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

NOVEMBER-DECEMBER 2025
SUPPLEMENT OF CIO&LEADER

CISOFORUM

Security For Growth And Governance

DPDP 2025 Playbook

What You Can't Afford to Ignore

SPECIAL

Ask Me Anything on DPDP Rules

Khushboo Jain
Managing Partner,
Arklegal

Satyanandan Atyam
Chief Risk Officer,
TATA AIG General Insurance

CIO&LEADER studiotalks

CIO&LEADER STUDIOTALKS—
WHERE TECHNOLOGY MEETS THE SPOTLIGHT!

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

WHY JOIN STUDIOTALKS?

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

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

Be featured among India's top technology leaders.

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

SECURE YOUR SPOT NOW!

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

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

Follow us: @CIOandLeader

The AI dilemma: Clear principles, cloudy implementation

India's AI Governance Guidelines from MeitY represent a watershed moment for cybersecurity leaders—but perhaps not as the government intended. While the framework's seven principles look progressive, CISOs face a troubling paradox: comprehensive obligations with minimal operational clarity.

Consider the 6-hour incident reporting requirement, mirroring CERT-In's aggressive stance. What will constitute a reportable AI incident? System errors? Bias detection? Adversarial attacks? Will mandatory transparency expose vulnerabilities to threat actors? How do we secure AI watermarking infrastructure against nation-state manipulation?

The "voluntary framework" label masks deeper concerns. Guidelines explicitly state that baseline measures may become mandatory, and sectoral regulators must enforce existing laws. So, you are implementing voluntary compliance today to avoid mandatory penalties tomorrow—without knowing which measures will become binding.

Security implications are also profound. CISOs must defend against adversarial attacks, data poisoning, and model manipulation while building incident response capabilities for novel threats that are emerging. The guidelines demand AI-specific security controls, yet provide no approved tool lists, benchmarks, or safe harbor provisions.

Most organizations will also lack the assumed resources. AI training costs alone could consume entire security budgets, while the cybersecurity talent pool remains critically constrained. The whole-of-government coordination sounds impressive until you are navigating conflicting guidance from MeitY, CERT-In, your sectoral regulator, and potentially NCIIPC. Each will want reports, audits, and compliance on undefined timelines with unspecified consequences.

The uncomfortable reality is that the guidelines provide principles; CISOs must provide professional judgment. This is not regulatory failure—it is the nature of emerging technology governance.

