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

OCTOBER 2025
SUPPLEMENT OF CIO&LEADER

CISOFORUM

Security For Growth And Governance

SECURING THE FUTURE

How India's CISOs are building enterprise resilience, governing AI risks, and enabling secure innovation amid rising volatility

Business Observability SPECIAL

Aravindan Raghavan
Quest Global

Anil Kuril
Union Bank of India

Dr. Pawan Kumar Sharma
Tata Motors

Ashwini Kumar Pandey
Punjab National Bank

CIO&LEADER **studiotalks**

CIO&LEADER STUDIOTALKS—
WHERE TECHNOLOGY MEETS THE SPOTLIGHT!

CIO&Leader proudly presents StudioTalks—a premium platform where India's most influential CIOs and CTOs take center stage. Captured with high-production aesthetics, sleek visuals, and dynamic backdrops, StudioTalks transforms leadership insights into an engaging cinematic experience, and brings India's most influential CIOs and CTOs into the spotlight.
This exclusive series explores visionary leadership, emerging technologies, and strategic transformation—all presented in a format that blends deep insights with the visual polish of a professional studio production.

WHY JOIN STUDIOTALKS?

Engage in powerful conversations that shape the future of enterprise IT.

Share your expertise in a high-impact, TV-style format.

Be featured among India's top technology leaders.

Be the voice of transformation. Be part of CIO&Leader StudioTalks.

SECURE YOUR SPOT NOW!

For more information
Jatinder Singh
Executive Editor - Enterprise Tech
jatinder.singh@9dot9.in, +919718154231

For Business Proposal
Hafeez Shaikh
National Sales Head, B2B Tech,
hafeez.shaikh@9dot9.in, +91 9833103611

Follow us: @CIOandLeader

The Quantum Dilemma: Prepare or Perish

ONCE A theoretical scientific pursuit, quantum computing is edging closer to commercial reality. Recent breakthroughs—from Google's Willow processor to significant advances in error correction and qubit stability—have accelerated what many anticipated would remain a distant threat.

For CISOs, this isn't merely the advent of another technology wave—it's the dawn of a cryptographic reckoning. The mathematics underpinning algorithms such as RSA, Diffie-Hellman, and ECC—mainstays of secure digital communication—will crumble before the computational might of a mature quantum machine. The repercussions extend beyond encryption alone: digital identities, blockchain systems, secure tunnels, and zero-trust architectures all depend on these primitives.

The problem is not tomorrow's risk; it's today's data. Information harvested now could be decrypted later, once quantum capabilities mature—a "store now, decrypt later" scenario already being exploited by advanced threat actors. The business impact is profound: quantum decryption could destabilize compliance frameworks, shatter reputational safeguards, and threaten the very continuity of enterprise operations.

CISOs must now step forward as strategic architects, shaping their organization's cryptographic transition with urgency and clarity. First, conduct a comprehensive cryptographic inventory—identify where vulnerable algorithms reside across your infrastructure. Second, prioritize migration of your most sensitive data and communications to post-quantum cryptography. Finally, establish a quantum readiness program with executive sponsorship and dedicated resources.

The transition to post-quantum cryptography is not a one-time upgrade—it's an organizational transformation. CISOs must champion the narrative: preparing for quantum is about securing digital longevity, not just warding off hypothetical attacks. Today's decisions will define whether tomorrow's data remains secure, or becomes a legacy liability.

The quantum era will test the CISO's capacity for long-range thinking. Security leaders have guided their enterprises through cloud, AI, and zero-trust revolutions. Now, they must navigate the next frontier—where cryptography itself must evolve. The question is not when quantum computing will arrive, but whether your defenses will be ready when it does.■

"Preparing for quantum is about securing digital longevity"

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

CONTENTS OCTOBER 2025

COVER STORY

Cover Design by:
Manish Kumar

Please Recycle This Magazine And Remove Inserts Before Recycling

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**

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

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

SALES & MARKETING
Senior Director - B2B Tech: **Vandana Chauhan**
Head - Brand & Strategy: **Rajiv Pathak**

National Sales Head - B2B Tech: **Hafeez Shaikh**
Reginal Sales Head - North: **Sourabh Dixit**
Senior Sales Manager - South: **Aanchal Gupta**

COMMUNITY ENGAGEMENT & DEVELOPMENT
Head - Databases: **Neelam Adhangale**
Senior Community Manager: **Vaishali Banerjee**
Senior Community Manager: **Reetu Pande**
Senior Community Manager: **Snehal Thosar**

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

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

For editorial queries write to:
editor@cioandleader.com

For sales/business queries write to:
responses@cioandleader.com

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, Printed and Owned by 9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
Published and printed on their behalf by Vikas Gupta. Published at 121, Patparganj, Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091, India. Printed at G. H. Prints Private Limited, A-256 Okhla Industrial Area, Phase-I, New Delhi - 110020.

Editor: **Vikas Gupta**

Vaibhav Sonavane appointed as CISO at CSB Bank Limited

CSB Bank has appointed **Vaibhav Sonavane** as **Chief Information Security Officer (CISO).** With 18 years of expertise in cloud security, risk management, and enterprise security architecture, he will lead the bank's cybersecurity strategy, compliance, and innovation. Formerly at Axis Bank, Vaibhav built the Cloud Security CoE and has held senior roles at Oracle, PwC, Wipro, and JLT Asia.

Aarti Bansal Lamba elevated to Head – Cyber Risk Governance at Wipro

Wipro has promoted **Aarti Bansal Lamba** to **Head – Cyber Risk Governance.** With over 15 years of experience in cybersecurity, compliance, and risk management, she will lead Wipro's cyber risk governance agenda. Since joining in 2022, she has driven AI-led security initiatives and frameworks, previously holding leadership roles at DXC Technology, SBI Card, EXL, PwC, and KPMG.

Sridhar Govardhan appointed as Group CISO at Angel One

Angel One has appointed **Sridhar Govardhan** as **Group Chief Information Security Officer (CISO).** With over two decades of experience in cybersecurity strategy, governance, and innovation, he will strengthen Angel One's information security roadmap. Previously, he held leadership roles at CoinDCX, Flipkart, and Wipro, driving enterprise-wide security transformations and advancing India's digital resilience across industries.

Alok Malik elevated to SVP, Global IT & Security (CIO & CISO) at GlobalLogic

Alok Malik has been elevated to **Senior Vice President, Global IT & Security (CIO & CISO)** at **GlobalLogic.** Based in Santa Clara, he will lead global IT, cybersecurity, and digital infrastructure strategy. With over 20 years at GlobalLogic, Alok has driven transformation initiatives worldwide and continues advancing cybersecurity innovation through advisory roles at BayAreaCISO and Cyber AI Commune.

Murtaza Bhatia joins Sify Technologies as VP & Practice Head – Cybersecurity

Murtaza Bhatia has joined **Sify Technologies** as **Vice President & Practice Head – Cybersecurity.** With over two decades of expertise in cybersecurity sales, consulting, and transformation, he will lead innovation and growth across India. Previously with NTT DATA, NTT Ltd., and Dimension Data, Murtaza has driven national security initiatives and enterprise resilience through advanced technology solutions.

Prajeesh K G appointed as CISO at Muthoot Capital Services Ltd – India

Prajeesh K G has been appointed **Chief Information Security Officer (CISO)** at **Muthoot Capital Services Ltd – India.** With nearly two decades of experience across financial services, retail, and technology sectors, he will lead the company's information security strategy. Previously with Joyalukkas, ESAF Bank, Dhanlaxmi Bank, and Wipro, Prajeesh excels in SOC operations, GRC, cloud security, and threat intelligence.

Durga Bharath Attaluri appointed as CISO & DPO at Bosch Global Software Technologies

Durga Bharath Attaluri has been appointed **Chief Information Security and Data Protection Officer** at **Bosch Global Software Technologies.** With over two decades of experience in compliance, governance, privacy, and cybersecurity, he will lead enterprise-wide security and data protection. Previously with Wipro, Honeywell, IBM, and Genpact, Durga has driven global GDPR, AI privacy, and compliance transformation initiatives across 60+ countries.

Lalit Lakhanpal appointed as CISO at JioBlackRock Investment Advisers

Lalit Lakhanpal has been appointed **Chief Information Security Officer (CISO)** at **JioBlackRock Investment Advisers.** With over two decades of experience in cybersecurity, IT security, and compliance, he will lead the firm's information security strategy. Previously with Avenue E-Commerce, Holcim, Edelweiss, GEP Worldwide, Travelex, and Syntel, Lalit has driven large-scale security transformations and strengthened enterprise cyber resilience.

AI ushers in an era of preemptive cybersecurity

Gartner predicts over half of security spending will shift to AI-powered, preemptive defense as reactive methods become obsolete.

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

THE CYBERSECURITY world is about to flip upside down. While companies today spend most of their security budgets playing defense—waiting for attacks to happen and then scrambling to respond—a new Gartner report reveals this reactive approach is becoming dangerously outdated in the age of AI-powered threats.

The Big Shift: From Firefighting to Fire Prevention

By 2030, more than half of all IT security spending will go toward "preemptive cybersecurity" technologies—a dramatic jump from less than 5% today. These aren't your typical antivirus programs. Instead, they use advanced AI and machine learning to predict and stop attacks before they even begin

Think of it like having a security guard who can see into the future, spotting trouble before it arrives at your door.

Why the Change is Urgent

The numbers tell a sobering story. Gartner predicts that documented cybersecurity vulnerabilities will balloon to over 1 million by 2030—a 300% increase from today's roughly 277,000. Carl Manion, a Managing Vice President at Gartner, warns that traditional "detect and respond" methods simply won't cut it against AI-enabled attackers.

"Organizations will need to deploy countermeasures that act preemptively and independently of humans," Manion explains.

> "Organizations will need to deploy countermeasures that act preemptively and independently of humans,"
>
> **Carl Manion,** Managing Vice President, Gartner

Enter the Cyber Immune System

The ultimate vision? An "Autonomous Cyber Immune System" (ACIS) that works like your body's natural defenses—automatically identifying and neutralizing threats without human intervention. While still in early development, this technology represents the future of digital protection.

Specialization is Key

Gone are the days of one-size-fits-all security solutions. The future belongs to specialized tools designed for specific industries—whether that's healthcare systems, manufacturing plants, or financial networks. This shift will create new opportunities for security vendors to carve out niche markets.

The Bottom Line

As cyber threats become more sophisticated and automated, our defenses must evolve too. Companies that cling to reactive security strategies risk exposing themselves to unprecedented dangers. The message is clear: it's time to stop chasing hackers and start staying ahead of them. ■

Cybercrime at Machine Speed: Defenders Are Falling Behind AI-Driven Attacks

Fortinet reports cybercriminals using AI, automation, and CaaS to exploit vulnerabilities faster than defenders can respond, demanding proactive exposure management.

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

THE FORTINET Global Threat Landscape Report 2025 reveals a digital battlefield where attackers increasingly outpace defenders. Automation, AI, and industrialized cybercrime have sharply reduced the time between vulnerability disclosure and exploitation. In 2024, active reconnaissance rose 16.7%, with over 36,000 scans per second targeting exposed services like SIP, RDP, and IoT, highlighting accelerating exploitation speed.

The Rise of AI-Powered Crime

AI has become a powerful weapon in the cybercriminal toolkit. Tools like FraudGPT, BlackmailerV3, and ElevenLabs are enabling deepfakes, phishing sites, and synthetic voice attacks at scale. Cybercrime-as-a-Service ecosystems now let low-skilled actors buy malware and stolen credentials. FortiGuard Labs reports a 42% rise in compromised credentials and a 500% surge in infostealer activity, driven by Redline and Vidar.

Cloud and IoT: The New Frontlines

The cloud remains a prime target, with attackers exploiting misconfigurations, open APIs, and identity abuse. In 70% of cloud compromises, adversaries logged in from unfamiliar geographies. IoT devices like routers, cameras, and firewalls are also hijacked for botnets and persistence. Asia-Pacific is most targeted, accounting for 42% of global exploitation attempts.

> "Active reconnaissance increased by 16.7%, with over 36,000 scans per second targeting exposed services."

Ransomware and Hacktivism Blur Lines

The ransomware ecosystem remains fragmented but potent. Thirteen new ransomware groups emerged in 2024, led by RansomHub, LockBit 3.0, and Play, which together accounted for over a third of all attacks. Alarmingly, hacktivists are now adopting ransomware tactics, merging ideological motives with financial gain. Telegram remains their favored hub for coordination.

From Defense to Exposure Management

Fortinet's key takeaway is clear: static defenses are no longer enough. The report calls for Continuous Threat Exposure Management (CTEM), emphasizing proactive exposure monitoring, adversary simulations, and automation. With cyberattacks evolving at machine speed, defenders must act faster, think smarter, and anticipate threats before they strike. ■

Airtel wins Indian Railways cybersecurity contract

Airtel Business will build a 24/7 AI-powered cybersecurity center to protect critical data and operations nationwide.

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

AIRTEL BUSINESS has won a major multi-year contract to safeguard the digital backbone of Indian Railways, one of the world's largest transportation networks. The deal, will see the company build a comprehensive 24/7 cybersecurity operations center to protect millions of daily transactions and sensitive passenger data.

