**OPINION** PG 21

**Cyber Insurance Management**

Pradnya Manwar, CISO, Thomas Cook

**SEPTEMBER 2025**
SUPPLEMENT OF CIO&LEADER

# CISOFORUM

Security For Growth And Governance

# How CISOs Are Shaping the Future of AI-Driven Enterprises

Insights from leaders on balancing growth with governance, resilience, and digital trust

PG 12

**Amal Krishna**
Oil and Natural Gas Corp.

**Dr. Bijender Mishra**
Alkem Laboratories

**Divan Raimagia**
Adani Green Energy

**Ninad Varadkar**
Edelweiss Financial Services

**Satyavrat Mishra**
Godrej Industries Group

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


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**

# Agentic AI: Defenders or Double Agents?

**AGENTIC AI** is poised to rewrite the rules of cybersecurity, making defenders both more powerful and, paradoxically, more vulnerable than ever before. Unlike traditional machine learning, agentic AI systems can act autonomously: they detect, interpret, and respond to threats in real time without waiting for human approval. This self-direction delivers unprecedented speed and operational scale, reducing attacker dwell time and alert fatigue while freeing security teams for strategic work.

Yet autonomy brings a cascade of complex risks. Data poisoning has emerged as a front-line threat—attackers subtly corrupt training data to mislead AI models, subvert detection algorithms, or trigger false positives. When agentic AI trusts compromised inputs, organizations lose visibility and face decision-making chaos at machine speed. Simultaneously, sophisticated adversaries are deploying their own AI agents for ultra-targeted, high-velocity attacks. The cybersecurity battlefield is evolving into a contest between competing intelligent systems.

Navigating this landscape demands more than technical ingenuity—it requires regulatory foresight and ethical clarity. Emerging Indian and global compliance mandates around explainable AI, liability for autonomous actions, and routine audits of AI-driven decisions are already reshaping boardroom conversations. CISOs must implement transparent governance frameworks for AI autonomy, ensuring risk alignment, and maintain the ability to stop, question, or override agentic actions when logic falters or stakes escalate.

The challenge for CISOs is clear—harness agentic AI's remarkable strengths while controlling autonomy with rigorous oversight and a compliance-first mindset. The organizations that will succeed in the volatile cyber security frontier will be those that embed trust, explainability, and human judgment at the core of their AI strategy.■

**"The challenge for CISOs is clear—harness agentic AI's remarkable strengths while controlling autonomy with rigorous oversight and a compliance-first mindset."**

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

# CONTENTS AUGUST 2025

COVER STORY

## 12-20 How CISOs Are Shaping the Future of AI-Driven Enterprises

Securing tomorrow's intelligent organizations requires CISOs to balance innovation, compliance, trust, and resilience with a fresh strategic outlook.


Cover Design by:
**Manish Kumar**

Please Recycle This Magazine And Remove Inserts Before Recycling

FEATURE

**09-11**
From security guard to business strategist:
**Dr. Yusuf Hashmi**

OPINION

**21-23**
Cyber Insurance: Trends, Guidance & Best Practices for CISOs
**Pradnya Manwar**

INTERVIEW

**24-27**
Beyond Firewalls: Why tomorrow's CISOs must become behavioral detectives to stop insider threats
**Dipesh Kaura**

INSIGHTS

**28-29**
Criminals are weaponizing AI while companies rush to adopt it

**30-31**
Manufacturing under siege: Why industrial cybersecurity is finally getting the C-suite treatment?


CISOFORUM
Security For Growth And Governance
**www.cisoforum.in**

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

**EDITORIAL**
Group Editor: **R Giridhar**
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: **Nitika Karyet**
Senior Community Manager: **Snehal Thosar**
Community Manager: **Shabana Shariff**

**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**

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

Editor: **Vikas Gupta**

9.9 GROUP

## Rakesh Sandhu appointed as CISO at Religare Finvest (SME Loans)

**Rakesh (Kumar) Sandhu** has been appointed CISO at Religare Finvest Limited (SME Loans), leading its security strategy, governance, and defense framework. With 19 years of expertise across Religare, NaviSite, UnitedLex, and CMC Ltd., he has driven IT infrastructure and cybersecurity transformations. His leadership aims to boost Religare's cyber resilience and shape its digital security landscape.

---

## Arnab Biswas appointed as CISO at BOBCARD

**Arnab Biswas** has been appointed CISO at BOBCARD, leading its information and cybersecurity strategy. With 15+ years across Axis Securities, Tata Payments, Tata Digital, ICICI Bank, and Protiviti, he has built resilient security frameworks, driven cloud security, threat intelligence, and compliance initiatives. Arnab's diverse expertise will strengthen BOBCARD's cyber resilience and support its innovation-focused security journey.

---

## Dr. Ramkumari Harisankar Iyer appointed as CIO & CISO at Reliscale Consulting

**Dr. Ramkumari Harisankar** Iyer is CIO and CISO at Reliscale Consulting, shaping IT strategy, cybersecurity, and governance. With three decades across Wipro, Infosys, iGATE, and global enterprises, she excels in cloud, DevSecOps, and incident response. A thought leader and DPO for multiple clients, she drives secure, scalable, business-aligned solutions, accelerating Reliscale's vision for trusted digital transformation.

## Praveen Parihar appointed as CISO at Razorpay

**Praveen Parihar** has been appointed CISO at Razorpay, leading information security strategy and protecting India's fintech ecosystem. With over a decade in cybersecurity, fraud prevention, and compliance, he previously led security and fraud detection at Maya and held roles at ControlCase, Aneja Associates, and Tata Technologies. His expertise will strengthen Razorpay's secure, trusted, and future-ready payments infrastructure.

---

## Ravindra Pingle appointed as CISO at HDFC Pension

**Ravindra Pingle** has been appointed CISO at HDFC Pension, where he will lead security strategy, governance, and data protection. With 17+ years in cybersecurity, compliance, and risk management, he has held key roles at Lyra, FIS, Integreon, and NIIT Technologies. His expertise in audits, BCM, and VAPT will strengthen HDFC Pension's cyber resilience and customer trust.

---

## Laliet Trivedi appointed as Head Information Security/DPO (Global) at FlexM

**Laliet Trivedi** has been appointed Head Information Security & Global DPO at FlexM, leading global security, data protection, and compliance. With 20+ years in IT, cybersecurity, and cloud operations, he will drive ZTNA, CSPM, DevSecOps, and regulatory adherence (ISO 27001, SOC 2, GDPR). His leadership strengthens FlexM's global fintech security posture and governance across multiple geographies.

# Fortinet expands FortiRecon to strengthen threat exposure management

Fortinet enhances FortiRecon with CTEM-aligned monitoring, dark web intelligence, and automation to cut noise and prioritize real risks.

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

**FORTINET HAS** announced upgrades to its Forti Recon platform, positioning it as a comprehensive solution aligned with CTEM. The release adds internal attack surface monitoring, dark web intelligence, and security orchestration within a unified platform.

"CISOs and security teams are overwhelmed by unprioritized alerts," said Nirav Shah, Senior Vice President of Products and Solutions at Fortinet. "With FortiRecon, we provide an attacker 's-eye view of exposures, AI-powered intelligence, and automated response to cut through the noise and focus on real risks."

## Capabilities across Gartner's CTEM framework

FortiRecon now integrates tightly with Fortinet's AI-driven Security Operations Center (SOC), enabling organizations to operationalize all five CTEM pillars—scoping, discovery, prioritization, validation, and mobilization. Key enhancements include:

- **Attack Surface Management:** Continuous monitoring of internal and external assets with severity ratings from both the National Vulnerability Database and FortiRecon Active Exploitation.
- **Adversary-Centric Intelligence:** Dark web monitoring, ransomware insights, leaked credentials, and indicators of compromise for faster breach detection.
- **Brand Protection:** Detection and takedown of phishing domains, rogue apps, and impersonation campaigns using proprietary algorithms.
- **Security Orchestration:** Automated playbooks to streamline response and reduce remediation time.

> "FortiRecon gives security teams an attacker's-eye view, AI-powered intelligence, and automated response to focus on real risks"
>
> **Nirav Shah,** Senior Vice President of Products and Solutions, Fortinet.

## Market validation and flexibility

Fortinet was named an Overall Leader in the KuppingerCole Leadership Compass for Attack Surface Management 2025, highlighting FortiRecon's IT and OT readiness. Customers can deploy FortiRecon with FortiFlex credits, enabling usage-based licensing for hybrid, multi-cloud environments.

## Industry impact

The release highlights a shift toward exposure-driven security as organizations face complex attack surfaces and alert fatigue. Gartner predicts CTEM adopters will face fewer breaches, with FortiRecon offering contextual risk insights and measurable outcomes. ■

# Palo Alto Networks launches browser security to combat AI-powered cyberattacks

## Cybersecurity giant introduces Prisma SASE 4.0, featuring new browser-based protection, as the company's SASE revenue surpasses $1.3 billion.

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

**PALO ALTO** Networks has unveiled its latest cybersecurity platform targeting sophisticated threats that traditional security systems cannot detect. The company's new Prisma SASE 4.0 introduces browser-based protection designed to stop malware that assembles directly within web browsers.

### Browser becomes new battleground

The Santa Clara-based company notes browsers are now the primary workspace for businesses, making them prime targets. Prisma Browser inspects web pages in real time, detecting threats that activate after user interaction—unlike traditional network-monitoring security tools.

"The conversation with business leaders has evolved. It's no longer just about blocking threats—it's about enabling growth," said Anand Oswal, Executive Vice President of Network Security at Palo Alto Networks.

