadership designed specifically for today's CISO & security experts.

The CISO Forum community is your gateway to insightful discussions, emerging technologies, and practical strategies - empowering you to lead with confidence in an ever-changing security environment.

Expand your network with the brightest minds in cybersecurity.

Join the CISO Forum LinkedIn Group today and elevate your leadership journey.

Follow us on @CSO Forum

Scan the QR code to follow

You can also visit us at:
https://www.csoforum.in

RNI No. DELENG/2012/42736

AMD PRESENTS

26th Annual Conference

CIO&LEADER

AI: From Pilot to Production

1st-3rd August, 2025 • Ritz Carlton, Pune

CO-PRESENTED BY NxtGen

#CIOandLeaderConference

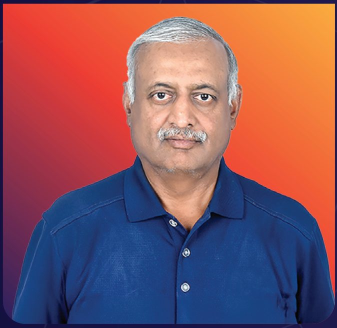
The 26th Annual CIO&Leader Conference is not just another tech gathering. It is a curated leadership experience where India's most forward-thinking CIOs converge to discuss, debate, and drive the transition of AI from experimentation to enterprise-wide impact. Over three dynamic days, the conference will bring together 200+ top CIOs and IT leaders, global AI experts, and many more.

Eminent Speakers @26th Annual CIO&Leader Conference

Guest of Honour

Shri Adv Ashish Shelar

Minister for Information Technology & Cultural Affairs, Government of Maharashtra



Partha Iyengar
Ex-Gartner Fellow, Country Manager Research (India), Gartner, HBR Author, Ex Board Member SBI, Speaker, Advisor

Prof Balaraman Ravindran
Head: Wadhwani School of Data Science & AI / Robert Bosch Centre for Data Science & AI / Centre for Responsible AI, IIT Madras

Anil Kumble
PadmaShri awardee and former captain & coach of the Indian cricket team

Annu Kapoor
Actor, singer, director, radio disc jockey and television presenter

Dr. Nitish Bharadwaj
Director, screenplay writer, actor, orator, and spiritual thinker

Chaitanya Devadhe
Indian Idol Season 15 finalist

Mohan Radhakrishnan
Acknowledged to be a voice reminiscent of Kishore Kumar

Know more: **https://annualconference.cioandleader.com/** **Follow us:** in **@CIOandLeader**

For partnership inquiries, write to **Hafeez Shaikh, hafeez.shaikh@9dot9.in, +91 9833103611**

PRESENTING PARTNER: AMD | CO-PRESENTING PARTNER: NxtGen | CO-POWERED BY PARTNERS: freshworks, TATA COMMUNICATIONS, VERTIV | GOLD PARTNERS: SentinelOne Secure Tomorrow, UNICOM, neat.

ASSOCIATE PARTNERS: DELTA, neysa | EXHIBIT PARTNERS: Barracuda Your business, secured., infraon Powered by EverestIMS | MEDIA PARTNER: CNBC TV18 | CONCEPT BY: CIO&LEADER, IT NEXT, 100