Massive scale of operations

Indian Railways operates over 13,000 trains daily, serving more than 20 million commuters while handling 1.5 billion tons of freight annually. This generates enormous volumes of sensitive data, including payment details, ticketing information, and operational databases that require robust protection against increasingly sophisticated cyber threats.

Advanced security architecture

The new Indian Railway Security Operations Centre (IRSOC) will deploy cutting-edge technology, including AI-driven threat detection systems, advanced endpoint protection, and real-time monitoring across 26 locations covering 160,000 employees. Notably, the solution will incorporate "Make in India" cybersecurity products alongside market-leading technologies.

Key capabilities include an industry-leading threat detection time of under 20 seconds, unified compliance monitoring, and protection for over 190,000 critical infrastructure assets. The system will also feature dark web monitoring and behavioral analytics to predict and neutralize threats before they impact operations.

> "Cyber security is of the utmost importance due to increased reliance on digital technologies,"
>
> **Dilip Kumar,** Executive Director, Railway Board

Protection recommendations

"Cyber security is of the utmost importance due to increased reliance on digital technologies," said Dilip Kumar, Executive Director, Railway Board. The centralized security operations center will enable continuous monitoring, efficient threat response, and collaboration with national cybersecurity agencies.

For over 1 billion Indians who rely on railway services for travel, freight, and digital transactions, this enhanced security infrastructure promises safer and more reliable access to essential transportation services. ■

New Security Platform Aims to Simplify Multi-Customer Management

Advanced tools promise to streamline operations and reduce costs for service providers managing cybersecurity

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

CISCO HAS launched a major upgrade to its Security Cloud Control platform, introducing capabilities specifically designed for managed service providers (MSPs) that handle cybersecurity for multiple clients simultaneously.

Single Dashboard for Multiple Clients

The enhancement allows MSPs to manage all their customers from one unified interface, eliminating the need to juggle numerous platforms and logins. Industry partners have praised this consolidation, with one noting they currently deal with over 15 different tools—a problem Cisco's solution aims to solve.

The platform integrates with Cisco's Hybrid Mesh Firewall, which protects organizations across data centers, cloud environments, and remote locations. Recent independent testing showed Cisco's firewall software blocked between 99.5% and 100% of threats, demonstrating strong security efficacy.

> "MSPs are on the front lines, helping businesses navigate the complexities of modern cybersecurity, especially as AI makes threats more sophisticated."

Business Benefits

For service providers, the new system promises three key advantages: faster customer onboarding, reduced operational expenses through automation, and easier opportunities to expand service offerings. The centralized approach cuts down manual work and human errors while providing precise control over which staff members can access specific customer accounts.

"MSPs are on the front lines, helping businesses navigate the complexities of modern cybersecurity, especially as AI makes threats more sophisticated," said Jeetu Patel, Cisco's President and Chief Product Officer.

Availability and Impact

The multi-customer management features are expected to become generally available in February 2026. MSPs will be able to choose between different licensing models, including enterprise agreements and consumption-based options, giving them flexibility in how they structure services for clients.

As cyber threats grow more advanced with AI, this platform could significantly reduce the complexity burden on security service providers while improving protection for the businesses they serve. ■

Asia-Pacific Faces Rising Cybercrime Threats from "Enterprising Adversaries"

Asia-Pacific faces corporate-style cybercriminal networks, with targeted ransomware, laundering marketplaces, and language-specific malware driving regional threats.

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

A NEW CrowdStrike report reveals a troubling evolution in cybercrime across Asia-Pacific and Japan (APJ), where threat actors now operate with corporate-level efficiency and strategic precision. These "enterprising adversaries" execute attacks with scalable infrastructure and business-like discipline, focusing on maximizing impact.

Ransomware Strikes Selectively

From January 2024 to April 2025, 763 APJ organizations appeared on ransomware leak sites, with India, Australia, Japan, Taiwan, and Singapore most affected. Though the region holds over half the global population, it accounted for only 9% of ransomware cases. Manufacturing, technology, and financial services suffered most. Notably, major ransomware groups largely avoided China, with some explicitly prohibiting attacks to avoid legal repercussions.

Underground Markets Fuel Criminal Activity

Chinese-language criminal marketplaces like Chang'an and FreeCity continue thriving despite government crackdowns, hosting a wide range of illicit services while prioritizing anonymity to evade law enforcement. The most notable platform, Huione Guarantee in Cambodia, enabled an estimated $27 billion in transactions tied to money laundering and "pig butchering" cryptocurrency scams. In May 2025, U.S. authorities labeled Huione a money-laundering concern, resulting in its shutdown.

"These 'enterprising adversaries' execute attacks with scalable infrastructure and business-like discipline, focusing on maximizing impact."

Targeted Attacks on Local Users

Chinese and Japanese speakers face targeted threats from malware like ChangemeRAT, ElseRAT, and WhiteFoxRAT, spread through fake software downloads and built to detect Chinese-language systems. Financial institutions across Bangladesh, India, Japan, Malaysia, and nearby regions are also attacked by SOLAR SPIDER through transaction-themed phishing campaigns delivering malware.

Vietnam's Social Media Focus

Vietnamese cybercriminals have specialized in compromising social media business accounts with significant advertising budgets. In 2024, authorities prosecuted over 20 individuals whose

What This Means

The report underscores how cybercriminals are professionalizing operations and exploiting regional vulnerabilities. Organizations must adopt AI-powered security, phishing-resistant authentication, and full visibility, demanding equally advanced defensive strategies to stay ahead. ■

IT Teams Think They're Resilient—But the Data Tells a Different Story

IT teams overestimate resilience—broken workflows, not tech gaps, undermine preparedness, morale, and customer experience.

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

A NEW SolarWinds report reveals a troubling disconnect: while 88% of IT professionals believe their organizations are operationally resilient, their day-to-day struggles suggest otherwise.

The Confidence Gap

Surveying over 600 IT leaders across nine countries, the research found one-third consider themselves "very resilient." Yet confidence drops sharply when addressing core challenges like AI adoption, cybersecurity, and remote-work management, with only half or fewer ratingthemselves highly effective. The impact is personal—over two- thirds say resilience affects job satisfaction and security. When systems fail,morale falls too.

Where Teams Struggle Most

The culprit isn't what you'd expect. Despite 87% believing they have the right technology, resilience gaps persist due to workflows. Over 51% cite broken processes, 36% blame staffing, and only 13% point to tools. Yet organizations still default to tech- first fixes, overlooking how people actually use those tools.

"While 88% of IT professionals believe their organizations are operationally resilient, their day-to-day struggles suggest otherwise."

The Cost of Firefighting

Resource allocation reveals deeper issues. Nearly two-thirds of IT teams spend 11–30% of their budget on service disruptions, yet higher spend doesn't guarantee resilience—strategy does. Time data shows 70% resolve critical issues within a quarter of their time, while 10% spend over half their time firefighting, leading to higher costs, lower morale, and 50% higher reports of understaffing—signaling workflow and tooling problems, not true staffing shortages.

Customer Experience on the Line

The stakes are high. Seventy-one percent cite customer experience as their most significant pain point from outages, while 32% report direct revenue loss. In e- commerce, even a 500-millisecond latency increase noticeably reduces activity. Brand damage affects 28% of organizations, resulting in long-term financial consequences that extend beyond immediate revenue losses.

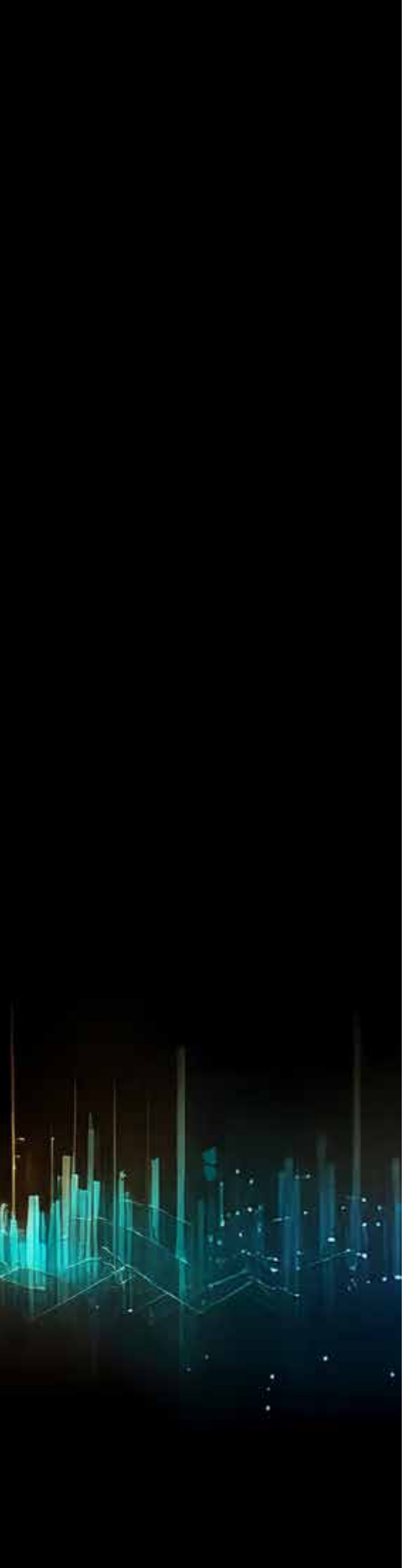
The Path Forward

The report recommends a systems-first approach: map team relationships before adopting new tools or hiring. Understanding interactions and friction points clarifies whether organizations need better processes, more staff, or different technology. As distributed workforces and AI increase complexity, operational resilience becomes essential for survival. Achieving it demands honest assessment of current capabilities and fixing workflow issues before implementing technology. ■

SECURING THE FUTURE

A look at how Indian CISOs are confronting complexity, enabling innovation, and reclaiming control in uncertain times

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



THE CISO Forum conducted a nationwide survey of CISOs and IT security leaders from large enterprises between June and August 2025. Combining quantitative and qualitative research methods, the study examined how Indian organizations are reimagining cybersecurity in a rapidly evolving digital and regulatory landscape.

The report reveals a cybersecurity landscape in rapid transition, shaped by digital transformation, regulatory pressures, and emerging technologies. The findings reveal a pivot toward proactive strategies, deeper business alignment, and operational modernization. CISOs are managing an expanding attack surface from AI/ML, cloud, and remote work, while grappling with compliance obligations and persistent talent shortages.

Most organizations are moving beyond reactive security, embracing proactive risk management, integration with business functions, and automation. However, challenges remain around regulatory compliance, operational visibility, talent management, and adapting to new technologies such as AI/ML and cloud-native applications.

This year's survey data provides a nuanced snapshot of how Indian enterprises are prioritizing targeted controls over wholesale security overhauls, reflecting the growing complexity of their digital operations.

Indian CISOs report widespread use of multi-metric risk quantification and a noticeable maturing of board- level engagement, with business- centric cyber metrics now in high demand. As threat intelligence becomes more integrated and proactive, cross-functional governance models are gradually replacing compliance only approaches.

Yet, the confluence of rapid regulatory change, driven by frameworks like DPDP and ongoing skill gaps continues to stretch and test the resilience of security teams, underscoring the urgent need for continual adaptation and investment in advanced, automated security solutions.

Key Takeways:

- **Cybersecurity strategies are evolving:** Most organizations have moved beyond reactive postures, embracing structured and proactive approaches, with nearly 80% conducting scheduled reviews or defined-trigger-based adjustments.
- **Digital transformation is a security driver:** While only 1% felt overwhelmed, over 85% had to make targeted or significant changes to their security posture to align with digital initiatives.
- **AI/ML and cloud-native technologies:** are the most pressing cybersecurity challenges, yet less than half have fully mature frameworks to address them.
- **Regulatory complexity:** especially due to the Digital Personal Data Protection Act (DPDP), is a major concern—72% identify consent management as the top challenge.
- **Zero Trust is the future:** with three-fourths of organizations either implementing or transitioning to this architecture model.
- **Security talent shortage is biting hard:** 42% cite increased workload due to unfilled roles; 62% face difficulty in finding qualified candidates.
- **Security is no longer siloed:** Over 80% report strong integration with business functions and frequent cross-functional governance.

The survey reflects a cyber security environment that is maturing, integrated, and business-aware, but facing operational strain from complexity, compliance, and talent shortages.

Targeted Controls Exceed Complete Overhauls in Digital Era

Digital transformation is a major driver of change, prompting most organizations to adapt or redesign their cybersecurity posture.
While only 14% of organizations reported undertaking a complete security redesign, a combined 71% implemented significant adjustments or targeted controls. This trend indicates that most companies are not doing a full reboot of their cybersecurity strategy but are instead layering controls to secure specific digital initiatives. The low percentage of respondents reporting "minimal impact" suggests that static security strategies are rare in today's environment.
Implication: CISOs must expect that digital transformation will require ongoing, targeted security enhancements. Most organizations are not overhauling their entire security architecture, but are making significant or targeted changes. This means CISOs should prioritize flexibility and modularity in their security programs, ensuring new digital initiatives are protected without disrupting existing operations. This requires a flexible architectural foundation and governance processes that allow iterative improvements.
Bottom-Line: Build flexible architectures that accommodate change, without destabilizing core operations.