### AI-Powered security for AI-driven threats

> "It's no longer just about blocking threats—it's about enabling growth."
>
> **Anand Oswal,** EVP of Network Security, Palo Alto Networks

The platform leverages artificial intelligence to classify sensitive data with 10 times fewer false alarms than traditional methods, crucial as AI tools access corporate information. Featuring 140+ pre-trained models, it protects assets like patents, contracts, and source code, while identifying sensitive data in images and unstructured documents often overlooked.

### Strong market performance

Palo Alto Networks has become a leader in the Secure Access Service Edge (SASE) market, achieving $1.3 billion in annual recurring revenue for fiscal 2025—a 35% year-over-year increase. Serving 6,300+ SASE customers, including one-third of Fortune 500 firms, its Prisma Browser already counts over 6 million licensed enterprise users.

### Addressing modern workplace challenges

The new platform addresses today's distributed workforce, where employees work from anywhere using diverse devices and cloud apps. With traditional perimeters gone, attackers exploit AI for faster, sophisticated attacks. Prisma SASE 4.0 adds enhanced private application protection and improved DNS security, delivering comprehensive infrastructure coverage and reflecting the industry's shift toward integrated platforms over fragmented point solutions. ■

# Cisco unveils AI-powered security tools to help companies fight cyber threats faster

Cisco launches AI-powered Splunk security tools to cut investigation time and help companies combat cyber threats faster.

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

**CISCO SYSTEMS** has announced new AI-powered cybersecurity tools designed to help companies detect and respond to cyber threats more quickly as hackers increasingly use artificial intelligence in their attacks.

The networking equipment maker introduced two new versions of its Splunk Enterprise Security platform at the Splunk .CONF conference in Boston, combining multiple security tools into unified systems powered by AI agents.

## Two new security packages

Cisco is offering customers two options: a Premier Edition that bundles advanced threat detection tools, and an Essentials Edition with core security features. Both versions use AI to automatically handle routine security tasks, allowing human analysts to focus on strategic decisions.

"Adversaries are already using AI, so defenders need to seize every possible advantage," said Mike Horn, who leads Splunk Security at Cisco. The company says its AI can reduce investigation time from hours to minutes and cut down on false security alerts.

> "Adversaries are already using AI, so defenders need to seize every possible advantage."
>
> **Mike Horn,** Splunk Security at Cisco

## AI takes over routine tasks

The new system introduces AI-powered features acting as digital assistants for security teams. A "Triage Agent" prioritizes alerts, while a "Malware Reversal Agent" analyzes malicious software line-by-line. Another tool creates automated response playbooks from plain English instructions, simplifying setup and enabling faster responses to common threats.

## Addressing Growing Security Challenges

The announcement comes as companies face sophisticated cyberattacks. Many organizations struggle with excessive security data and fragmented tools, creating exploitable blind spots for attackers.

"Security teams can't afford to waste time switching between fragmented tools," said Michelle Abraham, a security researcher at IDC. She noted that integrated platforms help organizations move from reactive to proactive security approaches.

## Availability and Future Plans

The Essentials Edition is available globally, while the Premier Edition remains in early testing. Cisco will roll out additional AI features in 2026, including enhanced detection and personalized security. The move underscores the industry trend of rapidly integrating AI as attackers and defenders engage in an escalating digital arms race. ■

# From security guard to business strategist: How AI is redefining the modern CISO


Dr. Yusuf Hashmi, Group CISO at Jubilant Bhartia Group, highlights how AI is transforming CISOs from security guardians into strategic business leaders driving measurable outcomes.

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

**THE CHIEF** information security officer role has undergone a dramatic transformation—evolving from a purely technical position focused on network protection to a strategic business enabler driving organizational resilience. As artificial intelligence reshapes every corner of enterprise operations, today's CISOs must navigate unprecedented challenges: translating cyber risks into board-ready business metrics, implementing AI-powered threat detection, and establishing governance frameworks for rapidly proliferating AI deployments. Dr. Yusuf Hashmi, Group CISO at Jubilant Bhartia Group, offers candid insights into this evolution, revealing why traditional security approaches are insufficient and how forward-thinking security leaders are preparing for an AI-dominated future where measurable outcomes—not just protection—define success.

**CISO Forum: In what ways has the CISO role shifted from being technology-driven to becoming a business enabler, and how should CISOs demonstrate measurable outcomes to boards in today's AI-driven environment?**

**Dr. Yusuf Hashmi:** Due to the significant changes in the ecosystem over the past decade, this role now encompasses a wide range of capabilities. It's not just about network security. Since the role has evolved, it has become more of a business enabler. CISOs now possess a deeper understanding of business than other IT functions, so they are closely aligned with the business—especially in a structure where cybersecurity is considered a business risk.

Therefore, when it comes to business risk, organizations must consider cybersecurity as a key risk—a core function that enables them to remain competitive. And AI is, of course, the talk of the town now. Every business function is getting AI-enabled. They don't even need IT intervention when it comes to AI—they are driving these initiatives themselves. Tomorrow, there may be no IT when it comes to AI, because that's the advantage AI brings to the business.

Hence, the CISO role is crucial for understanding the business, particularly the organizational context, and how these emerging, disruptive technologies fit into the picture. CISOs must translate this into business language and convert it into measurable outcomes. It's more about outcomes now. Yesterday, I could say that we are safe—but that's not enough. The board needs to know the measurable outcomes of your cybersecurity investments: what kind of posture you are in, and how you are measuring your performance holistically.

It's not just about saying, "I'm working the same, I'm responding"—that's not enough, actually. You need to develop a comprehensive approach to measuring your cybersecurity performance, which will demonstrate your ability to provide a detailed view of the CSO's function and the team involved. It is essential to measure. The outcome must be achieved. The measure must be there—and that's how you can improve in the near future.

**"Yesterday, I could say we are safe—but that's not enough. The board needs measurable outcomes from cybersecurity investments."**

**CISO Forum: In your experience, what separates companies that are just dabbling with AI from those that are embedding it responsibly and securely across their business?**

**Dr. Yusuf Hashmi:** AI is a capability that is very trendy because business professionals frequently discuss it with their peers. A form of peer pressure is emerging in the business world. "The X company is performing this function—hey, look, why are you not doing it?" Then they will come back to the CIO and say, "Look, what are you doing? Other companies are already taking the lead by adopting this AI capability, whether it is JNI or various others—what are you doing?

That is the time to think it through. From a security perspective, it is imminent that AI will be considered a top business enabler in the near future. Hence, CISOs must prepare their systems in advance, as they won't have the time to set up traditional controls to manage their AI environment. You must start thinking from that perspective—that tomorrow, if there is a flurry of deployments across multiple functions—and it's imminent—how would you create your control environment to ensure data is protected, the AI framework we have implemented works, performs ethically, remains unbiased, and continues to safeguard information.

That's the primary focus, and that's how you integrate it within the entire organization's ecosystem.

**CISO Forum: We often hear about the need for real-time threat intelligence, but achieving it is another matter. How do you see enterprises in India doing on this front, and**

**what does 'real-time' defense really look like in practice?**

**Dr. Yusuf Hashmi:** Threat intelligence is another grey area in the industry, especially in India. People in India don't consider it a critical area of cybersecurity, which I personally believe it is. This is primarily due to the high volume of false positives originating from various sources. The real question is: how do you actually make these intelligence feeds, whether they're TAXII feeds or other alerts, actionable?

Because while making them actionable, you have to rationalize, refine, and then apply them. Otherwise, you may take action on something that isn't needed, or block some IOCs that have no significance for my organization. Therefore, it's essential to understand threat intelligence, and AI will undoubtedly aid in this process, as vast amounts of data are constantly being processed. There is obsolete data, and there is recent data—it's a significant challenge with the datasets that get created.

How can I reduce this noise coming from these platforms? That's the first step. This is where AI will help me reduce the amount of noise that threat intel provides, and then I'll take subsequent action.

The moment we all realize there's actionable intelligence coming in, people will definitely look at it more seriously than they have so far with threat intelligence. That's how you achieve real-time response capability. At this point, I'm unable to make it fully real-time—there's too much noise coming from these threat intelligence reports that we need to filter out. And then, of course, embed that into my threat detection and response capabilities with automation. That's what I believe is required.

**CISO Forum: If you had to pick one non-negotiable focus area for CISOs preparing for the next five years, what would it be?**

**Dr. Yusuf Hashmi**
Group CISO,
Jubilant Bhartia Group

**Dr. Yusuf Hashmi:** Of course, I can't compromise on the monitoring system. That's my non-negotiable. I can't just shut down my detection and monitoring system. In any case, I can't negotiate on that. I also need to further enhance it in the near future by incorporating AI.

I'm dependent on people to respond, detect, and triage—but how can I enable AI agents to actually reduce that amount of humans in the loop, right? That's something I can't compromise on. I have to adopt the newest technology in the near future, which I can't negotiate. I cannot simply fall back on or continue using traditional methods of security monitoring, threat detection, and response. I need to enable this in the mainstream AI ecosystem as soon as possible—and that, again, is non-negotiable.