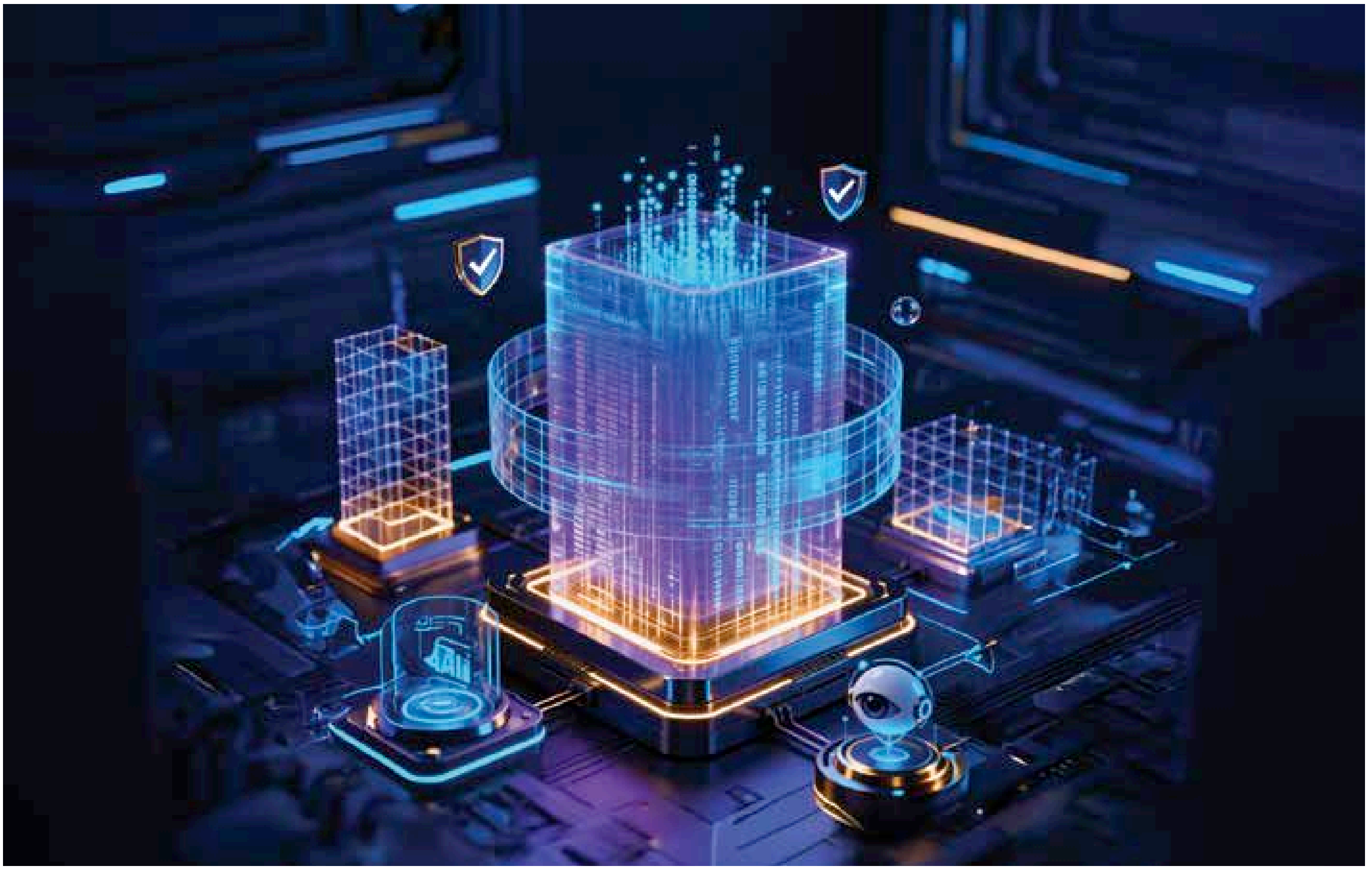
Until implementation details materialize, we will be compelled to build AI compliance programs on shifting sand—exposed to liability for frameworks that are still crystallizing. So, it would be wise to use this voluntary period to build AI inventories, establish risk frameworks, create incident protocols, document everything, and engage regulators proactively.

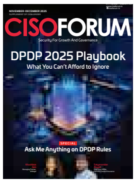
India's AI future will be built by CISOs who act decisively despite uncertainty, not those paralyzed by it. ■

"The guidelines provide principles; CISOs must provide professional judgment."

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

CONTENTS NOVEMBER DECEMBER 2025




CISOFORUM
DPDP 2025 Playbook
What You Can't Afford to Ignore
Ask Me Anything on DPDP Rules

Cover Design by:
Shokeen Saifi

Please Recycle This Magazine And Remove Inserts Before Recycling

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.

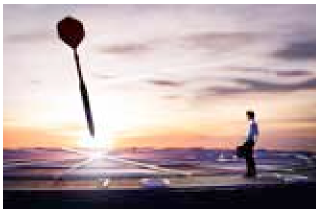
NEWS & VIEWS

EVENT REPORT

OPINION

INTERVIEW

INSIGHTS



CISOFORUM
Security For Growth And Governance
www.cisoforum.in

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

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

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

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

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

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

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

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

For editorial queries write to:
editor@cioandleader.com

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

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

Editor: **Vikas Gupta**

Sumeet Mishra appointed as CISO at Suryoday Small Finance Bank

Sumeet Mishra has officially become the Chief Information Security Officer at Suryoday Small Finance Bank Ltd after nearly six years in key leadership roles. With strong expertise in data privacy, compliance, and cybersecurity operations, he has strengthened the bank's security posture. Previously Deputy CISO, he led risk management, secure SDLC, vendor governance, ISO 27001 readiness, and brings 15+ years of deep cybersecurity experience.