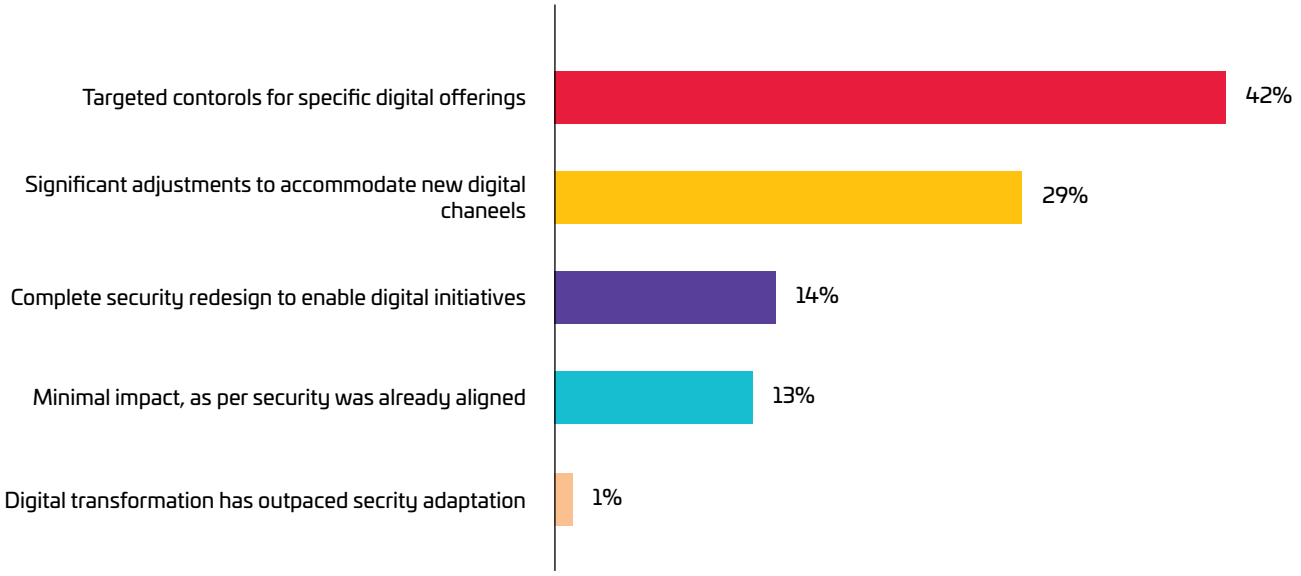
Agile Strategy Beats Static Security Playbooks

Organizations are institutionalizing agility, with nearly 80% reviewing or adjusting strategy regularly. Nearly half of the organizations conduct regular, scheduled cybersecurity strategy reviews, while another third make adjustments based on defined triggers. This reflects a shift from static, compliance-driven security to dynamic, risk-based management.
Implication: A proactive, regularly reviewed strategy is now the norm. CISOs should institutionalize frequent reviews and establish triggers for change (such as new threats, business initiatives, or regulatory shifts). Static or reactive approaches are no longer sufficient; agility is a competitive advantage in cybersecurity
Bottom-Line: Institutionalize strategy reviews with KPIs and scenario triggers to remain responsive.

Security Joins the Innovation Lifecycle

Risk assessment and security-by-design are being embedded into the technology development lifecycle in most enterprises, with 77% conducting risk assessments before major deployments. This strategy prevents reactive security postures, which can delay rollouts or introduce vulnerabilities. However, a notable minority still rely on post-implementation fixes or business-driven decisions, which could expose organizations to risk.

Targeted Controls Exceed Complete Overhauls in Digital Era



Most organizations prefer adapting targeted controls over implementing full-scale security overhauls to meet digital demands.

Implication: Most organizations are embedding security early in technology adoption. CISOs should champion risk assessments and security-by-design, ensuring security is not an afterthought. Where business-driven decisions dominate, security leaders should advocate for early-stage involvement in business and IT planning sessions to ensure cybersecurity considerations are part of the core design, and not an afterthought.

Bottom-Line: Embed security into procurement and design stages—don't wait for post-deployment remediation.

Multi-Metric Risk Quantification is Widespread

Organizations are adopting a diverse range of risk assessment methods, with many combining financial impact, threat modeling, qualitative analysis, and compliance assessments. This multidimensional view helps CISOs communicate risk in business terms, and supports better decision-making and alignment with business objectives.
Implication: CISOs must be able to communicate risk in both technical and business terms. Using multiple quantification methods enables more persuasive risk communication to management and supports better prioritization. Not quantifying risk is a major gap that must be closed. Security teams must invest in tools and frameworks that allow risk data to be quantified and visualized, supporting decision-making across executive and operational levels.
Bottom-Line: Develop a risk language that aligns with finance, legal, and business risk frameworks.

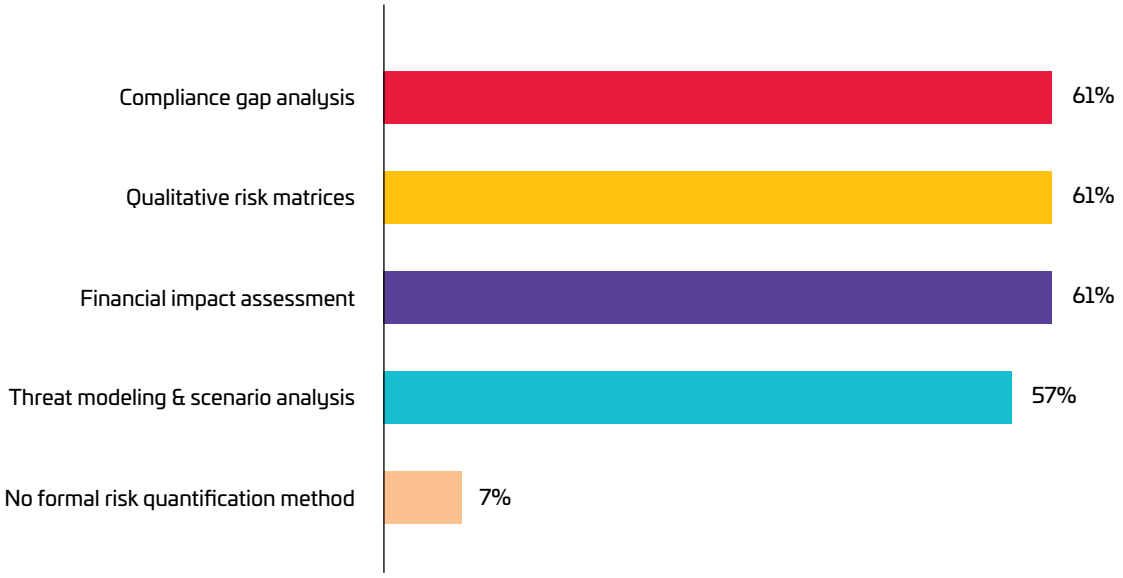
Cybersecurity Is No Longer an Island

Only 3% of organizations view cybersecurity as an isolated function, with the majority indicating that it is either well-coordinated or fully integrated with other business functions. This evolution reinforces the idea that cybersecurity is a business enabler, with organizations embedding security into business processes and ensuring alignment with organizational goals..
Implication: Integration is key. CISOs should build strong cross-functional relationships, embedding security in business processes and decision-making. This reduces friction and ensures security is seen as a business enabler, not a blocker.
Bottom-Line: CISOs should act as business leaders, ensuring cybersecurity aligns with enterprise priorities.

New Technologies Pose the Greatest Security Challenges

Emerging technologies are fundamentally reshaping enterprise security risk. The fact that AI/ML and cloud-native applications rank highest reflects both the technical novelty and lack of mature controls in these areas. Mobile/remote work and IoT/OT also present significant risks, reflecting the expanding attack surface.
Implication: CISOs must prioritize

Multi-Metric Risk Quantification is Widespread



Organizations rely on diverse risk quantification methods, with very few lacking formal approaches.

security for AI/ML, cloud, and mobile/remote work. These areas should be the focus for investment, skills development, and control implementation. CISOs must build capability—both in tools and talent—to secure AI and cloud-native environments. This includes threat modeling, continuous monitoring, and automated governance.
Bottom-Line: Focus investments on securing AI and cloud workloads, and managing workforce-related risks.

monitoring. Use lessons from cloud governance as a starting point. CISOs must tailor communications to both technical and business audiences about AI risks, using quantifiable metrics and industry comparisons.
Bottom-Line: Develop centralized AI governance including ethics, fairness, model validation, and red-teaming.

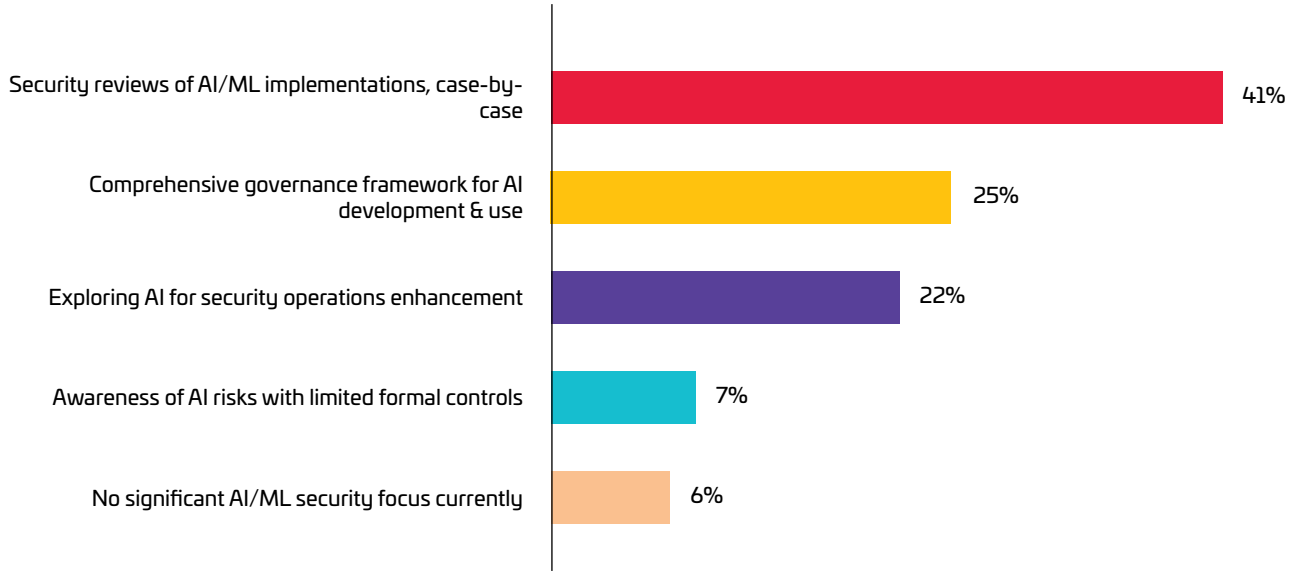
Boardrooms Demand Business-Centric Cyber Metrics

Boards expect actionable insights—not just technical detail. The majority of CISOs are responding by supplementing technical indicators with financial impact and regulatory status metrics. This supports informed decision-making at the executive level.
Implication: Security is becoming boardroom-relevant. Collecting relevant data and translate technical risks into business impact. Tailor board presentations to include business-aligned metrics and benchmarks. Establish a dashboard of leading indicators that

Legacy Systems, Cloud (In)Visibility Cause Operational Headaches

The dual burden of legacy environments and new cloud ecosystems poses visibility and control challenges. Legacy systems often lack patch support, while cloud environments demand continuous, API-driven monitoring. Alert fatigue and shadow IT highlight the need for automation and better visibility.
Implication: CISOs should focus on improving visibility and control in cloud environments, addressing legacy risks, and reducing alert fatigue through automation. Practitioners should prioritize remediation efforts and advocate for investment in modern security tools. Prioritize investments in visibility platforms and phase out unsupported legacy assets. Use hybrid cloud security tools that unify visibility across environments.
Bottom-Line: Build security programs that bridge legacy systems and cloud-native environments.

AI Security Readiness Still in Early Stages



AI/ML security efforts are nascent, with most organizations yet to adopt holistic governance or operational approaches.

AI Security Readiness Still in Early Stages

While most organizations are aware of AI/ML risks, only a quarter of organizations have formal governance frameworks for it. Many are still in the early stages of formalizing controls, and are managing AI risks reactively—which can lead to inconsistent or insufficient controls. While there is awareness, execution maturity is still low.
Implication: CISOs should build a structured AI risk framework, incorporating model validation, bias mitigation, access control, and

Cloud-Native Security Tools Take the Lead

Nearly half of respondents have adopted integrated cloud-native controls, indicating a shift toward cloud-first security postures. But many are still transitioning or relying on legacy approaches, which may not address cloud-specific risks. Traditional on-prem tools are being phased out for more agile, scalable alternatives.