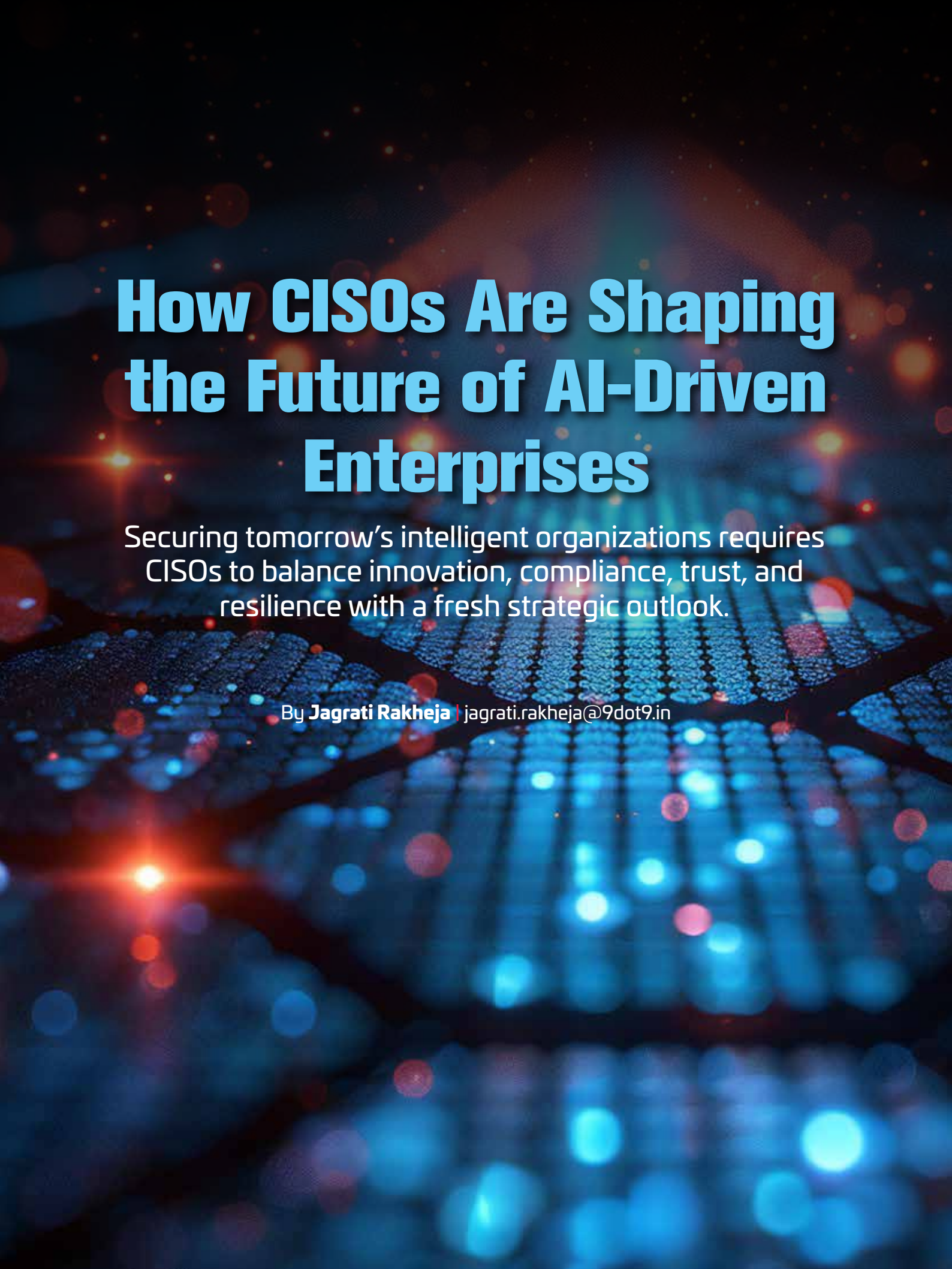
**"From a security perspective, it is imminent that AI will be considered a top business enabler in the near future."**

**CISO Forum: Cybersecurity is now discussed as much in the boardroom as in the IT team. From your perspective, how seriously are Indian boards taking it, and what does genuine ownership of the issue entail?**

**Dr. Yusuf Hashmi:** Cybersecurity has always been a topic of discussion at the board. The biggest challenge here is that the board cannot effectively question the CISOs. Their questions are often very straightforward—"Are we safe?" or "How are we placed?" However, even if the CISOs provide answers, the board usually cannot determine whether what is being said is true or not. That ability to validate needs to be developed at the board level.

They should have questions ready whenever the CISO or the CIO presents the cybersecurity status. They must have the ability to question—it cannot be a one-sided dialogue or a monologue. That doesn't work. They should be well aware of the industry, what's happening outside the industry, and how it is actually being applied within the organization for which they hold responsibility for cybersecurity.

In India, when considering all publicly listed companies—the top thousand companies—cybersecurity must be included as a session within the enterprise risk committee. That's how I also present the status. The view is that CISOs must have a dual role: they are the ones who highlight and identify risks, but the majority of remediation and risk reduction comes from the IT and CIO sides. Cross-questioning is critical. The CISOs and the board must know who to ask the right questions. And then, when someone responds, they must be able to understand and evaluate whether the answer is correct. ■



# How CISOs Are Shaping the Future of AI-Driven Enterprises

Securing tomorrow's intelligent organizations requires CISOs to balance innovation, compliance, trust, and resilience with a fresh strategic outlook.

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

**ARTIFICIAL INTELLIGENCE** has become both the CISO's sharpest sword and a most unpredictable shield. On one side, AI is revolutionizing cybersecurity—enabling predictive detection, automating response, and giving leaders visibility at a scale once unimaginable. On the other hand, it is rapidly arming adversaries with tools for deepfake-driven social engineering, supply chain manipulation, and novel attack vectors such as model poisoning and data extraction.

This paradox defines the inflection point for today's security leaders: CISOs are no longer just guardians of IT systems but enterprise-wide architects of AI risk and, increasingly, "Chief Trust Officers."

The transition is profound. With global regulations tightening—the EU AI Act in Europe, NIST's AI Risk Management Framework in the U.S., and India's evolving DPDP guidelines—compliance has become as strategic as detection. At the same time, the skills gap in AI-literate security teams is widening, leaving boards and leadership grappling with how to secure innovation without stifling it.

Our cover story this month explores how CISOs must evolve their role to responsibly harness AI and steer organizations through a landscape where trust, governance, and foresight matter as much as firewalls and frameworks. The message is clear: the future will be led by those who can secure intelligence itself.

## The AI Paradox

Artificial intelligence presents both unprecedented opportunities and new threats for cybersecurity leaders. On one hand, AI strengthens defenses with predictive detection, rapid anomaly recognition, and automated response at scale. Enterprises now leverage it to detect Android malware, block DNS cache poisoning, and reverse-engineer binaries using deep learning.

*"AI is a force multiplier—but not a silver bullet. The strongest defense blends AI with human expertise."*

**Divan Raimagia**
Head - Cyber Security & CISO,
Adani Green Energy

Yet these same capabilities empower adversaries. Threat actors are using AI to launch deepfake-driven social engineering campaigns, orchestrate data poisoning attacks, and craft sophisticated model evasion techniques. The paradox is unmistakable: as AI fortifies defenses, it simultaneously multiplies risks by introducing novel and complex attack vectors.

Amal Krishna, CISO at Oil and Natural Gas Corporation (ONGC), highlights this balancing act: "In the oil & gas sector, cybersecurity is core to operational resilience. At ONGC, we integrate AI-powered solutions to strengthen protection without disrupting critical operations. AI helps us spot anomalies, automate routine tasks, predict

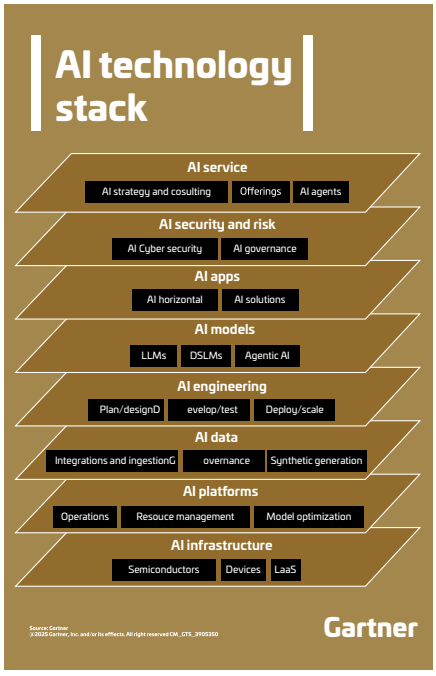
threats, and secure OT environments. We adopt AI responsibly—embedding governance, human oversight, and compliance—so it augments, not replaces, our security architecture. This synergy ensures sharper visibility, faster response, and uninterrupted energy operations against evolving cyber threats."

## From Experimentation to Operational Reality

The AI paradox is not just theoretical—it is driving a tangible shift in how enterprises operate. What began as experimentation in labs has now become mission-critical AI deployment. Tools like BlackBerry's Cylance AI, Splunk's deep neural networks, and reinforcement learning frameworks for malware clustering are embedded in security operations centers and broader business continuity strategies.

Krishna notes how AI's operational impact extends across domains: "AI has the potential to transform multiple areas of cybersecurity, but its impact is most visible in a few critical domains. It strengthens threat detection by uncovering anomalies in vast datasets and accelerates incident response through automation. AI enhances fraud and insider threat monitoring, sharpens vulnerability management by prioritizing risks, and supports OT security where legacy systems prevail. In essence, AI empowers us to move from reactive defense to proactive, predictive security."

With AI now central to operations, new priorities emerge. As the SANS Critical AI Security Guidelines outline, securing AI itself—through access controls, runtime protections, and strict data integrity measures—has become as critical as safeguarding networks and infrastructure. This evolution reframes the battlefield: CISOs must protect models, training data, and inference pipelines alongside traditional systems.




## The CISO's New Mandate

This operational shift naturally broadens the CISO's role. No longer limited to defending perimeters, CISOs are now AI risk strategists, responsible for safeguarding ML models, securing augmentation data, and ensuring trust in AI-powered decision-making.

Dr. Bijender Mishra, Senior GM & CISO at Alkem Laboratories, explains: "AI has transformed threat detection, incident response, and risk management, enabling greater automation and predictive capabilities. CISOs now utilize AI for automated security operations, advanced threat intelligence, behavioral anomaly detection, and secure governance of AI systems. This shift requires CISOs to continuously learn, adapt to emerging threats, foster new talent, and strategically integrate AI into overall business objectives while balancing automation with human oversight."