Abhilash Verma appointed as Senior VP & GM at Citrix

Abhilash Verma has taken on the role of Senior Vice President and General Manager at Citrix, leading its global Security Business Unit and Citrix–Google partnership initiatives. With over two decades at Citrix—including steering the NetScaler business and serving as Chief Product Officer—he has shaped major security products. Earlier, he contributed to cybersecurity roles at Mahindra SSG and Network Security Solutions.

Surendra Nemani appointed as VP & Head of Cybersecurity at Hexaware Technologies

Surendra Nemani has become VP & Head of Cybersecurity at Hexaware Technologies, leading cybersecurity strategy and governance for Hexaware and its group companies. With 17 years of leadership experience across Flipkart, Cleartrip, and Infosys, he has driven enterprise security architecture, cyber defense, and GRC programs. His deep expertise positions him to strengthen Hexaware's security posture as it advances its cloud-first, AI-led growth.

Subhajit Deb appointed as Global Head – Cyber Engineering and Technology Operations at Cargill

Subhajit Deb has become Global Head – Cyber Engineering and Technology Operations at Cargill, leading global cybersecurity engineering and technology operations across network, endpoint, cloud, data, and identity security. With 20+ years of cybersecurity leadership across Envoy Global, Dhani, Dr. Reddy's, Max Life, SMBC, and Bank of America, he brings strong expertise in innovation, resilience, and talent development to strengthen Cargill's cybersecurity ecosystem.

CyberArk tackles machine identity security crisis with new automated solutions

CyberArk introduces automated tools to secure rapidly growing machine identities as organizations face outages, breaches, and AI-driven credential risks.

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

CYBERARK HAS launched enhanced discovery and management tools to help companies secure machine identities—digital credentials used by software, applications, and automated systems. As businesses adopt more AI and cloud technologies, these machine identities now outnumber human users by 82 to 1, creating massive security challenges.

Growing Security Threats

The explosion of machine identities has led to serious consequences. According to CyberArk's research, 72% of security leaders have experienced certificate-related system outages, while 50% reported security breaches caused by compromised machine credentials. Traditional manual tracking methods can no longer handle the scale of today's digital environments.

"Organizations are struggling with shorter certificate lifespans, AI agents, and complex software supply chains."

Comprehensive Security Overhaul

"Organizations are struggling with shorter certificate lifespans, AI agents, and complex software supply chains," said Kurt Sand, GM of Machine Identity Security at CyberArk. The new tools provide automated visibility and control to manage these challenges efficiently.

The enhanced portfolio includes three major updates. CyberArk Secrets Hub now offers discovery capabilities for HashiCorp Vault systems and a centralized dashboard for identifying high-risk security areas. Certificate Manager introduces a specialized dashboard to prepare for upcoming TLS certificate lifespan reductions—dropping from 398 days currently to just 47 days by 2029. SSH Manager adds real-time authorization tracking to combat unmanaged access.

Strategic Timing

These announcements come one year after CyberArk acquired Venafi, signaling the company's commitment to building comprehensive machine identity security solutions. The enhancements aim to help security teams automatically find, understand, and protect all machine identities across their enterprise—from certificates and encryption keys to secrets and workloads—reducing risk while simplifying compliance requirements at scale. ■

The Human factor in a data-driven storm

Human behavior, data sprawl, and AI are converging to redefine enterprise data security risks and resilience.

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

THE PROOFPOINT 2025 Data Security Landscape Report reveals a troubling paradox: while artificial intelligence transforms organizational operations, it amplifies long-standing vulnerabilities tied to human behavior and data sprawl. Drawing insights from 1,000 security professionals across 10 countries, the report shows AI, cloud expansion, and insider risks colliding to create unprecedented challenges in protecting enterprise data.