Implication: Cloud-native security is becoming standard. CISOs should invest in cloud-native controls and integrated monitoring, rather than relying solely on providers or legacy tools. CISOs must evaluate and deploy cloud-native security tools, such as CSPM, CIEM, and container security solutions, to address modern infrastructure demands.

Bottom-Line: Invest in CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platform), and cloud-trained teams to maintain visibility and control.

Threat Intelligence Moves from Passive to Proactive

Enterprises are integrating threat intelligence into their operational workflows. With threat intelligence is becoming a core component of security operations, automation playing a growing role in timely response. This means security teams are not only collecting threat data but acting on it through automation and contextual analysis.

Implication: Automated, actionable threat intelligence is a differentiator. CISOs should push for integration of threat intelligence into security operations, enabling faster, more informed responses. Build threat intel programs that integrate with SIEM and SOAR platforms. Make threat feeds actionable by mapping them to MITRE ATT&CK or internal incident taxonomies.

Bottom-Line: Practitioners should ensure threat intelligence is operationalized, not just collected.

Mature Incident Response Is Now the Norm

Most organizations now have well-defined incident response (IR) procedures, with nearly half simulating breach scenarios. This marks a significant maturity step in security operations, which is critical for resilience in a dynamic threat environment.

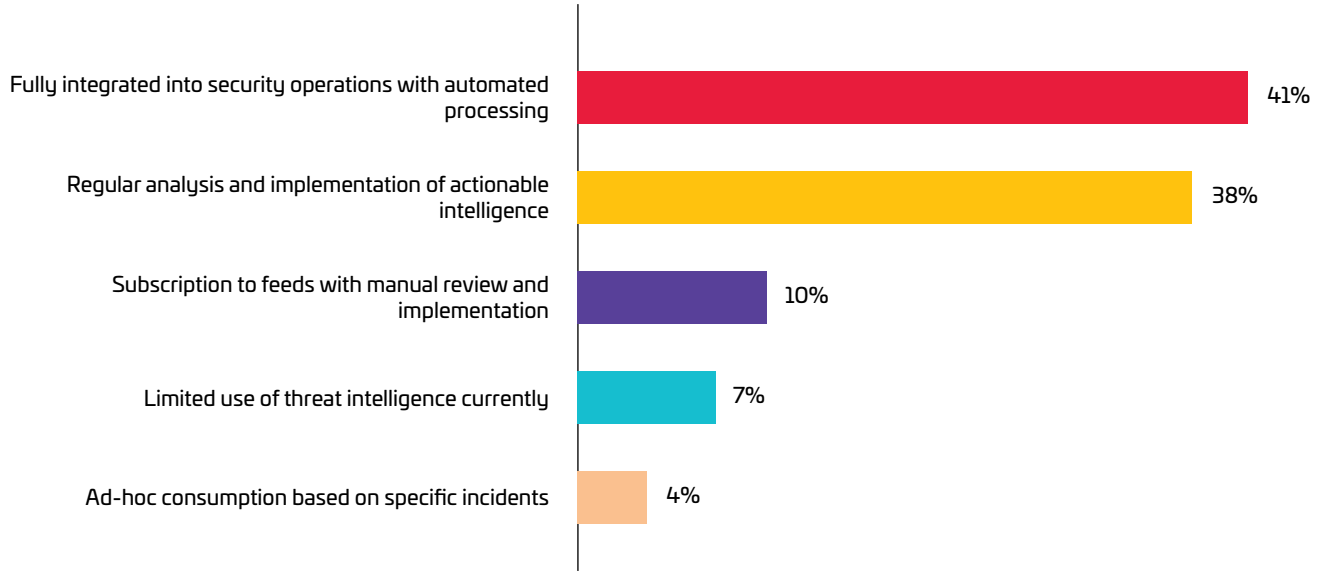
Implication: Regular simulation and mature incident response are essential for resilience. CISOs should ensure incident response plans are tested and updated regularly. Practitioners should participate in exercises and maintain readiness for real-world incidents. Ensure lessons learned from simulations are integrated back into IR plans.

Bottom-Line: Run frequent tabletop and red-team exercises—IR must be practiced, not theoretical.

Risk-Based Vulnerability Management Dominates

Regular, risk-based vulnerability

Threat Intelligence Moves from Passive to Proactive



Organizations are shifting toward proactive, automated threat intelligence to strengthen security operations.

management is now the norm, reducing exposure to known threats. The combination of regular scanning and risk-based prioritization enables teams to focus on vulnerabilities that matter most.
Implication: Regular, risk-based vulnerability management is best practice. CISOs should ensure comprehensive coverage and timely remediation—and move beyond CVSS scores to include exploitability, business impact, and threat actor relevance in the vulnerability triage. Practitioners should.
Bottom-Line: While patch hygiene still matters, prioritize vulnerabilities based on risk, not just compliance.

Automation Targets Volume, Not Yet End-to-End Security

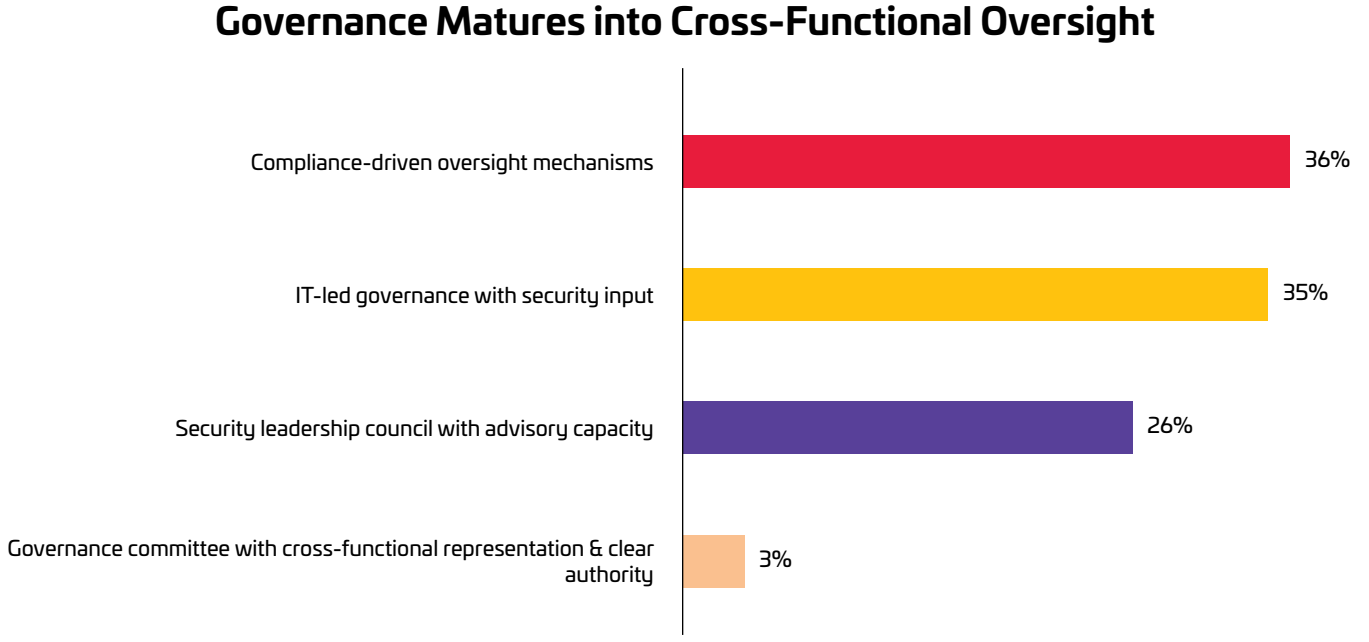
Most organizations are automating high-volume, repetitive tasks like alert handling or basic threat response. Full end-to-end automation, however, is still nascent. Only a fifth of respondents have extensive automation across all security functions.
Implication: Automation is key to scale and efficiency. CISOs should invest in automation for repetitive tasks and incident response. Prioritize automation initiatives that yield immediate ROI. Use early wins to justify broader investment in SOAR and AI-based defense systems.
Bottom-Line: Start with automating repetitive tasks—alerts, phishing triage—and scale to orchestration across operations.

Zero Trust Emerges as the Dominant Security Paradigm

Zero Trust is emerging as the dominant architecture, reflecting the need for adaptive, identity-based security in cloud and remote environments. The majority of respondents are either transitioning or have implemented Zero Trust models. This approach emphasizes identity verification, micro-segmentation, and least privilege access.
Implication: Zero Trust is the future. CISOs should lead the transition, focusing on identity, segmentation, and continuous verification. Map out a Zero Trust roadmap aligned with business priorities, and implement across the organization.
Bottom-Line: Use identity as the core control plane, and continuously monitor access behavior.

Governance Matures into Cross-Functional Oversight

Security governance is no longer confined to IT. The rise of security councils and governance committees ensures that cybersecurity is aligned with business outcomes and risk appetite.
Implication: Strong, cross-functional governance is critical for alignment and accountability. CISOs should participate in, or lead, governance bodies. Practitioners should ensure their activities are aligned with organizational policies and priorities, and have the representation of IT security in enterprise risk committees, compliance reviews, and digital steering groups.



Effective governance increasingly involves cross-functional collaboration and shared authority beyond compliance.

Bottom-Line: Strong governance enables effective risk management and regulatory compliance

Vendor Risk Is a Board-Level Concern

With supply chain attacks on the rise, organizations are formalizing third-party risk processes. Many now assess vendors during onboarding and continuously throughout the relationship, with formal programs that reflect the complexity of modern supply chains.

Implication: Third-party risk is a major exposure. CISOs must establish comprehensive vendor risk management programs, including assessment, monitoring, and contractual controls. Practitioners should support due diligence and ongoing oversight. Use third-party risk platforms to automate assessments, and track SLA violations or exposure trends. Embed cybersecurity clauses into contracts. Vendor risk management is critical for regulatory compliance and business integration.
Bottom-Line: Use continuous monitoring tools and build risk-based supplier tiers for effective governance.

DPDP Tops the Compliance Challenge List

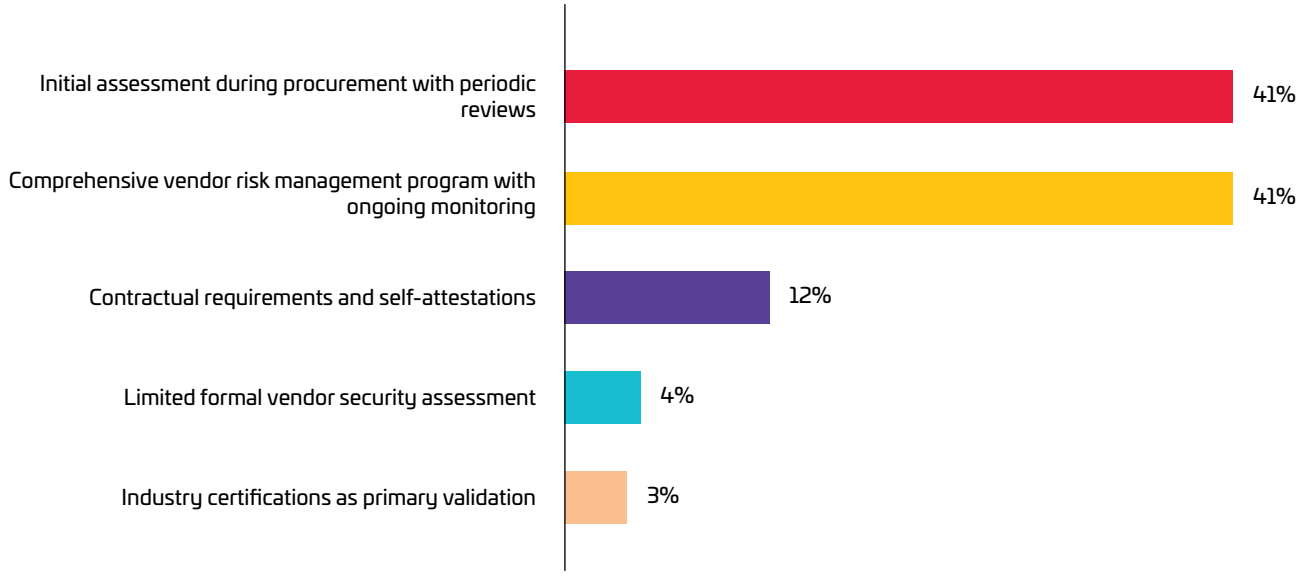
The Digital Personal Data Protection Act is creating operational strain for many organizations. Its focus on consent, breach notification, and data localization is forcing structural changes. Compliance with global standards also posing significant hurdles for many security practitioners.
Implication: Regulatory complexity is increasing. CISOs must ensure compliance with both local and global frameworks, often requiring new processes and technologies. CISOs must work with legal and data owners to create enterprise-wide privacy programs. Practitioners should stay current on requirements, and support compliance initiatives.
Bottom-Line: Build centralized compliance dashboards and automate reporting workflows.

Consent Management Is the Toughest DPDP Requirement

Operationalizing consent and data rights is the biggest hurdle, reflecting the technical and process complexity of modern privacy laws. Implementing mechanisms to capture, store, audit, and revoke consent at scale is proving the most difficult aspect of DPDP compliance. These challenges reinforce the need for automation, mature governance, and integration with business.