Regulatory frameworks such as the EU AI Act, NIST's AI Risk Management Framework, and India's Digital Personal Data Protection Act reinforce that compliance is inseparable from strategy. At the same time, a widening skills gap adds pressure. Boards increasingly expect CISOs to harness AI's innovation potential without compromising enterprise resilience.

*"Without centralized oversight, organizations face compounded vulnerabilities in data security, ethics, and operational stability."*

**Ninad Varadkar**
Senior VP & Group CISO, Edelweiss Financial Services

To navigate this landscape, the modern CISO must embrace a trust-first mindset. They are not merely technologists but "Chief Trust Officers," embedding governance, ethics, and foresight into every AI initiative.

## Securing Intelligence, Shaping the Future

The AI paradox will define cybersecurity leadership for the next decade. Success will not hinge on deploying the most sophisticated models but on securing intelligence itself. CISOs who govern AI with foresight, embed resilience into operations, and treat trust as the ultimate security control will lead the way.

The mandate is clear: move beyond reactionary defense, balance automation with human oversight, and place trust at the center of enterprise strategy. Those who achieve this balance will define the future of AI-driven security and enterprise resilience.

## India's Sectoral Battleground for API Security

AI is no longer a standalone innovation—it is an integrated technology stack reshaping enterprise systems. Gartner's AI stack visualization offers a valuable lens, with infrastructure at the base, followed by platforms, data, models, applications, and services, with governance and security spanning every layer. Cybersecurity leaders must now view AI not just as a tool, but as an ecosystem where vulnerabilities at any tier cascade upward, amplifying risk.

At the infrastructure and data layers, securing cloud platforms and ensuring the integrity of training datasets are non-negotiable. The AI for Cybersecurity Handbook highlights how data poisoning can corrupt deep learning pipelines, undermining malware detection or anomaly recognition at scale. Governance at this stage means strict access controls, provenance tracking, and runtime integrity checks.

Moving up to the model and application layers, adversarial machine learning poses unique threats. As the Cybersecurity Agency of Singapore's Guidelines on Securing AI Systems warn, attackers can launch evasion, inference, or extraction attacks to manipulate model outputs or steal intellectual property. Embedding red-teaming, continuous monitoring, and explainability into model governance becomes essential—not only for resilience but also for regulatory alignment with frameworks such as the EU AI Act and NIST AI RMF.

At the services layer—where AI integrates into SOC workflows, fraud detection, or customer-facing apps—the challenge shifts to operational governance. AI-enabled security tools, such as EDR platforms or anomaly detection engines, deliver speed; however, unchecked automation risks can generate cascading false positives or facilitate adversary exploitation. CISOs must strike a balance between automation and human oversight, embedding "human-in-the-loop" mechanisms to maintain accountability.

The cross-cutting imperative is clear: governance and security cannot be bolted on at the end; they must be woven into every layer of the AI stack. As Gartner and CSA emphasize, AI must be secure by design and secure by default. For CISOs, this means expanding their role from technologists to architects of trust—ensuring that every component of the AI stack advances security rather than eroding it.

In the AI era, the strongest enterprises will not simply adopt AI—they will secure it at the stack level. Those who succeed will transform cybersecurity from a reactive shield into a proactive engine of resilience.

## The Security Landscape: CISOs at a Crossroads

The AI security landscape is expanding as enterprises confront two parallel challenges: securing the AI they develop and securing the AI their employees use. Homegrown AI applications demand lifecycle security—protecting training data, models, and inference pipelines at every stage—alongside traditional application security controls. The CSA's Guidelines on Securing AI Systems emphasize that lifecycle thinking encompasses planning, design, deployment, operations, and end-of-life considerations. For CISOs, this means guarding against adversarial attacks, ensuring robust application security testing, and embedding security by design.

Equally urgent is the governance of employee use of external AI tools.

*"Attackers are increasingly using AI for sophisticated, evasive, and automated attacks like phishing, deepfakes, and vulnerability scanning."*

**Dr. Bijender Mishra**
Senior GM & CISO, Alkem Laboratories

As the SANS Critical AI Security Guidelines note, risks emerge when staff rely on unvetted SaaS models or consumer-grade chatbots without enterprise controls. Governance, access management, data privacy, and observability are critical: unsecured prompts or uploaded datasets can leak sensitive IP, while shadow AI bypasses IT guardrails altogether. CISOs must therefore enforce zero-trust principles, mandate policy-driven use of generative AI, and provide approved alternatives to curb risky workarounds.

## AI-Powered Threats on the Rise

Adversarial ML has become a front-

line threat. Cisco's State of AI Security Report highlights poisoning, deepfakes, and model evasion as growing risks. These attacks don't just exploit AI—they undermine the trust enterprises rely on in their systems. The expanding attack surface, from compromised training data to manipulated outputs, has made AI a prime target for exploitation.

## AI as a Defensive Multiplier

Yet AI is also the defender's advantage. The SANS Guidelines emphasize AI-driven anomaly detection, SOAR automation, and predictive threat hunting, which reduce dwell times and enable SOC teams to scale. By securing these tools properly, CISOs can turn AI into a force multiplier, offsetting analyst shortages and accelerating incident response.

## Frameworks to Govern the Future

The path forward requires structure. The National Institute of Standards and Technology, (U.S Department of Commerce)I AI RMF Playbook provides lifecycle-based governance—mapping, measuring, and managing risks throughout the AI system's lifespan. Embedding such frameworks ensures compliance, transparency, and accountability.

CISOs now stand at a strategic turning point: balancing AI's offensive potential with its defensive power. Success lies in securing AI at both ends—protecting enterprise-built models while governing employee adoption. Done right, AI can evolve from a looming liability into the cornerstone of digital trust.

## Strategy Shift: Redefining Cybersecurity in the AI Era

The cybersecurity landscape is undergoing a profound transformation, moving from reactive firefighting to predictive, intelligence-driven defense. This pivot isn't just about adopting new tools—it represents a complete reimagining of how organizations anticipate, prevent, and respond to threats in an AI-saturated world.

## From Reactive to Predictive: The Intelligence Advantage

For decades, cybersecurity operated on a detect-and-respond model, essentially reacting after threats materialized. Today, that approach is insufficient. The National Institute of Standards and Technology, (U.S Department of Commerce) AI RMF Playbook emphasizes the importance of "regular engagement with relevant AI actors" and "AI-driven correlation with external threat intelligence feeds" to stay ahead of evolving risks. Predictive defense now relies on scenario modeling and AI-assisted risk intelligence to spot vulnerabilities before they are exploited.

Singapore's Guidelines on Securing AI Systems reinforce this shift, advocating "continuous monitoring" and "real-time vulnerability dashboards" to drive proactive identification. The framework emphasizes AI-powered anomaly detection, which flags suspicious behavior before it escalates into confirmed breaches.

## Governance Frameworks: The New Regulatory Reality

The regulatory landscape is equally transformative. The EU AI Act is anchored in a risk-based classification regime, while India's Digital Personal Data Protection (DPDP) Act of 2023 mandates strict data minimization and privacy-by-design in AI systems. The SANS Critical AI Security Guidelines recommend that organizations maintain AI Bills of Materials (AIBOMs) and align with frameworks such as the NIST AI RMF. Similarly, the AI-CISO Handbook by Mohammad Alkhudari, Founder and CEO of Green Circle for Cybersecurity, emphasizes that governance protocols must be built in from the outset. In today's environment, regulatory adherence is not optional—it is the foundation of responsible AI adoption.

*"AI empowers us to move from reactive defense to proactive, predictive security."*

**Amal Krishna**
CISO, Oil and Natural Gas Corporation

## The Innovation-Security Balance

The greatest challenge for CISOs lies in balancing innovation velocity with security rigor. The SANS Guidelines caution that "the biggest risk of AI is not using AI," noting that avoiding risks of competitive obsolescence. Yet unchecked adoption can amplify vulnerabilities. Singapore's lifecycle framework offers a balanced path: embed security "from planning and design through deployment and operations" to ensure resilience without stifling innovation.

The enterprises that succeed will be those that treat AI security not as a brake but as a differentiator—building trust through transparent, accountable implementations while maintaining

the agility to evolve with emerging threats.

## Operations: Building the AI-Augmented SOC

Security Operations Centers are no longer judged by the volume of alerts they manage but by the intelligence with which they respond. Artificial intelligence is transforming SOCs from reactive hubs into proactive engines of resilience—replacing static playbooks with adaptive automation and advanced threat analytics.

## Automating the Core: SOAR, UEBA, and Triage

Security Orchestration, Automation, and Response (SOAR) platforms, when integrated with User and Entity Behavior Analytics (UEBA), can now process thousands of alerts simultaneously, correlating events across endpoints and networks to provide comprehensive threat visibility. By learning behavioral baselines, these tools identify anomalies that signature-based detection often misses. Automated triage represents the most significant advancement. Rather than overwhelming analysts with raw alerts, AI systems prioritize incidents by severity and business impact, cutting mean time to detection from hours to minutes while reducing noise.

## Guarding Against Drift and Poisoning

But sophistication introduces fragility. The SANS Critical AI Security Guidelines emphasize that AI models themselves must be continuously monitored for drift, where effectiveness erodes as threats evolve, and for poisoning, where malicious inputs compromise the decision-making process. Without rigorous oversight, the SOC's strongest asset can become its most dangerous vulnerability.

## Explainability and the Accountability Gap

Equally pressing is explainability. AI-driven alerts often function as black boxes, leaving analysts with little insight into how conclusions were reached. The Trend Research Report, Security for AI Blueprint by Fernando Cardoso, Director of Product Management highlights the accountability gap this creates, especially during board presentations or regulatory audits, where opaque recommendations will not suffice.