People Still at the Center of Breaches

Despite rapid adoption of automation and AI, human error remains the leading cause of data loss. About 85% of organizations faced at least one incident last year, with careless employees or contractors responsible for 58%. Proofpoint data shows just 1% of users account for 76% of data loss, highlighting the need for behavior-aware, adaptive security.

“Human behavior remains the weakest link in data security, even as AI and automation reshape enterprise defenses.”

Data Growth and Sprawl Escalate Risks

Enterprise data volumes are exploding, with 29% of companies recording growth above 30% last year. Among large organizations, over 40% now manage more than a petabyte of data. Meanwhile, 27% of cloud data remains unused, increasing costs and vulnerabilities, as cloud and SaaS sprawl heighten governance and compliance risks.

AI: The Double-Edged Sword

AI tools present both risk and remedy. Two in five organizations fear GenAI data leaks, while 32% worry about unsupervised AI agents. Yet many already use AI for data classification and anomaly detection, making secure design, visibility, and strong governance essential to prevent misuse.

Fragmentation and Fatigue Among Security Teams

Security operations are buckling under complexity. 64% of companies juggle six or more security vendors, and a fifth take up to four weeks to resolve incidents. With 35% citing a lack of skilled personnel, teams are stretched thin, managing endless alerts without unified oversight.

A Unified, AI-Driven Future

Proofpoint concludes the path forward lies in unified, AI-powered data security platforms integrating detection, response, and insider risk management, combining human-centric insights with machine intelligence to secure data at scale. ■

Cisco simplifies security for MSPs with unified cloud control platform

Cisco's new Security Cloud Control upgrade lets MSPs manage multiple customers seamlessly, simplifying operations and boosting efficiency.

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

CISCO HAS unveiled a significant advancement in its Security Cloud Control platform, introducing foundational multi-customer management capabilities explicitly designed for Managed Service Providers (MSPs). The upgrade enables MSPs to manage multiple clients from a single interface—streamlining operations, reducing costs, and accelerating the delivery of next-generation security services across hybrid environments.

The new capabilities are built to help MSPs navigate today's AI-driven, hyper-distributed threat landscape while boosting profitability and efficiency.

"Security Cloud Control leverages AIOps and AgenticOps to manage Cisco's Hybrid Mesh Firewall and Secure Access solutions."

As Jeetu Patel, Cisco's President and Chief Product Officer, noted, "The new multi-customer management capabilities in Security Cloud Control, coupled with our Hybrid Mesh Firewall, are designed to eliminate operational friction and empower partners to deliver superior security outcomes."

Unified Platform, Broader Control

Security Cloud Control is a unified, AI-powered management console using AIOps and AgenticOps to manage Cisco's Hybrid Mesh Firewall and Secure Access solutions. It enables MSPs to apply consistent security policies across data centers, clouds, and edge networks, with AI accelerating threat detection and response. The Hybrid Mesh Firewall offers zero-trust segmentation and AI-driven protection, while new enhancements support faster onboarding, automated provisioning, and granular, role-based access control.

Driving Efficiency and Growth

Cisco's new features target three critical outcomes:

Faster time-to-market: Simplified customer onboarding and multi-product service bundling.

Lower operational costs: Unified dashboards reduce manual effort and human error.

Easier upsell opportunities: A single platform enables consistent, repeatable service expansion.

Cisco's Secure Firewall 200 and 6100 Series deliver high-performance protection with 99.5%–100% threat detection. Industry leaders welcomed its potential to transform managed security operations. Multi-customer management arrives by February 2026, simplifying security delivery. ■

Asia-Pacific cybersecurity: From risk to resilience

Asia-Pacific enterprises face escalating AI-driven cyber threats, yet preparedness and cybersecurity investment remain critically low.