Implication: Privacy requirements are operationally complex. CISOs must prioritize consent management and data subject rights in their privacy programs. Practitioners should work on implementing technical solutions for data localization and erasure. Invest in Consent Management Platforms (CMPs) and ensure audit trails are maintained. Build interfaces for individuals to manage their data rights.
Bottom-Line: Design user-rights management portals and build data traceability.

Vendor Risk Is a Board-Level Concern



Continuous assessment and monitoring are now essential practices for managing vendor risks at the board level.

Skill Gap is Stretching Security Teams Thin

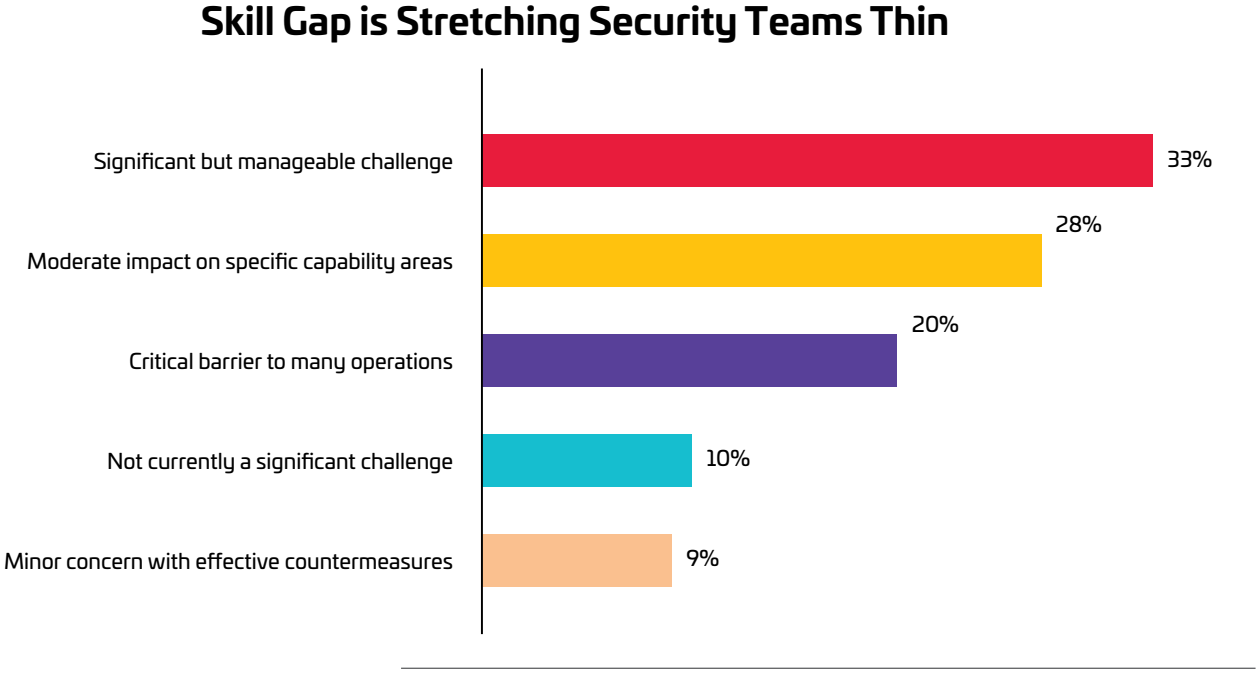
The majority of organizations are experiencing operational strain due to the cybersecurity skill gap. Workforce shortages are leading to overburdened teams, delayed initiatives, and increased reliance on external consultants. This affects morale and incident response readiness.
Implication: CISOs must invest in training, upskilling, and retention. Conduct workforce capacity assessments and implement staff augmentation strategies. Make burnout prevention part of your cybersecurity resilience plan. Practitioners should aim for continuous learning and certifications.
Bottom-Line: Invest in hiring, upskilling, certifications. Managed services should not be a crutch

Hiring and Retention Are Equally Broken

The cybersecurity job market is squeezed from both ends: organizations can't find qualified talent, and those they do hire often leave due to burnout or better offers. Talent acquisition and retention are the top challenges, compounded by evolving skill needs and rising salary demands.
Implication: Hiring, retention, and upskilling are ongoing issues. CISOs need to develop robust talent pipelines, offer competitive compensation, and foster a culture of learning. They should foster a culture of growth and provide clear career paths. Practitioners should take ownership of their professional development, and focus on adaptability and continuous professional growth to stay relevant.
Bottom-Line: Build compelling employee value propositions, invest in mentorship, and align compensation with market dynamics.

Security Awareness Is Common, But Engagement Isn't

Training is still largely compliance-driven with most organizations investing in regular training. Few organizations have embraced advanced, engaging methods like gamified or adaptive learning models. This diminishes long-term behavior change.
Implication: A strong security culture reduces risk from human error. CISOs should integrate behavioral science into awareness programs, and move beyond compliance to create engaging, continuous awareness programs that foster a security-first mindset. This includes the use of phishing simulations and gamified modules to build a security-first mindset. Practitioners can champion creative approaches, and act as role models for secure behaviors.
Bottom-Line: Move from checkbox compliance to gamified, behavior-focused awareness.



Skill shortages remain a significant and ongoing challenge, increasing strain on cybersecurity teams

Conclusion

Indian enterprises are evolving toward automated, integrated, and business-driven cybersecurity. Despite advances in Zero Trust, cloud security, and governance, challenges like compliance, operational visibility, and talent persist. Leadership, skills, and culture now define effectiveness, making CISO roles critical for driving enterprise security outcomes.■

Trust as the New Currency: Reimagining Cybersecurity for the AI Era

Anand Jethalia, Country Head of Cybersecurity at Microsoft India & South Asia, believes digital trust now depends on viewing security not as a cost, but as a catalyst for resilience, confidence, and innovation.

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

IN AN era where artificial intelligence and cloud innovation are redefining business models, cybersecurity has moved from the backroom to the boardroom. For Anand Jethalia, Country Head of Cybersecurity at Microsoft India & South Asia, the future of digital trust lies in seeing security not as a defensive cost but as a strategic driver of resilience, confidence, and Innovation.

At the heart of this transformation is Microsoft's Secure Future Initiative (SFI) — a blueprint for embedding secure-by-design principles, AI-first defense, and end-to-end Zero Trust into every layer of enterprise technology. Under Jethalia's leadership, this approach is helping organizations simplify their fragmented security ecosystems, accelerate the adoption of responsible AI, and turn compliance into a catalyst for growth.

In this exclusive conversation with CISO Forum, Jethalia unpacks how Indian enterprises are navigating the convergence of AI, identity, and trust, how Microsoft is reshaping cyber resilience across industries, and why he believes security is the true enabler of Innovation in the digital economy.

CISO Forum: What key strategic objectives are your clients focusing on today, and how do you ensure Microsoft's cybersecurity solutions not only meet technical requirements but also support these broader business goals?

ANAND JETHALIA: Microsoft's strategy is to position cybersecurity not as a cost center that merely meets technical requirements, but as a strategic business enabler that fosters the trust necessary for clients to adopt transformative technologies like AI and the cloud confidently.

At Microsoft, our cybersecurity strategy is anchored in the Secure Future Initiative (SFI), which embeds secure-by-design engineering, AI-first defense, and default protections across our platforms—ensuring that security is not just a technical requirement but a strategic enabler of trust.

In client conversations, three imperatives consistently emerge: the need to securely navigate the AI and agentic era, simplify and unify the Security Operations Center (SOC), and implement true end-to-end, identity-centric Zero Trust.

Clients are deploying generative AI tools like Microsoft 365 Copilot to reimagine productivity, but they want assurance that Innovation doesn't compromise security. Microsoft's approach ensures AI agents are governed, private, and secure by design—turning Copilot into a trusted copilot for transformation.

At the same time, SOC teams are under pressure to accomplish more with fewer resources. Our integrated platform—Sentinel, Defender XDR, and Security Copilot—helps reduce tool sprawl, operational overhead, and response time. Our unified data lake ingests signals from over 350 connectors, providing clients with comprehensive visibility without the burden of stitching siloed data.

As hybrid work and multi-cloud environments become permanent, organizations are moving beyond perimeter-based security to verify every user, device, and application explicitly. Microsoft Entra enables this shift, simplifying Zero Trust adoption across all platforms.

From unified security operations and agentic defense to proactive risk reduction and secure identity access, our solutions are designed to meet these strategic objectives head-on—helping clients build resilience, reduce complexity, and unlock Innovation with confidence.

CISO Forum: With rapid digital transformation, what are the most pressing cyber risks you see organizations facing today?

ANAND JETHALIA: As digital transformation accelerates, CISOs are navigating a threat landscape that is more fragmented, sophisticated, and fast-moving than ever.

Identity has become the new perimeter, with attackers exploiting credentials and tokens to move laterally across environments. Software supply chains are increasingly vulnerable, as trust in third-party code and APIs becomes critical. State-level adversaries and ransomware groups are becoming increasingly stealthy, while tool sprawl continues to fragment visibility and response capabilities. Exposure management is now essential, requiring defenders to map and reduce their attack surface proactively. As AI adoption increases, threats such as prompt injection, model poisoning, and data leakage are no longer theoretical. These risks demand a security architecture that's engineered for resilience, governed by design, and ready to adapt at machine speed.

Microsoft's Secure Future Initiative addresses these challenges head-on by embedding identity and secrets protection into our engineering lifecycle, positioning Sentinel as a unified security data lake to reduce fragmentation, and treating AI as both a battleground and a defense accelerator. Our approach is designed not just for technical soundness, but for business resilience, regulatory trust, and continuous adaptation.

CISO Forum: How do you balance Innovation in cloud and AI technologies with security and compliance requirements?

ANAND JETHALIA: At Microsoft, we believe Innovation without trust is just risk. We consider that Innovation and security are not opposing forces—they are co-drivers of confidence and resilience. Our Secure Future Initiative (SFI) embeds security into every layer of our engineering and operational lifecycle, ensuring

that every AI or cloud capability we launch is secure by design, compliant by default, and governed through responsible Innovation.

A leading private-sector bank, for instance, utilized Sentinel's unified log analytics and Defender's endpoint telemetry to meet the 24-hour incident-reporting guideline, demonstrating how secure-by-design Innovation accelerates compliance.

We believe AI innovation must advance hand-in-hand with responsible governance, and that's exactly what we enable through our Responsible AI Standard. When combined with Microsoft Purview and Entra, it ensures consistent data classification, retention, and access controls across all platforms.

Our integrated security platform—Defender XDR, Sentinel SIEM, Purview, Entra ID, and Security Copilot—helps CISOs consolidate fragmented tools, reduce detection times, and meet compliance across sectors. With Security Copilot, Indian SOC teams are transforming Level 1 triage into automated, AI-assisted investigations—freeing analysts to focus on proactive threat hunting.

In today's India, where digital acceleration is redefining every industry, we see security as the steering wheel of Innovation—not the brake.

CISO Forum: What role does a Country Manager play in fostering a culture of cybersecurity across enterprise clients?

ANAND JETHALIA: At Microsoft, we view cybersecurity not just as a technological imperative, but as a national priority that underpins trust, fuels Innovation, and safeguards digital progress. My role is to help translate this vision into action by shaping the enterprise mindset around cyber resilience and responsible AI.

I work closely with CXOs to elevate cybersecurity from a cost center to a boardroom capability, anchoring conversations in operational continuity, reputation, and regulatory assurance. We co-create sector-specific resilience playbooks that map Microsoft solutions—Defender, Sentinel, Entra, and Purview—to industry mandates, helping CISOs operationalize compliance while improving detection and response maturity.

As India accelerates cloud and AI adoption, we support clients in embedding Zero Trust and Responsible AI principles into transformation programs. Building a security-first culture also means investing in people, and we actively amplify initiatives like CyberShikshaa and Future Ready Skills in partnership with MeitY and NASSCOM.

We also work closely with industry and government bodies—strengthening collaboration through shared threat intelligence, digital forensics, and policy guidance on AI safety. I see my role as contributing to making cybersecurity a shared national mission—helping every enterprise in India innovate fearlessly, protect data responsibly, and build digital trust that fuels economic growth.

CISO Forum: How do you measure the impact of cybersecurity initiatives on business outcomes?

ANAND JETHALIA: At Microsoft, we fundamentally view cybersecurity not as an IT cost, but as a driver of business value and trust. Measuring impact means shifting the conversation from technical metrics to outcomes that matter to the board—risk reduction, operational resilience, and innovation enablement.

Our approach focuses on how well security is built in and enforced, using indicators like ransomware protection scores, exposure reduction, and critical asset coverage to quantify risk mitigation. Metrics such as the percentage of accounts with enforced Multi-Factor Authentication (MFA) directly reflect progress against identity-based threats, while operational measures like time-to-contain and analyst productivity gains—especially with Security Copilot—demonstrate how AI is transforming response speed and efficiency.