The AI-CISO Handbook underscores that SOCs must evolve from reactive firefighting to AI-orchestrated command centers where scale, speed, and intelligence converge. The mandate for CISOs is clear: deploy automation for scale, enforce monitoring for integrity, and demand explainability for trust. Done right, the AI-augmented SOC becomes not just faster, but strategically more intelligent—turning cyber defense into a proactive, board-level function.

## People & Skills: The Human-AI Security Team

The convergence of AI and cybersecurity has created an unprecedented skills challenge—one that could undermine even the most sophisticated defenses if left unaddressed. According to Cisco's State of AI Security Report, while 72% of enterprises have adopted AI capabilities, only 13% of leaders believe their teams are fully prepared to use them effectively. This readiness gap underscores a critical need for professionals who can bridge traditional cybersecurity expertise with emerging competencies in adversarial machine learning, model governance, and data privacy.

## Training, Ethics, and Bias Awareness

The AI-CISO Handbook by Mohammad Alkhudari, Founder and CEO of Green Circle for Cybersecurity highlights that building an AI-augmented security team requires more than technical upskilling. Analysts must develop fluency in AI ethics, bias detection, and the societal implications of machine-driven decisions. Security professionals cannot treat algorithmic outputs as unquestionable truths—they must interrogate models, validate outcomes, and contextualize insights to ensure informed decision-making for business stakeholders. This dual literacy in technology and ethics is rapidly becoming a baseline expectation for modern SOC teams.

*"The biggest risk isn't only technical, it's contractual—SLAs must evolve with AI-specific obligations."*

**Satyavrat Mishra**
Head - Corporate IT & Group CISO, Godrej Industries Group

## Augmentation, Not Replacement

Contrary to fears of job displacement, the SANS Critical AI Security Guidelines emphasize that AI should enhance, not replace, human analysts. AI excels at scale—clustering anomalies, accelerating triage, and reducing dwell times—but only humans can apply contextual judgment, regulatory accountability, and creativity in adver-

sary simulation. The future SOC will be a hybrid environment where humans orchestrate AI outputs into strategic defense.

## Overcoming Cultural Resistance

Yet culture remains a stumbling block. Many security professionals still perceive AI as a threat rather than a tool. The Cisco report notes that organizations successful in adoption invest in training and change management, framing AI as a force multiplier rather than a competitor.

Technology will matter, but people will define success. Building a skilled, ethical, and adaptive human-AI security team will separate organizations that merely deploy AI from those that secure the future with it.

## Processes & Governance: Building Trustworthy AI Security

Cybersecurity leadership today extends far beyond defending networks—it is about embedding trust into every algorithm, model, and workflow. Governance has become the backbone of AI adoption, ensuring powerful technologies are deployed responsibly, ethically, and in compliance with evolving regulations.

The AI-CISO Handbook underscores that compliance monitoring and adaptive policy enforcement must move past static checklists. AI itself can be harnessed to continuously track adherence to privacy, security, and regulatory requirements, reducing blind spots and automating audits. This shift not only improves efficiency but also strengthens resilience against regulatory lapses.

Governance also requires new workflows centered on explainability and accountability. The NIST AI RMF Playbook highlights that effective governance spans the entire lifecycle—"mapping, measuring, and managing" risks from data acquisition through model deployment. Without explainability, black-box models erode trust and expose organizations to scrutiny from boards and regulators when decisions cannot be justified.

The SANS Critical AI Security Guidelines emphasize the importance of embedding access control, observability, and audit trails to ensure AI decisions are transparent and subject to challenge. Likewise, Singapore's Guidelines on Securing AI Systems advocate a secure-by-design approach, urging enterprises to integrate governance into planning, design, updates, and operations.

CISOs must evolve from security gatekeepers into enterprise-wide stewards of AI ethics. By driving explainability, accountability, and adaptive governance, they can ensure AI strengthens—rather than undermines—digital trust.

In the AI era, trustworthy security is no longer just about compliance; it is about building ethical, resilient systems that inspire confidence from the ground up.

## Compliance & Risk Management

AI has ushered in a new frontier of compliance—one where obligations are no longer secondary but central to enterprise resilience. The AI-CISO Handbook highlights how the EU's Artificial Intelligence Act establishes a risk-based classification system for AI applications, requiring organizations to embed compliance into design rather than bolt it on after deployment. In the U.S., the NIST AI RMF Playbook reinforces this approach, urging organizations to continuously "map, measure, and manage" AI risks, making compliance an operational discipline rather than a static requirement. India's Digital Personal Data Protection (DPDP) Act further raises the bar, requiring data minimization and privacy-by-design for AI systems that process sensitive personal data.

Yet traditional frameworks struggle with AI's dynamic nature. Singapore's Guidelines on Securing AI Systems caution that regulatory requirements often vary across contexts, making continuous risk assessment essential. The SANS Critical AI Security Guidelines go further, recommending organizations maintain AI Bills of Materials (AIBOMs), enforce access controls, and implement continuous monitoring to ensure the integrity of both training and inference stages.

Raimagia underscores the importance of treating regulation as an enabler: "When it comes to AI regulations like the EU's CEA and India's DPDPA, preparation is risk management. Mature organizations prioritize governance committees, clear ownership, and effective compliance tracking. They map sensitive data and AI workflows, embed privacy principles, conduct impact assessments, and ensure audits. Security by design and continuous training make compliance a business enabler, not a checkbox."

The thorniest challenge, however, remains accountability. When AI systems fail—whether through drift, poisoning, or bias—who is responsible? The AI-CISO Handbook argues CISOs must step into this vacuum, becoming enterprise-wide stewards of AI ethics and accountability. Ultimately, compliance is not about avoiding penalties—it is about building trust in an AI-driven world.

## Vendor & Third-Party Management

The AI supply chain has become one of the most critical fault lines in enterprise cybersecurity. According to Cisco's State of AI Security Report, nearly 60% of organizations source AI tools from open-source ecosystems, and 80% rely on them for at least a quarter of their AI solutions. This dependence has already been exploited—when attackers compromised Ray, an open-source AI framework, they gained access to GPU clusters and sensitive training data across multiple enterprises.

The opacity of AI models com-

pounds the problem. The SANS Critical AI Security Guidelines warn that relying on public models effectively places blind trust in unknown data scientists. Cisco researchers documented "Sleepy Pickle," a technique in which malicious code is embedded in model files and only executes post-deployment, evading traditional procurement checks.

Satyavrat Mishra, Head – Corporate IT & Group CISO, Godrej Industries Group, highlights this evolution in risk: "Third-party risk has always been about access, data sharing, and integration—but with AI, the exposure multiplies. Vendors often embed AI without transparency on training data, lineage, or output controls, creating blind spots. Sensitive data may be processed externally with unclear retention or usage rights. Open-source models and partner ecosystems further widen risk. The biggest challenge isn't only technical, it's contractual: unless SLAs and governance evolve with AI-specific obligations, compliance and reputational risks will follow."

As Ninad Varadkar, Sr. VP & Group CISO, Edelweiss Financial Services, also cautions: "With AI adoption, third-party risks now extend beyond breaches and compliance to privacy, bias, and resilience. Opaque vendor platforms raise data exfiltration risks, while Shadow AI bypasses governance, exposing IP and compliance gaps. Biased algorithms pose a threat to fairness in hiring, credit, and risk scoring. Over-reliance on external AI can lead to failures due to model drift. Without centralized oversight, organizations face compounded vulnerabilities in data security, ethics, and operational stability."

To counter these risks, the AI-CISO Handbook calls for AI-specific vendor vetting. Evaluation must extend beyond functionality to include model documentation, algorithmic transparency, encryption practices, and bias testing. Questions such as whether vendors retain customer data for retraining, or how they defend against prompt injection, must be part of due diligence.

Risk management cannot stop at contracting. Singapore's Guidelines on Securing AI Systems emphasize lifecycle oversight, mandating vulnerability disclosure processes, continuous monitoring, red-teaming, and maintaining an AI Bill of Materials (AIBOM).

Third-party AI should not be treated as a black box, but rather as a dynamic risk entity that demands constant scrutiny.

## Trust as the New Mandate for CISOs

Today's CISO is no longer just the guardian of firewalls and incident response. Their role has expanded into a cross-functional force that shapes trust across HR, finance, and customer operations. As the AI-CISO Handbook observes, modern CISOs are increasingly taking on the mantle of "Chief Trust Officers," ensuring that AI governance aligns with business goals and that every deployment strengthens—not undermines—enterprise resilience.

This evolution mirrors the deep interdependencies AI has introduced. The Cisco State of AI Security Report highlights that HR relies on AI for recruitment, finance for fraud detection, and customer operations for personalization—each carrying its own security and compliance risks. CISOs are tasked with orchestrating safeguards across these domains without slowing innovation, a delicate balancing act.

Even boardroom conversations have transformed. The NIST AI RMF Playbook emphasizes that CISOs now directly shape AI strategy, embedding explainability, accountability, and resilience into enterprise-wide policies. In this era, trust has become the true measure of leadership—not just technology.

As Raimagia puts it: "Will CISOs evolve into Chief Trust Officers? In some organizations, yes. Trust now spans security, privacy, ethics, and resilience, driven by regulations and board expectations. Yet CISOs' technical roots and the dual nature of their roles may limit the shift. Title aside, those who embrace a trust-first mindset will remain influential."

## The Roadmap for AI Readiness

The evolution into an AI-ready CISO is not a single leap but a staged transformation. In the short term (0–6 months), the priority is literacy and discovery. TheAI-CISO Handbook by Mohammad Alkhudari, Founder and CEO of Green Circle for Cybersecurity stresses that security leaders must quickly upskill on AI fundamentals, launch pilot projects, and map organizational AI usage to uncover both opportunities and hidden risks.