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

THE IDC InfoBrief, sponsored by Fortinet, shows Asia-Pacific enterprises racing to harness AI while confronting rising AI-driven cyberattacks. Despite heightened awareness, cybersecurity investment and readiness remain dangerously low, signaling urgent gaps in resilience across the region's rapidly evolving digital landscape.

AI: The Double-Edged Sword

AI is reshaping both sides of the cybersecurity battlefield. Sixty-one percent of organizations have faced AI-powered threats, with 27% saying they outpace detection, yet only 15% of IT budgets support cybersecurity. IDC warns that AI empowers defenders but equally strengthens attackers through deepfakes, intelligent malware, and automated exploitation tools.

A Region Under Siege

Cyberattacks are increasing across every front, with software supply chain attacks, ransomware, and phishing rising sharply. AI-enhanced threats like credential hijacking, deepfake scams, and data poisoning are testing defenses. The core message remains: "Complexity is the enemy of security," as organizations struggle with too many tools and insufficient integration.

> "AI is accelerating both defense and attack—resilience now depends on simplicity, automation, and uncompromising security leadership."

People and Process: The Weakest Links

The human layer remains fragile. Only 15.6% of organizations have a dedicated CISO, while 63% combine cybersecurity with broader IT functions. Skills shortages, tool sprawl, and burnout are undermining resilience. IDC notes that automation and platformization—using fewer, more innovative tools—are essential to counter both human error and talent scarcity.

From Fragmentation to Platform Resilience

Nearly 97% of surveyed firms are consolidating or evaluating security–networking convergence to achieve faster response times, better visibility, and a stronger security posture. IDC highlights identity security, zero trust, and cloud-native protection as key priorities. AI adoption is accelerating, with over 90% using it for predictive modeling and automated response, though trust gaps persist around autonomous AI decision-making.

The Road Ahead

IDC's guidance urges zero trust, aggressive automation, and responsible AI, evolving security into a platform-driven business enabler and transforming cybersecurity from reactive defense to a strategic resilience pillar built on intelligence, collaboration, and trust. ■

DPDP 2025 Playbook

What You Can’t Afford to Ignore

As the DPDP Act reshapes enterprise data obligations, CISOs have a pivotal opportunity to convert compliance demands into stronger trust and business advantage.

By **CSO Forum** | editor@csoforum.com

THE DIGITAL Personal Data Protection (DPDP) Act is now operational, setting a comprehensive framework for how digital personal data must be collected, processed, and safeguarded in India. While some provisions are already in effect, the bulk of requirements will come into force by May 2027. The law balances the rights of individuals—Data Principals—with the responsibilities of organizations—Data Fiduciaries—fundamentally reshaping the enterprise data landscape.

In a data-driven business environment, many organizations have historically underinvested in governance and control. The phased timeline offers some breathing room, but the scale of transformation required across IT, HR, legal, marketing, product, and analytics is significant. CISOs and CIOs now face pressing questions: where personal data resides, how consent flows are redesigned, how to map data to lawful purposes, rethink access models, manage legacy datasets, strengthen cloud environments, and meet stringent breach-notification mandates.

This month's cover story decodes the DPDP for CISOs and highlights the critical steps to build fully compliant, data-resilient enterprises.

The Consent Shock

One of the foremost challenges confronting CISOs and IT leaders today is the new consent framework under the DPDP Rules, which places explicit consent at the core of lawful data processing. The Rules introduce a stricter, verifiable, purpose-linked consent regime that demands redesigning systems, tightening governance, and giving users meaningful control over their data.

> *"At the heart of compliance is consent: without it, all security mechanisms and safeguards are meaningless."*

*-**Ninad Raje,** Group Chief Information Officer, Times Group*

Phased Implementation Timeline

1. Immediate Effect – Nov 2025
India's Data Protection Board is established. Key provisions on breach notifications and initial regulatory powers take effect, making breaches reportable events.

2. 12-Month Phase – Nov 2026
Consent Manager registration, Data Protection Officer disclosures, and routine compliance obligations begin. Organizations must operationalize consent systems, update capture flows, and re-permission legacy data.