As organizations advance their Zero Trust maturity, these metrics help CISOs show how security investments are enabling secure collaboration, regulatory assurance, and long-term resilience. Ultimately, the most meaningful measure is trust—because when security empowers confident adoption of new technologies, it becomes a catalyst for growth.

CISO Forum: Can you share an example of a strategic cybersecurity solution that significantly improved client resilience?

ANAND JETHALIA: At Microsoft, we define resilience not just by how organizations respond to threats, but by how confidently they adapt and scale in the face of change. One example is our global rollout of Security Copilot Guided Response within Defender XDR, which uses large-scale AI to assist SOC analysts in investigation, triage, and remediation—reducing alert fatigue, improving consistency, and enabling lean teams to scale defense.

Closer to home, LTIMindtree, an Indian IT services company, adopted Microsoft's integrated security suite to secure a rapidly expanding hybrid workforce. With these integrations, LTIMindtree has established a unified command center for investigations, threat intelligence, and incident response. The solution has enabled the organization to build a next- generation Security Operations Center with enhanced agility and operational efficiency.

These examples demonstrate how Microsoft's cybersecurity solutions are enabling organizations to transition from reactive defense to proactive resilience, with AI, identity, and data protection working in concert to secure what matters most. ■

From Alert Chaos to Strategic Defense: Redefining SOC Operations for the AI Era

ManageEngine's Manikandan Thangaraj outlines how AI-driven, unified SOC platforms are transforming alert fatigue into precision-focused cybersecurity intelligence.

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

IN AN era where security operations centers are inundated with over 80% false-positive alerts, operational burnout has become a silent threat undermining enterprise cybersecurity. Manikandan Thangaraj, Vice President at ManageEngine, is leading a paradigm shift—moving beyond volume-based detection to precision-engineered security intelligence. With Log360's enhanced platform, featuring over 1,500 cloud-updated detection rules mapped to MITRE ATT&CK and SIGMA, ManageEngine is answering a critical question: how do we empower analysts to work smarter, not harder? In this exclusive interview, Thangaraj reveals how unified SOC platforms, identity-centric monitoring, and AI-driven augmentation are transforming security from a cost center into a strategic business enabler for modern enterprises.

CISO Forum: SOC teams face constant operational burnout. What do you see as the main drivers of alert fatigue in enterprises today?
MANIKANDAN THANGARAJ: Alert fatigue in Security Operation Centers (SOC) is driven primarily by three intertwined factors, creating a crisis of operational burnout.

First, false positives flood the system, forcing analysts to waste critical time investigating benign activity. When over 80% of alerts are false positives, analysts are incentivized to ignore the queue, thereby burying genuine threats. Second, tool sprawl creates a complex environment where multiple, unintegrated security solutions generate redundant or conflicting notifications. This forces manual correlation, slowing response, and amplifying cognitive load. Third, the persistent lack of context in alerts prevents rapid triage. A generic "suspicious activity" alert demands hours of manual investigation to determine asset criticality and actual risk. The cumulative effect is a team perpetually fighting fires, leading to high turnover and a dangerous decline in security efficacy. We must shift focus from simply generating more alerts to generating high-fidelity, context-rich signals.

"The future SOC will combine curated, human-driven detection engineering with AI-driven investigation and response—faster, sharper, and more resilient."

CISO Forum: ManageEngine has enhanced Log360 to reduce false positives. How does the platform streamline analyst workflows and improve SOC efficiency?
MANIKANDAN THANGARAJ: We approached this challenge by re-engineering detection around precision and adaptability. Instead of broad, one-size-fits-all rules, Log360 enables object-level filtering across users, groups, and organizational units, letting analysts scope detections to what truly matters.

The most significant drain on SOC teams is time lost chasing false positives. Log360 helps streamline this by combining detection logic, rule management, and tuning insights into a single console. Analysts can fine-tune detections with granular controls, applying rules only to high-value assets such as executive accounts, sensitive data stores, or critical servers, while suppressing benign alerts from less critical endpoints.

This is supported by a catalog of over 1,500 curated, cloud-updated detections, mapped to MITRE ATT&CK and SIGMA, and continuously updated from the cloud. Along with interactive visibility into rule performance metrics such as hit frequency and alert volume, analysts can constantly refine their detections. The result is a more focused, high-fidelity workflow that improves triage speed and strengthens response.

CISO Forum: With 1,500+ detection rules mapped to MITRE ATT&CK® and SIGMA, how are detection technologies reshaping enterprise threat detection and response?
MANIKANDAN THANGARAJ: Detection engineering has shifted from focusing on the number of rules to the quality of regulations. Frameworks such as MITRE ATT&CK and SIGMA provide a global language for mapping adversary techniques; however, enterprises require actionable, production-ready detections rather than just frameworks.

This threat modeling approach offers two key advantages:

- It enables enterprises to identify and respond to threats more quickly by providing contextual information.
- SIGMA and MITRE standardize the sharing of threat information in a consistent format. Being community-driven, these frameworks are continually updated and refined to meet the evolving needs of the community.

Out-of-the-box rules help reduce mean time to detect (MTTD), while the added context helps lower mean time to respond (MTTR). Each detection rule is researched, curated, and validated by ManageEngine's in-house threat research team, and then tested against real-world attack simulations to ensure high precision and minimal false positives.

CISO Forum: What broader trends in enterprise security modernization are driving the demand for unified, scalable, and intelligent SOC platforms worldwide?

MANIKANDAN THANGARAJ: Identity has become the new perimeter, with most modern breaches involving compromised credentials or the misuse of privilege. The challenge for SOC teams is that identity signals are scattered across Active Directory, cloud identity providers, VPNs, and SaaS platforms. A unified SOC platform consolidates these signals into a single location and correlates them with endpoint and network events. This means analysts can immediately connect an anomalous login to privilege escalation, lateral movement, or data exfiltration without having to juggle multiple tools or miss context.

Scale and distribution are also redefining enterprise security. Organizations today operate workloads across on-premises infrastructure, multiple cloud environments, and remote endpoints, which demands horizontally scalable platforms that can maintain resilience while keeping detection-to-response cycles tight. This kind of unification not only ensures visibility across identity, data, and infrastructure risks but also enables faster and more confident decision-making.

Operational efficiency has become another decisive factor. Security teams must achieve more with fewer people. By consolidating Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), and threat intelligence into a single console, enterprises can reduce tool sprawl, minimize context switching, and accelerate detection-to-response cycles. This unification isn't just cost-effective; it's what makes identity, data, and infrastructure risks visible together, enabling faster and more confident decisions.

CISO Forum: Balancing compliance, productivity, and risk is a challenging task. What practical strategies should CISOs adopt to strengthen security while enabling business growth?

MANIKANDAN THANGARAJ: The key is to shift from compliance-first to risk-first. Compliance frameworks provide guardrails, but absolute protection comes from contextual visibility. CISOs should invest in unified monitoring that ties compliance requirements directly to detections; for example, using rule libraries that cover Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), or Network and Information Systems Directive (NIS2), while still surfacing anomalies and insider threats. Automating routine reporting frees up teams to focus on active risks. Equally important is collaboration. Embedding security into DevOps, IT, and business workflows ensures security is not a blocker but an enabler of growth.

CISO Forum: Looking ahead, how do you see the future of SOC operations evolving in the era of AI-driven cybersecurity advancements?

MANIKANDAN THANGARAJ: AI is poised to transform SOC operations in two key ways. It will act as a force multiplier for analysts, with AI-driven assistants summarizing incidents, suggesting playbooks, and auto-triaging routine alerts, allowing human expertise to be focused on complex investigations. At the same time, it will raise detection fidelity by leveraging machine learning models trained on identity behaviors, cloud activity, and threat intelligence to flag subtle anomalies that traditional rules often miss. That said, AI is not a replacement but an augmentation. The future SOC will combine curated, human-driven detection engineering with AI-driven investigation and response. The result will be operations that are faster, sharper, and more resilient against evolving adversaries. ■

Cybersecurity Talent Development

Global cybersecurity faces a talent shortage of 4 million people, requiring diverse recruitment, internal training, realistic hiring, and retention strategies to combat evolving threats.

By **Sandeep Walia** | CISO, Associate Director, Security Consulting PCI Program Office, Kyndryl

THERE IS a global skills shortage of nearly 4 million cybersecurity experts. This shortfall exposes organizations to severe cyber threats. An Organisation requires a multifaceted approach to address this skills shortage. This includes attracting diverse talent, removing entry barriers, developing security coordinators within organizations to work alongside core information security teams, implementing internal training programs, and strategies to retain skilled professionals. These measures will help organizations in building a robust cybersecurity workforce capable of defending against an ever-evolving threat landscape.

The Global Cybersecurity Talent Shortage

According to the World Economic Forum's Strategic Cybersecurity Talent Framework, the global cybersecurity workforce faces a shortfall of 4 million professionals. India had 40,000 cybersecurity job vacancies in May 2023, yet 30% remained unfilled due to a lack of qualified talent. This happens when we produce nearly one-third of the world's STEM graduates.

This highlights the urgent need to develop strategies that attract, train, and retain cybersecurity professionals to meet growing demand.

Escalating Cyber Threats

The need for cybersecurity professionals is rapidly growing. There is an increase in the frequency and sophistication of cyberattacks. This impacts businesses and organizations worldwide. Artificial Intelligence enables hackers to automate attacks, making

them more efficient and difficult to detect.

Industries such as fintech, logistics, utilities, and professional services are particularly vulnerable. Their systems are complex, and their data has a sensitive nature. Finding cybersecurity experts familiar with industrial systems is even more challenging.

Challenges in finding skilled Cybersecurity Talent

Several factors contribute to the difficulty in finding skilled individuals for cybersecurity roles:

1. Conduct a cyber risk assess ment

- **Evolving Cyber Threats:** The cybersecurity threat landscape is constantly changing. This requires professionals to engage in continuous learning, making it challenging to keep pace with new developments.
- **Diverse Regulatory Requirements:** From PCI to HIPAA, GDPR to the Digital Personal Data Protection Act, Industries and geographies have different cybersecurity regulations, necessitating specialized expertise that is difficult to find in a single candidate.
- **Unrealistic Job Descriptions:** Employers frequently post exaggerated job requirements. For example, an "entry-level" cybersecurity analyst position may demand five years of experience, proficiency in multiple programming languages, and 24/7 on-call availability, discouraging prospective candidates from applying.
- **High-Stress and Demanding Hours:** Cybersecurity professionals often face high job pressure and demanding work hours, which can be a deterrent for some
- **Lack of Diversity:** The cybersecurity field suffers from a lack of diversity, which limits innovation and effective problem-solving.

Sandeep Walia
Associate Director, Security Consulting
PCI Program Office, Kyndryl

Gender bias, particularly in network security roles, further shrinks the talent pool.

Strategies for Bridging the Cybersecurity Talent Gap

To address these challenges, organizations can implement these strategies:

1. Encouraging Cross-Disciplinary Transitions

Organizations should encourage professionals from various fields, including networking, software development, desktop support, and audit teams, to transition into cybersecurity roles. These individuals already possess valuable knowledge and, with proper training, can become effective security professionals. This approach also boosts employee retention and career development.

2. Management's Role in Cybersecurity Talent Development

Senior leadership must foster an environment where cybersecurity is a shared responsibility, rather than restricting it to the information security team. This involves aligning security initiatives with business goals and providing clear career progression opportunities.

3. Removing unrealistic requirements

Revising job descriptions to focus on core skills rather than unrealistic requirements can make roles more accessible and appealing. Emphasizing practical experience and competencies over certifications will help broaden the talent pool.

4. Outsourcing Security Roles

Given the global cybersecurity talent shortage, outsourcing is a viable solution. Organizations can outsource functions such as vulnerability assessments, penetration testing, awareness training, security audits, and compliance testing, depending on their specific risk profile.

5. Encouraging Cybersecurity Careers Within the Organization

Organizations must actively promote cybersecurity as a viable career path for employees by:

- Raising internal awareness about cybersecurity opportunities.
- Mentorship programs to guide aspiring professionals.
- Job rotations to help employees discover cybersecurity roles.
- Encouraging a culture of continuous learning and innovation to attract talent from both technical and non-technical backgrounds.

6. Training and Upskilling Employees

Map the core competencies and skills you currently have in your cybersecurity team. Identify the skills you will need in the future. When you compare the list of current skills against the list of critical future skills, you will be able to ascertain the "skills gap" that will help you plan your upskilling programme. Bridging this gap requires investments in training and education.

Some of the strategies could be:

- Provide certification opportunities.
- Collaborate with educational institutions and online learning platforms.
- Utilize adaptive learning platforms that tailor training to individual progress and learning styles.

7. Retaining Talents

CISOs must focus on retaining their own employees. This includes a focus on creating a supportive work environment and clear career growth pathways:

- **Career Development:** Offering personalized career plans enhances job satisfaction and loyalty.
- **Avoiding Unrealistic Expectations:** Employers should recognize that demands like 24/7 availability and "zero incidents" are impractical. If round-the-clock coverage is required, additional staff should be hired to prevent burnout.

"Addressing the global cybersecurity talent gap isn't just about hiring—it's about cultivating, empowering, and retaining future defenders."