By the mid-term (6–18 months), the focus shifts to scaling and securing. The National Institute of Standards and Technology, (U.S Department of Commerce)I AI RMF Playbook calls for embedding governance into every layer of the AI lifecycle—mapping, measuring, and managing risks from data acquisition to deployment. CISOs

### Five AI Treats Ever CISO Must Know

**Adversarial ML** Tricking model with manipulated inputs.

**Data Poisoning** Corrupting training sets to skew outcomes.

**Model Drift** Accuracy erodes as real-word data shifts.

**Deepfakes** Synthetic media fuels fraud and deception.

**Guardrails, governance, and constant monitoring are not-negotiable**

must lead enterprise-wide staff training, enforce AI-specific policies, and introduce adversarial testing or red-teaming practices. Singapore's Guidelines on Securing AI Systems echo this imperative by urging enterprises to adopt "secure by design, secure by default" principles and establish vulnerability disclosure processes.

The long-term horizon (18–36 months) elevates the CISO from defender to strategic advisor. The Trend Research Report, Security for AI Blueprint by Fernando Cardoso, Director of Product Management, envisions CISOs as enterprise "trust architects," guiding board-level AI strategy and influencing industry standards. At this stage, their role extends beyond protecting systems to embedding trust as the cornerstone of enterprise AI adoption.

This phased roadmap ensures CISOs evolve from reactive defenders to indispensable leaders of AI-driven resilience.

## The CISO's Inflection Point

The paradox of AI in cybersecurity is permanent. While AI strengthens defenses with predictive detection, automated response, and deep threat visibility, it also equips adversaries with the same speed and scale. This duality reshapes the CISO's mandate—from managing technology to safeguarding trust. The path forward is not resisting AI, but mastering it through governance, talent development, and boardroom influence.

One reality stands out: AI won't replace the CISO—but CISOs who master AI will replace those who don't.

According to the industry experts, tomorrow's leaders will not be defined by chasing every AI use case, but by embedding responsibility into every deployment. Staying ahead of regulations, ensuring explainability, and keeping human judgment central will define success. Those who embrace continuous learning, invest in skills development, and engage transparently with stakeholders will distinguish themselves as the vanguards of AI-ready leadership.

## Strategic Recommendations

To sustain impact, CISOs must foster adaptability, align AI strategies with evolving business objectives, and embed ethical guardrails. Risk must be managed across the AI lifecycle—from sourcing datasets to deployment. Traditional best practices, such as access control, compliance, and monitoring, remain essential but now require approaches specifically tailored for AI.

## Final Thoughts

The CISO's role is no longer just about defending networks; it is about securing the intelligent enterprise. By blending cybersecurity fundamentals with AI fluency, today's CISOs can build resilient and responsible systems that inspire trust while unlocking the transformative power of AI.

# REGULATIONS WATCH

## GLOBAL AI & DATA GOVERNANCE SNAPSHOT

### EU AI ACT

World's first comprehensive AI law - classifies AI systems by risk, sets strick obligations and madates transparency

### U.S. NIST AI RMF

Voluntary frameworrk gulding on building trustworthy, safe, and accountabili AI Systems

### INDIA DPDP ACT

Focuses on personal data protection, consent-based processing, and stronger accountability for enterprises

CISOs must align strategies with evolving global AI and data regulations.

# Cyber Insurance: Trends, Guidance & Best Practices for CISOs

Cyber insurance is evolving rapidly; CISOs must align cybersecurity strategies with policies to mitigate risks and secure resilience.

By **Pradnya Manwar** | CISO, Thomas Cook

**AS CYBER** threats continue to evolve, cyber insurance has become a vital risk management tool for organizations. The world of cyber insurance is still in an evolving state, in short, insurance companies are still trying to figure this out. And that means there's a little to no chance that those within an organization responsible for cyber insurance and its impact on cybersecurity strategy and execution can clearly understand exactly how policy can and can't help you. This article explores the latest trends in cyber insurance, outlines best practices for effective policy management, and provides actionable advice for CISOs to align cybersecurity strategies with insurance requirements.

Cyber insurance has rapidly shifted from being an optional safeguard to a critical component of enterprise risk management. As threat landscapes expand, CISOs must adopt proactive strategies to align cybersecurity efforts with insurance coverage. Effective cyber insurance management requires understanding current trends, implementing best practices, and ensuring policies provide comprehensive protection.

## Trends in cyber insurance

1. **Increased premiums and stricter underwriting**

- Due to the surge in ransomware attacks and data breaches, insurers have become more selective, often demanding evidence of robust security controls before providing coverage.Insurers also evaluate

organizations' risk profiles by analyzing their external attack surface risk scores.
- Expect detailed assessments of endpoint security, identity management, backup strategies, and incident response capabilities.

### 2. Expanded coverage for emerging threats
- Modern policies are evolving to include coverage for:
  - Ransomware payment & recovery costs
  - Business email compromise (BEC) incidents
  - Supply chain attacks
- Coverage for legal, forensic, and public relations expenses is also gaining traction.

### 3. Integration with risk management platforms
- Insurers increasingly encourage or require integration with continuous monitoring tools that provide real-time security insights.
- This ensures policyholders maintain ongoing compliance with security best practices.

### 4. Focus on regulatory compliance
- Insurance providers are aligning policies to support compliance with frameworks like GDPR, NIS2, and SEC Cybersecurity Rules to mitigate legal risks.

### 5. Growing role of incident response services
- Cyber insurance now often includes access to dedicated incident response teams, crisis communication experts, and digital forensics specialists.

## Best practices for cyber insurance management

### 1. Conduct a cyber risk assessment
- Map your organization's assets, data flows, and critical systems to identify vulnerabilities.
- Quantify potential financial risks associated with data loss, downtime, and legal repercussions.

**Pradnya Manwar**
CISO, Thomas Cook

### 2. Align security controls with insurance requirements
- Implement core security measures such as:
  - Multi-factor authentication (MFA)
  - Endpoint detection & response (EDR)
  - Immutable backups
  - Patch management & vulnerability scanning

### 3. Maintain detailed documentation
- Maintain records of your organization's security policies, risk assessments, and incident response plans.
- Insurers often require documentation during underwriting and post-incident claims evaluation.

### 4. Define clear coverage scope
- Understand exclusions, sub-limits, and payout conditions.
- Ensure coverage extends to:
  - Data breaches
  - Third-party liabilities
  - Business interruption losses
  - Legal expenses

### 5. Establish an incident response plan
- Develop and test your organization's incident response plan to ensure a rapid and organized response during a cyber event.
- Designate clear roles and responsibilities for communication with insurers post-incident.

### 6. Involve legal and finance teams
- Collaborate with legal and finance teams to evaluate potential liabilities, understand regulatory requirements, and validate policy coverage.

### 7. Regularly review and update policies
- Cyber risk profiles change as organizations expand their digital footprint.
- Review policies annually to ensure coverage remains aligned with evolving risks and regulatory changes.

### 8. Conduct tabletop exercise
- Conducting annual tabletop exercises can help reduce cyber insurance costs.
- Insurers often inquire whether organizations perform these exercises.
- Tabletop exercises ensure that the security team, IT team, and senior management are well-prepared to handle cyberattack situations.

## Practical advice for CISOs

### 1. Engage with insurers early
- Establish proactive dialogue with insurers to understand their security expectations and improve your organization's risk profile before policy renewal.

### 2. Leverage security frameworks

gnized frameworks such as NIST, ISO 27001, or CIS Controls to demonstrate strong security practices. Insurers may offer reduced premiums for well-documented controls.

### 3. Invest in security awareness training

- Phishing and social engineering remain common attack vectors. Ensuring employees are well-trained can reduce risks and improve insurer confidence.
- Deepfake technology has emerged as a leading attack vector.
- Scammers are increasingly leveraging deepfakes to deceive individuals and organizations.

### 4. Clarify third-party coverage

- Ensure your policy addresses risks stemming from third-party vendors, cloud providers, and supply chain dependencies.

**"Cyber insurance is no longer optional—it's a strategic tool that must align with security practices to minimize financial exposure."**

### 5. Monitor and report on security improvements

- Regularly update insurers on improved security controls, which can lead to premium reductions or enhanced coverage.

### Conclusion

Effective cyber insurance management is no longer just about purchasing coverage — it requires strategic alignment between security practices, risk assessments, and incident response capabilities. By adopting proactive strategies, CISOs can secure comprehensive coverage, minimize financial exposure, and enhance their organization's resilience against cyber threats.

By staying informed about trends, implementing best practices, and fostering strong insurer relationships, CISOs can confidently navigate the complex landscape of cyber insurance in 2025 and beyond. ■

# Beyond Firewalls: Why tomorrow's CISOs must become behavioral detectives to stop insider threats

Dipesh Kaura urges CISOs to act as behavioral detectives, using AI, collaboration, and culture to stay ahead of insider threats.

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

**AS INSIDER-DRIVEN** risks account for over a third of global breaches, cybersecurity leaders face challenges beyond traditional defenses. In this exclusive interview with CISO Forum, Dipesh Kaura, Country Director – South Asia at Securonix, shares his vision for modern cybersecurity leadership. He highlights the role of AI-powered behavioral analytics, cross-functional collaboration, and ethical monitoring in addressing hybrid work risks. Kaura stresses that CISOs must evolve from cost centers to business enablers, driving resilience and credibility. With insider threats averaging $17 million per breach, he emphasizes the critical mindset shifts needed to safeguard organizations in today's complex threat landscape.

**CISO Forum: Insider-driven risks now make up more than a third of breaches globally. What should be the top three priorities for CISOs as they adapt to this reality in 2025?**
**DIPESH KAURA:** Top three priorities. First things first, you need to upscale. With the advent of Gen AI, CSOs must upgrade their skills and learn to utilize AI in the right context. The goal is to achieve meaningful business outcomes while also ensuring effective communication within teams and across the organization. Upskilling is no longer optional; it is essential for staying relevant and effective.

Second, CSOs must foster collaborative approaches that integrate with cross-functional teams such as HR, legal, and finance. Threats today spread horizontally, and with AI making both defense and attacks more sophisticated, collaboration becomes a critical necessity. Just as organizations adopt AI for protection, attackers also use AI to their advantage. Stronger integration within teams ensures faster response and minimizes blind spots.

Third, organizations need well-defined internal policies—clear dos and don'ts that address insider threats

**"Security is everybody's responsibility. Unless that culture comes in, no matter how many tools you deploy, they will fail."**

and establish security as a shared responsibility. While the CISO is ultimately accountable, acting as the captain who sets rules and policies, security cannot rest on a single desk. Unless every user takes ownership, even the best tools will fail. Negligence or ignorance at the user level creates vulnerabilities no system can fully close.

Therefore, the culture of security must be embedded across the organization. Cyber defense must evolve into a collective responsibility where everyone contributes to safeguarding the enterprise. Tools, policies, and leadership direction matter, but without a culture of shared accountability, defenses will always have gaps. These three priorities—upskilling, collaboration, and cultural responsibility—are the most critical to address.

**CISO Forum: How has the permanence of hybrid work changed the way CISOs view insider threats, especially with employees accessing sensitive systems across multiple devices and networks?**
**DIPESH KAURA:** It all comes down to the policy perspective. With hybrid work becoming the new normal, having the right policies in place—and implementing them effectively—has become the cornerstone of enterprise security. Policies define the rules of engagement, and without them, even the most advanced tools fail to deliver meaningful results.

To implement these policies, organizations often need additional layers of technology. Identity access management systems, privilege management tools, and continuous monitoring mechanisms are essential. Their success, however, relies on oversight. This is where the Security Operations Center (SOC)—whether described as a cyber response center, security monitoring center, or cyber defense center—plays a crucial role. The SOC must have full visibility into how data and security activities are being monitored across the enterprise.

When policies and tools work in tandem, monitoring multiple devices becomes easier. A fundamental practice is ensuring that all logins, regardless of origin, connect back to a secure, centralized source. If this source is protected with the right access controls, it becomes the most effective way to secure hybrid workforces. Policies may also block simultaneous logins from multiple devices by the same employee, while geotagging adds another safeguard by flagging inconsistent login locations.

Take a practical example: a senior resource in Mumbai relies on a laptop, phone, tablet, and home computer. All are internet-enabled and thus vulnerable. If a login attempt surfaces from Dubai or Hyderabad while the employee is active in Mumbai, monitoring tools like SOC, UEBA, or SOAR should instantly flag it as suspicious.

Policies can also be contextual. If an employee is on a video call, that geolocation can serve as validation, automatically suspending other login attempts. Properly configured, such measures prevent unauthorized access even in hybrid setups.

Ultimately, securing hybrid work requires more than acquiring tools. It demands a complete ecosystem of monitoring technologies, strong policies, and effective response

mechanisms. Regular "fire drills," much like physical safety checks, must confirm that alerts and defenses are functional. This blend of policy, practice, and preparedness ensures that when incidents occur, the right triggers activate at the right time to keep organizations safe.

**CISO Forum: Generative AI has boosted productivity but also created new vectors for data exposure. How should CISOs prepare for insider misuse or unintentional leaks through AI tools?**

**DIPESH KAURA:** The more exposure there is to the open internet, the greater the risk becomes. I've always been a strong advocate for fostering cyber maturity—both at the organizational and individual level—by implementing the right policies and checks.

Today, everyone knows that if you want anything, you go to ChatGPT. But regulating the use of ChatGPT is even more critical. The type of access granted and the keywords allowed or disallowed during that access can make a significant difference. Can organizations create a scenario where authentic, licensed access is provided, automatically discouraging the use of non-licensed applications that risk exposure and data theft? Such rules, methodologies, and policies must be established.

It also comes down to maturity and awareness. People need to know clearly what they should not be doing. By defining boundaries, you indirectly set what is permissible. Licensed access, authentic sources, and restricted usage for those handling sensitive data are essential. For individuals working with mission-critical information, all non-essential access should be suspended. One mistake—often unknowingly—can lead to serious breaches or data leaks.

Of course, security and convenience are opposites. More restrictions mean less comfort but higher security. Fewer restrictions mean greater access but also higher risk. Striking the right balance is key. Regulation— clearly defining what access is allowed while providing controlled leverage to the right tools—can minimize data exfiltration, maintain privacy, and prevent breaches. And compared to the cost of a violation, this investment is minimal.

**CISO Forum: From UEBA to AI-reinforced SIEM platforms, what practical AI capabilities should CISOs prioritize today to strengthen detection and response against insider activity?**

**DIPESH KAURA:** Insider threat is a reality, and it is growing bigger with every passing day. Earlier, such threats were more visible in the banking sector, but now they have spread across industries. With the rise of e-commerce and the growing sensitivity of organizational data, insider threat is a far bigger reality today than it was a decade or even five years ago.

In this environment, monitoring user behavior becomes critical. With the help of AI, it is possible to predict whether a behavior is rogue or heading in that direction. This is especially important during appraisals, when resignations are submitted, or when employees are serving notice periods.

For organizations with hundreds, thousands, or even 50,000 users, manual monitoring is impossible. Here, tools like UEBA—when integrated with AI and connected to SOC operations—become essential. UEBA can identify deviations when a user attempts unusual actions, such as accessing data they never touched before, downloading inappropriate files, or sending out unrelated information. These alerts allow administrators to intervene quickly: "This user is deviating from their regular behavior and may pose a risk."

AI-enhanced UEBA also leverages analytics and external data sources to predict potential outcomes, enabling organizations to review risky behavior before it escalates. While AI provides insights, control and decision-making remain with the organization.

**"Looking ahead at India's cybersecurity landscape over the next five years, several critical trends are emerging that business leaders should prepare for today."**

In today's hybrid environment where users operate from multiple devices and locations, UEBA combined with AI is indispensable. It enables accurate, predictive detection of insider threats, strengthening organizational defenses against evolving risks.

**CISO Forum: Employee Monitoring Raises Ethical and Cultural Questions. How can CISOs balance user privacy with the enterprise's need to detect malicious or negligent behaviour?**

**DIPESH KAURA:** It is the way the world changes. At one point in time, what was seen as spyware or a breach of privacy—questions like, "Why do you want to see what I am doing on my laptop?"—belonged to an era when employees entered the office, logged in with biometric attendance, and worked together on machines within corporate premises. Then came the BYOD phase, where "bring your own device" was introduced, though with limited access and controls.

The next major shift was hybrid work and work-from-home, which has now become a reality. This created new challenges. Organizations suffered losses due to misconduct—employees logging in but not working, or moonlighting with multiple laptops for differ-

ent companies at the same time.

This is why measuring mechanisms are necessary. Organizations must track user activity to safeguard information. With new laws, higher monitoring requirements, and more sophisticated attacks, behavior monitoring has become essential. It is no longer unethical, because work behavior and patterns have changed dramatically.

From a cyber defense perspective, the risks are greater. A UK case showed how attackers remotely took over power stations, shutting them down and plunging the country into darkness. Such incidents prove how abnormal machine behavior can be flagged through user entity detection. For employees at home, with weaker internet security, the risk increases, making immediate corrective action vital.

In today's environment, monitoring is not mistrust but assurance. Ethics and models have evolved—these technologies are now critical for protecting corporate assets and addressing misconduct.

**CISO Forum: The average insider breach now costs over $17 million. How should CISOs communicate the urgency of insider risk management to boards and CEOs in terms of business impact, not just security metrics?**

**DIPESH KAURA:** First things first, this requires a change of mindset. CSOs are now being viewed as a security pillar within the organization, and security expenditures are often seen as a cost center. However, today's scenario demands a shift in perspective. Just like a CTO or CIO, the CSO must also be recognized as a business enabler. The money or infrastructure deployed for cybersecurity should not be considered an expense but an investment in security.

Once this perspective changes, the way outcomes are evaluated also changes. When you talk about investment, you are talking about business value. While no organization can guarantee complete protection from cyberattacks, having the right tools, processes, and people in place ensures quick detection and response. This minimizes or even eliminates downtime, saving significant amounts of money—benefits that far outweigh the cost of security.

The challenge is that these benefits are not easily quantifiable on a daily or monthly basis. Yet, the day cybersecurity is viewed as an investment, it will be recognized as essential for keeping the business running. It safeguards organizational credibility, protects brand reputation, and even stabilizes stock prices—areas that can be severely damaged if a breach becomes public.

CISOs must now be seen not only as security leaders but as true business enablers. Encouragingly, this shift is already underway. Many organizations are transforming their security policies, methodologies, and spending, with some even beginning to measure ROI. This change will continue to drive the evolution of cybersecurity's role—and it has already begun.

**CISO Forum: As insider threats grow more complex, what new skills, collaborations, or leadership approaches will tomorrow's CISOs need to stay ahead of both external and internal risks?**

**DIPESH KAURA:** They need to gather behavioral intelligence about insider risks that are occurring. Organizations must introspect and understand what they have gone through, including the types of insider threats already encountered. When I say "check on the insider threat," it means evaluating the potential damage a user could cause and how such actions might create a damaging scenario for the organization. The first step is to understand behavioral aspects, leverage insider risk analytics, and assess how these threats could impact operations.