- **Work-Life Balance Initiatives:** Given the high-stress nature of cybersecurity roles, organizations should implement flexible policies to enhance work-life balance, job satisfaction, and long-term retention. Increased flexibility in work hours and location helps increase employee satisfaction, which in turn leads to retention, and also enhances an employer's competitiveness and attractiveness in attracting top talent.
- **Responsive Management:** Listening to employees' concerns and acting on feedback fosters a positive workplace culture.

Conclusion

The cybersecurity talent shortage is a complex challenge, This requires a proactive and strategic approach. By enhancing diversity, providing specialized and adaptive training, refining hiring practices, and implementing effective retention strategies, organizations can develop a strong cybersecurity workforce. Rather than relying solely on external hiring, companies should cultivate cybersecurity talent internally, ensuring long-term security resilience and business continuity. Outsourcing part of information security jobs could also be a practical option.

A comprehensive approach that integrates talent attraction, education, recruitment, and retention will enable organizations to build a capable and dedicated cybersecurity workforce—one that is prepared to mitigate evolving threats and protect critical digital assets. ■

Exposure Management: The Future of Cyber Risk Reporting

Exposure management transforms cyber reporting by linking vulnerabilities to business risk, enabling strategic board discussions over technical metrics.

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

CORPORATE BOARDROOMS across the world share a common moment of dread: the quarterly cybersecurity briefing. Directors roll their eyes, muttering, "Oh God, it's the cyber update," while chief information security officers (CISOs) struggle to translate technical jargon into business terms that matter.

A new report from the Exposure Management Leadership Council—featuring CISOs from companies like GEICO, Dell, and Mastercard—explains why these presentations consistently fail and offers a path forward.

Why cyber reporting falls short

The communication gap began in the early 2010s, when CISOs first appeared in boardrooms without clear reporting standards. With little guidance, they relied on operational metrics: the number of vulnerabilities patched, systems updated, or phishing attempts blocked. These figures, though accurate, meant little to directors seeking answers to fundamental questions: Are we exposed? What does it mean for the business?

One CISO recalled presenting such metrics, only to be told by a director: "I get it, you're busy. I don't give a s***. I don't ever want to see those metrics again." A decade later, not much has changed. CISOs still spend hours compiling numbers from an average of 83 different security tools, often producing inconsistent or misleading results—a "garbage in, garbage out" problem.

Enter exposure management

Exposure management aims to close this gap. Instead of cataloging isolated vulnerabilities, it shows how weaknesses—misconfigurations, software flaws, excessive permissions—can combine into dangerous "attack paths" leading to critical assets.

This approach reframes the update. Rather than pages of spreadsheets, a CISO can now say: We've identified 25 exposures that create three potential attack paths threatening our operations. Here's our plan to close them.

Speaking the board's language

The innovation lies in translation. Exposure management reframes cybersecurity in terms of likelihood, business impact, and remediation priorities. Council members see it as the foundation for a standardized framework, akin to Generally Accepted Accounting Principles (GAAP), that would allow boards to benchmark progress, compare against peers, and track maturity over time.

"Exposure management reframes cybersecurity in terms of likelihood, business impact, and remediation priorities."

The AI wildcard

Artificial intelligence adds new urgency. Leaders flagged risks from employees using public AI tools, shadow AI projects, and vendors embedding AI without transparency. Policies, sandboxed alternatives, and stricter monitoring can help, but the pace of AI adoption is outstripping organizations' ability to control exposures.

The road ahead

With 71% of security leaders admitting that managing cyber risk isn't getting easier, exposure management offers a way forward. Done right, it could transform the dreaded quarterly cyber update into what it should have been all along: a strategic dialogue about protecting business value.. ■

Why do traditional DLP tools no longer work?

Traditional DLP tools lack visibility, delaying response and costing millions; companies now demand smarter, behavior-driven data protection.

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

A NEW study of 883 cybersecurity professionals reveals a troubling reality: the very tools designed to protect company data might be creating more problems than they solve. The findings come from the "Are Traditional DLP Solutions a Barrier to Preventing Data Loss? - Data Security Report 2025," published by Cybersecurity Insiders in partnership with Fortinet.

Data breaches are becoming the new normal

The numbers are stark. Nearly 8 out of 10 organizations (77%) suffered insider-related data breaches in the past 18 months, with more than half experiencing six or more incidents. What's particularly concerning is that most of these breaches aren't caused by malicious employees—49% resulted from simple carelessness or negligence, while only 16% involved confirmed malicious intent.

The financial impact is devastating

When data gets exposed, companies feel it in their wallets. Nearly half (45%) of organizations reported direct financial losses from their worst incident, with 41% estimating damages between $1 million and $10 million. Only 8% said the impact was negligible, meaning almost every breach carries meaningful consequences.

The most commonly stolen data includes customer records (53%) and personal information (47%), followed by sensitive business information like financial reports and strategic plans (40%). In industries where intellectual property matters most, a single leaked design or algorithm can damage competitive advantage for years.

Traditional security tools can't keep up

Here's the surprising finding: while 47% of companies say their Data Loss Prevention (DLP) tools are effective, most can't actually see what's happening with their data. A striking 72% admit they lack visibility into how employees use sensitive information across computers and cloud applications.

The problem gets worse with implementation. Only 24% found their DLP systems easy to deploy, and 75% had to wait weeks or months before gaining meaningful insights from their security investment.

What companies really need?

Security leaders are demanding better solutions. Two-thirds (66%) want real-time behavioral analytics that can spot unusual patterns, while 61% need immediate visibility from day one of deployment. Over half (52%) specifically want control over shadow AI tools and unauthorized software that employees might use.

"Organizations need smarter, more adaptive security that delivers insight—not just enforcement."

The path forward

The report suggests companies should shift from simply blocking data transfers to understanding user behavior and context. Modern data protection requires tools that can follow sensitive information wherever it goes—whether through email, cloud storage, messaging apps, or AI platforms—while distinguishing between normal work activities and genuine threats.

As data continues moving through increasingly complex digital environments, organizations need smarter, more adaptive security approaches that provide insight, not just enforcement. ■

India sees 3,237 cyberattacks weekly

India endures 3,237 cyberattacks weekly as ransomware and AI-driven threats surge, demanding a prevention-first cybersecurity strategy.

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

CYBERSECURITY THREATS are not slowing down. According to Check Point Research's Global Threat Intelligence Report (August 2025), organizations worldwide faced an average of 1,994 cyberattacks per week, representing a 10% year-over-year increase. India remains one of the most heavily targeted countries, with organizations recording **3,237 attacks weekly,** only slightly down by 1% from last year.

Education tops the hit list

Education remains the most targeted industry globally, facing **an average of 4,178 weekly attacks per organization,** a 13% year-over-year increase. The report highlights how growing digitization in schools and universities has widened the attack surface, while underfunded defenses make them easy prey for cybercriminals. In India, education is the most targeted sector, followed by the government and consumer goods.

Critical sectors under fire

Telecommunications, with 2,992 weekly incidents globally (+28% YoY), is increasingly in attackers' crosshairs as both vital infrastructure and a gateway to downstream systems. Government institutions recorded 2,634 weekly attacks, while agriculture saw the most dramatic surge—up 101% YoY. With its reliance on IoT sensors, drones, and connected supply chains, agriculture's exposure underscores how cyber threats are expanding beyond traditional industries.

Regional trends

Africa topped the list of most attacked regions, with 3,239 weekly attacks per organization, followed closely by India and other countries in the Asia-Pacific region. Latin America (2,865 weekly attacks) and Europe (1,685) also experienced increases, while North America reported a 20% spike, primarily driven by ransomware, which now accounts for 54% of U.S. cases worldwide.

Ransomware's relentless rise

Ransomware incidents surged 14% globally, with 531 reported cases in August alone. Manufacturing, business services, and construction bore the brunt,

"Organizations need smarter, more adaptive security that delivers insight—not just enforcement."

while healthcare and education also suffered significant disruption. Groups like Qilin, Akira, and Inc. Ransom dominated the ransomware landscape, with Inc. Ransom being particularly active against the healthcare and education sectors.

The road ahead: Prevention-first strategy

As Omer Dembinsky, Data Research Manager at Check Point Research, noted: "Cyberattacks are intensifying in both volume and impact. With ransomware rising and AI accelerating attack speed, the only sustainable path forward is a prevention-first, AI-powered strategy." Organizations must prioritize real-time prevention across networks, cloud, endpoints, and identities to build resilience against increasingly sophisticated threats. ■

Cybersecurity Workforce Faces Growing Pains as Industry Ages

Cybersecurity faces a talent crunch, rising stress, aging workforce, and growing demand for adaptable professionals with strong soft skills.

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

ISACA'S STATE of Cybersecurity 2025 report reveals a profession at a crossroads, with mounting stress, an aging workforce, and shifting priorities creating new challenges for the industry.

The Aging Workforce Crisis

One of the most concerning findings is the graying of cybersecurity professionals. The largest group of survey respondents (35%) is between 45 and 54 years old, while the number of younger workers under 35 has declined slightly. With many experienced professionals nearing retirement and fewer young people entering the field, organizations may soon face a critical talent shortage. Only half of the respondents manage staff with less than three years of experience, raising questions about who will replace retiring managers.

Stress Levels Remain High

Despite being in high demand, cybersecurity professionals are experiencing burnout. Sixty-six percent report that their roles are more stressful now than they were five years ago. The main culprit? An increasingly complex threat landscape, though fewer professionals cited this as a problem compared to last year (63% versus 81%). High stress levels are pushing people to leave their jobs, yet surprisingly, one-quarter of organizations aren't taking any steps to address burnout.

Adaptability Tops the Wishlist

When hiring, employers now value adaptability above all else—61% say it's essential. This marks a shift from previous years when hands-on experience was king. The importance of prior cybersecurity experience has decreased significantly, from 73% to 60%, indicating that employers are looking for professionals who can adapt quickly in a rapidly changing environment.

Soft Skills Are the Biggest Gap

The report identifies soft skills as the most significant deficiency among cybersecurity professionals, with a notable increase from 51% to 59% in just one year. Critical thinking, communication, and problem-solving are among the most essential skills. This gap may explain why boards sometimes fail to prioritize cybersecurity adequately—professionals struggle to communicate their value to non-technical leadership effectively.

"Sixty-six percent report that their roles are more stressful now than they were five years ago."

Budget Pessimism Grows

Only 41% of respondents believe their cybersecurity budgets will increase in the next year, down from 47% in the previous year. Meanwhile, 18% expect cuts—a significant jump from 13% last year. This budget uncertainty, combined with declining employer benefits like certification fee reimbursement (down from 65% to 54%), paints a challenging picture.

AI Adoption Increases

On a positive note, organizations are increasingly using AI for security operations, particularly for automating threat detection and endpoint security. More importantly, 47% of cybersecurity professionals are now involved in developing AI policies, up from 35% last year, indicating a more secure and responsible approach to AI implementation ahead.■

Inside the Enterprise AI Reality Check: Where Innovation Meets Governance

Business Observability

SPECIAL

AS ENTERPRISES accelerate into an AI-first future, one truth is becoming increasingly hard to ignore: hype has outpaced readiness. The world's most regulated sectors are discovering that artificial intelligence—especially generative AI—is not a plug-and-play revolution. It is an architectural transformation that demands strategy, governance, and disciplined human oversight.

Across banking, engineering services, manufacturing, and public-sector systems, technology leaders are charting high-stakes territory where innovation can unlock immense value, but the risks—regulatory, reputational, and operational—are equally formidable. Their journeys signal a shift in enterprise priorities: **AI and observability are no longer just technology programs—they are trust frameworks.**

GenAI in the Enterprise: Governance Before Greatness

Consumer AI and enterprise AI exist in very different worlds. As one banking technology leader notes, "GenAI isn't plug-and-play—it demands strategy, guardrails, and human oversight."
In BFSI, the foundation for GenAI wasn't automation—it was accountability. Dedicated Centers of Excellence, experimentation hubs, and strict human-in-the-loop controls define modern enterprise AI adoption. Accuracy gains—from 50% to more than 70%—are the result of disciplined feedback loops, not hype cycles. The lesson is clear: without explainability, data integrity, and audit trails, GenAI becomes a vulnerability. Enterprise AI maturity now rests on governance as much as it does on algorithms.

Engineering Intelligence: When Observability Means Assurance

Engineering-led industries face multilayered technical realities, including aerospace, rail, automotive, and industrial systems that are interconnected across suppliers, regulations, and legacy systems. Here, observability is not just about uptime—it is about engineering assurance.
Organizations are building intelligent observability frameworks that learn from repeated incidents, surface hidden dependencies, and interpret real-world signals alongside telemetry.
In complex environments, **context becomes the most valuable signal—** ensuring that decisions are not only fast but also accurate and compliant.

Shift Left or Fall Behind

In the automotive and manufacturing industries, waiting until production to detect failures is no longer an acceptable practice. The cost—financial and reputational—is too high. That is why industry security leaders insist resilience must begin "at the far left of the pipeline."