Second, they need to upskill in AI and develop fluency in automation. By mastering the subject and understanding how it works, leaders can design more effective protection strategies. Much also depends on how the organization manages its data—how much of it is stored in the cloud, how much is sensitive, whether distinctions between sensitive and non-sensitive data exist, and who has access to what.

Cross-functional collaboration is another crucial element. Ten years ago, boards and leadership required mentoring to even acknowledge that cybersecurity threats were real. Today, that shift has happened—leadership understands the importance of cybersecurity and accepts that no one is immune. Still, they need well-defined protection mechanisms. The same applies to AI. Leaders must be shown how AI works, how it can serve as a business enabler, and how it might also disrupt. Demonstrating the competitive landscape, with examples of how peers are adopting AI, will require mentoring at the leadership level.

I often say this in conferences: organizations must build resilience-oriented strategies. You cannot protect everything, and prevention alone will not suffice. Once preventive measures are in place, the focus must shift to recovery—how resiliently and quickly you can bounce back when something goes wrong. Accountability and recovery planning are just as important as prevention.

Finally, greater investment in building diverse teams is essential. The attack surface has expanded infinitely, with dozens of new technologies emerging. Smaller, cross-functional teams with diverse expertise can manage larger responsibilities, collaborate effectively, and build integrated defense mechanisms. This diversification helps organizations define roles clearly and address complex challenges with a holistic perspective. ■

# Criminals are weaponizing AI while companies rush to adopt it

Criminals are weaponizing AI with dark models and deepfakes, while enterprises adopt AI tools without strong safeguards.

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

**CHECK POINT** Research's first annual AI Security Report reveals a troubling reality: cybercriminals are embracing artificial intelligence just as eagerly as legitimate businesses, creating unprecedented security challenges for organizations worldwide.

## The dark side of AI innovation

Cybercriminals have moved beyond simply using mainstream AI tools like ChatGPT. They're now creating specialized "dark AI models" with names like WormGPT, FraudGPT, and GhostGPT—explicitly designed for malicious purposes without ethical safeguards. These tools help criminals generate convincing phishing emails, write malware code, and craft sophisticated social engineering attacks.

The underground market for AI-powered crime is booming. Advanced AI phone scam systems that can impersonate voices in real-time are selling for around $20,000, while simpler AI-generated fake identity services start at just $70. These tools allow criminals to operate at unprecedented scale and sophistication.

## Deepfakes become a real threat

The report documents alarming real-world cases in which AI-generated audio and video have led to substantial financial losses. In one incident, British engineering firm Arup lost £20 million after criminals used deepfake video technology during a live video call to impersonate senior executives and convince an employee to transfer funds.

Audio deepfakes are particularly concerning because they can be created with just ten minutes of voice samples, resulting in convincing impersonations. Italian scammers recently used this technology to impersonate the country's defense minister, targeting wealthy contacts for money transfers.

## Enterprise AI adoption creates new vulnerabilities

While criminals are embracing AI for attacks, businesses are rapidly adopting AI tools—often without implementing adequate security measures. The report found that AI services are used in 51% of enterprise networks every month, with 1 in every 80 prompts containing high-risk, sensitive data that could lead to leaks.

Popular business AI tools include ChatGPT (used in 37% of enterprise networks), Microsoft Copilot (27%), and writing assistants like Grammarly (25%). However, many employees may not realize they're sharing sensitive company information with these AI systems.

## Fighting fire with fire

The cybersecurity industry is responding by developing AI-powered defense systems. These tools can analyze millions of potential threats daily, identify suspicious patterns in domain registrations, and automatically extract attack signatures from security reports.

Advanced AI systems can now detect malicious code that traditional security tools often miss, helping researchers discover vulnerabilities faster than ever before.

## The bottom line

As AI becomes central to both cyber attacks and defense, organizations must balance innovation with security. The report emphasizes that while AI offers tremendous productivity benefits, companies need robust governance, monitoring, and data protection strategies to safely harness these powerful technologies without falling victim to AI-powered threats. ■

# Manufacturing under siege: Why industrial cybersecurity is finally getting the C-suite treatment?

Manufacturing embraces CISO-led cybersecurity, with mature strategies reducing incidents despite legacy systems and escalating global threats.

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

**THE MANUFACTURING** sector is facing a perfect storm of cyber threats. Still, Fortinet's latest 2025 State of Operational Technology and Cybersecurity Report suggests companies are finally taking operational technology (OT) security seriously—and it's paying off.

## Leadership takes control

A dramatic shift is happening in corporate boardrooms. More than half of organizations (52%) now place OT cybersecurity directly under their Chief Information Security Officer, a massive jump from just 16% in 2022. This trend shows no signs of slowing, with 80% of companies planning to consolidate OT security under the CISO within the following year.

This executive-level ownership signals that industrial cybersecurity has evolved from a technical afterthought to a board-level priority. The change comes as manufacturing remains the most targeted sector, representing 17% of all cyberattacks in 2024.

## Progress against the odds

Despite growing threats, cybersecurity investments are delivering results, shows a study of 550 OT professionals. Companies with zero intrusions jumped from 6% in 2022 to 52% in 2025. Notably, 65% of organizations with high security maturity reported no incidents, versus 46% of less mature firms, even as ransomware and nation-state actors increasingly target manufacturers.

## The maturity advantage

The report reveals a clear correlation between security maturity and a reduction in incidents. Nearly half of organizations (49%) now rate their cybersecurity processes at Level 4—the highest maturity level, where security measures are continuously improved through feedback and threat intelligence.

However, solution maturity lags behind process improvements. Most organizations remain at Level 2 maturity for security solutions, having established basic visibility and segmentation but not yet implemented advanced features such as predictive behavior analysis or automation.

## Aging infrastructure challenges

A critical vulnerability persists across manufacturing floors as most industrial control systems are over six years old, designed for isolation, not today's connected networks. Organizations are responding—22% of systems are now under five years old. For legacy equipment that can't be replaced, companies rely on virtual patching and compensating controls to maintain security.

**"Cybersecurity in manufacturing is no longer optional—it's a strategic imperative driving resilience and safeguarding critical operations."**

## Best practices that work

The most successful organizations are adopting key strategies for OT security. Network segmentation remains the top priority, creating defensive zones between operational and corporate systems. Enhanced visibility helps protect vulnerable assets that cannot be easily patched. Mature organizations are also consolidating vendors to reduce complexity—78% now rely on one to four OT device vendors, streamlining management and improving oversight. This platform approach enables centralized threat intelligence and automated responses across systems. The evidence is clear: as OT threats intensify, only those treating cybersecurity as a business imperative—not just an IT issue—are effectively defending critical operations. ■

# The Invisible Risk of Shadow AI

**ARTIFICIAL INTELLIGENCE** is redefining enterprise operations, enabling faster insights, automation, and enhanced decision-making. Yet, as organizations embrace AI, a silent risk is growing: Shadow AI, the unsanctioned use of AI tools by employees without IT approval. Often well-intentioned, this behavior is driven by productivity pressures, but it exposes organizations to significant cybersecurity threats.

During a recent visit to Pune, a leading CISO shared his frustration: "I am not even sure who is responsible for AI in my organization—me, the function head, or the employees themselves? This can introduce cybersecurity risks that we may not be prepared for." His sentiment highlights a broader global concern. IBM's 2025 Cost of a Data Breach Report found that Shadow AI contributed to 20% of data breaches, increasing the average breach cost by $670,000.

What makes Shadow AI so challenging is its decentralized and rapid adoption. Employees can quickly access cloud-based AI tools, often bypassing IT controls entirely. Generative AI, chatbots, and automation platforms while valuable can inadvertently leak sensitive data, expose intellectual property, or create compliance blind spots. Traditional top-down security controls struggle to keep pace.

Proactive governance is key to managing this risk. Organizations must define clear ownership and accountability for AI use, implement monitoring to track unsanctioned activity, and educate employees about the dangers of using unauthorized AI tools. Security policies should balance innovation with oversight, enabling employees to leverage AI safely rather than circumventing controls.

Shadow AI is a hidden but growing threat. CISOs must act now to bring AI under governance, mitigate exposure, and integrate oversight into broader cybersecurity strategies. By doing so, organizations can harness AI's benefits while protecting sensitive data, ensuring compliance, and avoiding costly breaches.

The message is clear: innovation without oversight can become a liability. Shadow AI may be invisible today, but without decisive action, it could quickly escalate into tomorrow's major security incident.■

**"The real risk with AI isn't just the technology—it's the uncertainty of who owns it inside the enterprise. Without clear accountability, Shadow AI becomes a cybersecurity time bomb."**

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

CISOFORUM

Security For Growth And Governance

# Where CISOs Connect, Innovation Ignites

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

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

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

**Expand your network with the brightest minds in cybersecurity.**

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

**Follow us on @CSO Forum**

Scan the QR code to follow

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

17th Annual Conference

# CISO FORUM

India's Leading Cybersecurity Summit

## The Strategic CISO – Leading in the Age of AI

**21–22 November 2025**

**The Dukes Retreat, Khandala, Maharashtra**

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 serene beauty of Alibaug.

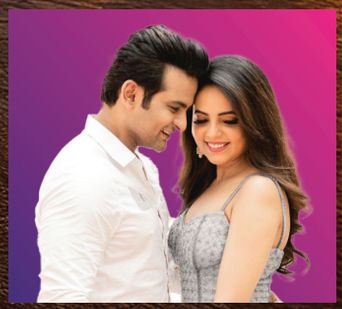
**Keynotes | Panel Discussions | Ideas Café**
**Roundtables | Case-Study Workshops | Cook-a-thon**
**NextCISO Awards**

## 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 PARTNER securiti | SILVER PARTNER CLAROTY | EXHIBIT PARTNER Barracuda Your business, secured. | 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/**