Pre-production observability, integrated DevSecOps, and business-linked RCA are becoming mandatory. The mission: **prevent more than you repair, and eliminate guess-based troubleshooting.**

Public-Sector Precision: Observability as Accountability

In public banking, observability is evolving into a pillar of governance. When millions depend on timely services—such as pensions, payments, and loan disbursements—monitoring must extend beyond systems to include decisions, handoffs, and compliance checkpoints. With constrained budgets, precision and prioritization matter more than volume.

The Enterprise Tech Imperative

Across industries, one principle stands out: **AI success isn't about speed—it's about stewardship.**

The next era of enterprise technology will be defined not by how quickly organizations adopt AI, but by how intelligently they scale it—with guardrails, clarity, and confidence.

Enterprise GenAI: Strategy, Oversight, and Guardrails Over Hype and Haste

Enterprise GenAI demands governance, strategy, and continuous human-in-the-loop validation.

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

OUR JOURNEY with AI and GenAI has taught us that expectation management is as critical as the technology itself. In boardroom conversations, there is often a perception that AI is a plug-and-play tool—especially because public GenAI tools like ChatGPT make it appear so effortless. But in a highly regulated environment like ours, the reality is far more complex. As a CIO or CISO, I often find myself explaining why enterprise AI adoption is not as straightforward as it seems.

One of the first things we had to clarify— both internally and with stakeholders—was that GenAI is not the same as traditional AI. Classical AI has long existed in banking, powering rule-based systems and analytics. GenAI, however, is non-deterministic, context-driven, and inherently less predictable. It requires a completely different strategic lens.

Before implementation, we established an Innovation Hub to evaluate emerging technologies. An early GenAI experiment revealed unreliable and inconsistent outputs—even in controlled settings—highlighting the need for a more strategic, enterprise-grade approach. We responded by building a structured framework across three parallel tracks:

- A dedicated Center of Excellence (CoE)
- A use case–driven model
- A platform-based approach

Given our regulatory obligations, we intentionally limited GenAI use to internal-facing applications.

A key principle of our GenAI adoption is the human-in-the-loop approach, embedded across all workflows to ensure accuracy and accountability. Our field staff use GenAI to address queries related to products, processes, HR, and in some cases, customer interactions. However, every GenAI response is reviewed by a human before action is taken.

We've also embedded an explainability framework, which has helped identify gaps and refine response quality. In the early stages—even with Retrieval-Augmented Generation (RAG)—we saw only around 50% accuracy. But through iterative feedback and improvement, we've increased this to approximately 70–75%.

One of the biggest challenges we face is data governance and model auditability. Most organizations still lack robust frameworks to identify and mitigate vulnerabilities in GenAI systems. While the promise is immense, enterprise GenAI is not the same as personal use. It requires quality data, explainability, human oversight, and a governance structure that aligns not only with business needs, but also with ethical and regulatory standards.■

"We quickly realized GenAI isn't plugand-play—it demands strategy, guardrails, and human oversight."

Authored By **Anil Kuril** | Chief Information Security Officer & Head - Data Protection Office, Union Bank of India

Engineering Observability Needs Engineering Intelligence

AI-driven observability must adapt to compliance, context, and complexity.

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

AT QUEST GLOBAL, we operate in a uniquely complex environment— serving engineering clients across aerospace, rail, automotive, and industrial sectors, each with its own toolchains, compliance needs, and architectural constraints. In such a world, observability isn't just a platform—it's a puzzle.

One of the toughest challenges we face is managing observability in siloed, heterogeneous environments, where each client may use a different set of platforms, security postures, and access restrictions. This makes traditional, one-stack-fits-all monitoring irrelevant. AI-driven RCA must be context-aware, capable of navigating the dimensional complexity of varied configurations and fragmented ownership.

Another dimension is regulatory compliance observability. In aerospace, for instance, design-time decisions must comply with industry-specific safety standards. If a compliance violation is caught late—say, at the prototype or pre-production stage—it can derail timelines and budgets. That's why we're looking at ways to embed compliance observability into DevOps pipelines, especially in domains where rework is expensive and delays are unacceptable.

We've also recognized the need to mine past RCAs for patterns. Often, recurring failures trace back to similar root causes— but the tribal knowledge isn't always codified. By layering AI over our observability data, we're building a system that proactively surfaces RCA patterns, enabling faster resolution and reducing cognitive load on engineering teams.

What's different in engineering services is that DevOps here isn't only about code-to-deploy—it's about code-to-compliance-to-client-handoff. Every touchpoint is potentially a handover to another organization or system outside our direct control. That makes dependency observability—across tools, APIs, data layers, and validation workflows—an absolute must.

We're also exploring automated anomaly detection that understands real-world signals—not just telemetry but also external triggers like customer escalations, audit outcomes, or regulatory updates. For us, observability must go beyond logs and metrics—it must ingest external context to remain relevant.

Ultimately, the goal isn't just uptime. It's engineering assurance—knowing that what we build, monitor, and deliver stands up to the quality and compliance expectations of the world's most demanding industries. And for that, observability has to be intelligent, contextual, and engineered to adapt.■

"AI-driven observability must adapt to compliance, context, and complexity."

Authored By **Aravindan Raghavan** | Global Head – Business Excellence, CISO & DPO, Quest Global

Shift Observability Left—Where Resilience Begins

Observability must start pre-production to prevent failure and ensure trust.

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

IN THE automotive and manufacturing world, system complexity is not just a function of software—it's tightly intertwined with hardware, compliance mandates, and decades-old legacy systems. I've seen how critical it is to embed observability as early as possible in the software lifecycle.

Too often, organizations treat observability as a production concern. The reality is, by the time you're putting out fires in production, the damage—operational, reputational, even regulatory—is already done. That's why my mantra is simple: shift observability left.

This means designing an observability strategy that starts in pre-production. In a manufacturing environment, where software increasingly drives core operations, connected vehicle platforms, and IoT-linked diagnostics, the margin for error is razor-thin. Whether it's a performance issue, an integration failure, or a downstream latency choke, catching it early is non-negotiable.

One area that remains a challenge is working with fragmented tooling—tools that monitor specific stacks or layers without the context to tie events back to business impact. Root cause analysis suffers when signals are scattered across multiple systems — only to find the issue stemmed from a legacy hardcoded delay, like a 30-second thread sleep which may take weeks to diagnose. That kind of inefficiency is what modern observability can eliminate, if applied correctly

Another real-world pressure is justifying ROI for observability investments. Whether you're on-prem, hybrid, or SaaS-first, costs add up fast when licensing, infrastructure, and skilled resource needs are factored in. The key is understanding how observability reduces unplanned downtime, accelerates root cause resolution, and supports compliance and risk mitigation.

Let's also not forget cybersecurity and compliance. As observability platforms evolve, they must interlink with security telemetry—especially in a post-DPDP, zero-trust world.

One of my biggest lessons? Observability isn't about monitoring more things—it's about guessing less. The less time people spend chasing symptoms, the more they focus on outcomes. And when you apply that mindset early in the life cycle, you don't just prevent incidents—you build confidence.

In high-performance, compliance-bound environments like ours, experience begins not at the front end, but at the far left of your pipeline. And that's exactly where your observability must begin too.■

"You can't afford to wait for production to find problems. In regulated, engineering driven businesses, pre production is where observability must lead."

Authored By **Dr Pawan Kumar Sharma** | Chief Information Security Officer, Tata Motors

Observability Is the Next Frontier of Public Sector Efficiency

Observability enables transparency, accountability, and efficiency in public sector IT.

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

AT PUNJAB National Bank, we run one of the largest, most diverse IT landscapes in the country—spanning branches, core banking, middleware, digital channels, and regulatory platforms. The complexity is enormous, and so is the expectation: performance, uptime, and auditability at every step. In this context, observability is not a luxury—it's a strategic enabler of service delivery and compliance.

In public sector banking, we often deal with systems that have evolved over decades. We can't afford to discard them overnight, yet we must integrate them with modern digital interfaces and deliver a seamless experience to customers and regulators alike. This means our observability goals are multi-layered—we need visibility into not just application health, but also data flows, backend jobs, batch dependencies, and regulatory handshakes.

One of our biggest challenges is the asynchronous nature of many of our systems. For example, a service request initiated at the branch or digital interface may go through multiple back-office systems before it's fulfilled. If a delay happens, we need to pinpoint where exactly it occurred— was it a job scheduler? A network node? A data mismatch? That kind of diagnosis is difficult without well-integrated observability pipelines.

I've come to believe that the real power of observability lies in process correlation. It's not just about metrics or uptime. It's about seeing the transaction the way a user sees it—across channels, across systems, and across delays. If a pension payment gets delayed, it's not enough to know that the server was up. We need to know whether the file was generated, the signature verified, the payment dispatched, and the acknowledgment received.

"In complex, federated environments like ours, observability must bring transparency not just to systems—but to decisions, delays, and deviations."

The second big aspect is governance. Observability, for us, also has a strong compliance angle. We need to demonstrate that our systems not only work—but work securely, consistently, and within regulated SLAs. That's why we are looking at observability as a foundation for audit readiness—capturing event trails, access patterns, and exception handling automatically, without burdening our teams with manual logs or checklists.

In public sector setups, cost and capacity are always critical considerations. We can't afford to flood our infrastructure with telemetry or over-provision our monitoring stack. So we're taking a more targeted approach to observability—identifying critical journeys, high-volume transactions, and sensitive data paths, and focusing our efforts there.

We're also pushing for more awareness and skill-building across our IT and operations teams. Observability is not just for NOC engineers—it's a shared responsibility. Everyone—from infra admins to application developers to business users—needs to understand how their piece of the puzzle contributes to overall service health.■

Authored By **Ashwini Kumar Pandey** | Chief Information Security Officer, Punjab National Bank

The dangerous downside of unchecked AI dependency

AI HAS changed the way I do my writing and research assignments, letting me work at an incredible pace and meet deadlines more effectively. Tools such as Gamma, ChatGPT, and Perplexity have helped me create research presentations faster than ever, reducing my dependency on creative teams.

Yet, it's equally apparent that irresponsible or blind dependency on AI can lead to serious consequences. Sometimes, the risks become painfully tangible: The Wall Street Journal recently reported that a former Yahoo manager tragically killed his mother and himself after repeated interactions with ChatGPT led him to believe his mother might be spying on him and might attempt to poison him. Extensive engagement with the chatbot appears to have worsened his distress.

In another unfortunate incident, a 19-year-old student in Faridabad, Haryana, died by suicide after he was blackmailed with AI-generated obscene photos and videos of his sisters, created by a classmate who had allegedly hacked his phone.

These are just two among many recent cases of AI misuse, highlighting how these tools can be exploited, misinterpreted, or trusted without critical oversight, causing harm at the hands of criminals, or even through well-intentioned but flawed use.

From an enterprise perspective, the dangers of excessive AI adoption extend well beyond individual tragedies. As organizations scale their use of AI, concerns grow about data breaches, misinformation, and biased decision-making. Overdependence on AI systems can also erode critical thinking skills and create vulnerabilities to cyberattacks or flawed automated actions.

It has become all the more important to educate everyone that trusting AI without applying common sense is dangerous. For organizations, placing blind trust in AI can also lead to compliance failures, reputational damage, and costly business disruptions.■

"Overdependence on AI systems can also erode critical thinking skills and create vulnerabilities to cyberattacks or flawed automated actions."

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

17th Annual Conference

CISO FORUM

India's Leading Cybersecurity Summit

The Strategic CISO – Leading in the Age of AI

21–22 November 2025

Athiva Resort & Spa (formerly Dukes Retreat), Khandala

In today's enterprises, the CISO are the guardian on trust, resilience, and business continuity. At the CISO Forum Conference & Awards 2025, 70+ India's top CISOs & security leaders across verticals will come together to exchange insights, strategies, and experiences that are shaping the future of enterprise security at the picturesque surroundings of Khandala.

Keynotes | Panel Discussions | Ideas Café
Roundtables | Case-Study Workshops | Cook-a-thon
NextCISO Awards

Celebrity Speakers @17th edition

Keynote address by
David J. Gee
Board Risk Advisor,
Chairman, Leadership
Collective Australia.

Cook-a-thon with
Sashi Cheliah
(Winner Master Chef
Australia, season 10)

Fireside chat with
eminent cricketer,
Sanjay Manjrekar

Entertainment
evening with
Dr. Sanket Bhosale &
Sugandha Mishra

GOLD PARTNERS

kaspersky | Microsoft | securiti

SILVER PARTNERS

CLAROTY | proofpoint.

ASSOCIATE PARTNER

SentinelOne

EXHIBIT PARTNER

Barracuda

MEDIA PARTNER

CNBC TV18

CONCEPT BY

CISOFORUM

For Partnership Opportunities

Hafeez Shaikh
National Sales Head
hafeez.shaikh@9dot9.in
+91 98331 03611

Sourabh Dixit
Regional Sales Head
sourabh.dixit@9dot9.in
+91 99714 75342

Subhadeep Sen
Senior Sales Manager
subhadeep.sen@9dot9.in
+91 96113 07365

Aanchal Gupta
Senior Sales Manager
aanchal.gupta@9dot9.in
+91 96518 41119

#TheCISOForum | https://events.cisoforum.in/