3. 18-Month Phase – May 2027
Full enforcement for all Data Fiduciaries, especially Significant Data Fiduciaries. Continuous compliance is required, legacy data without consent is a liability, cross-border transfers must meet safeguards, and incidents face immediate investigation.

Key DPDP Penalties and Enforcement Triggers

Violation / non-compliance type	Maximum penalty / fine
Failure to implement reasonable security safeguards (resulting in a data breach)	Up to ₹ 250 crore
Failure to notify the board and affected data principals of a personal data breach	Up to ₹ 200 crore
Non-fulfilment of obligations when processing children's personal data	Up to ₹ 200 crore
Non-compliance by a designated "Significant Data Fiduciary" (failure to meet heightened obligations for large/sensitive data processors)	Up to ₹ 150 crore
Violation of duties of data principals (e.g. misuse of data-rights or false complaints)	Up to ₹ 10,000
Breach of any other provision of the Act or rules (not otherwise categorized)	Up to ₹ 50 crore
Failure to honour a voluntary undertaking accepted by the Data Protection Board (DPB)	Penalty up to the quantum applicable for the underlying breach (i.e. same as relevant violation)

This shift fundamentally changes how Indian businesses interact with personal information. Organizations long accustomed to broad or implied data collection must now adopt stringent operational and technological measures to ensure compliance.

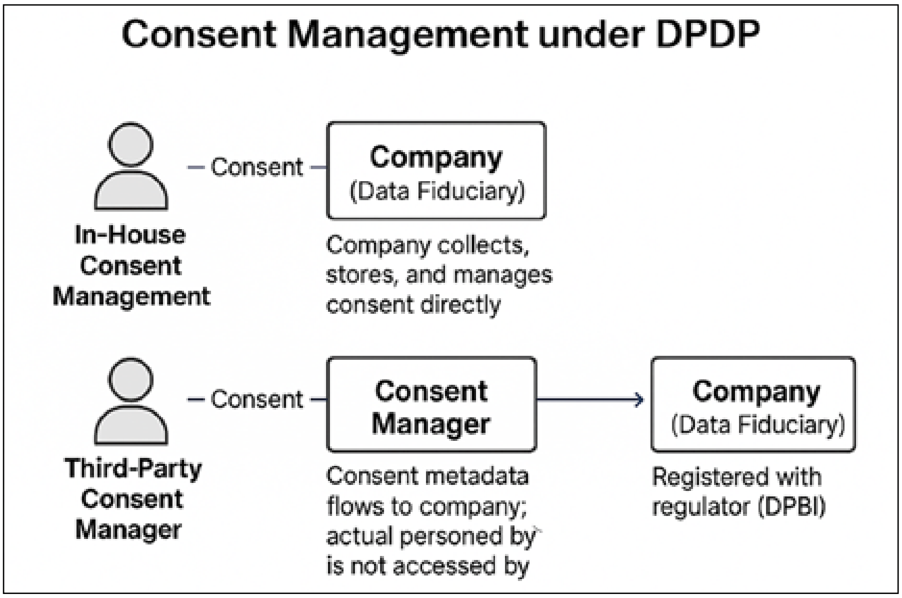
Under the DPDP Act, consent is the mandatory legal basis for handling personal data. The Rules require that consent be:

- **Free, informed, and unambiguous:** Individuals (Data Principals) must clearly understand and affirmatively agree to data usage.
- **Specific:** Consent cannot be generic; it must directly correspond to well-defined purposes communicated by the Data Fiduciary.
- **Explicit:** Required for all personal data, with heightened diligence for sensitive categories such as financial, health, biometric, or sexual-orientation data.

Organizations must clearly communicate the data categories collected, retention periods, and any third-party sharing. Crucially, consent is revocable at any time, which means enterprises must implement robust, user-friendly mechanisms for withdrawal.

While this framework may initially feel like a significant operational burden, it also presents a strategic opportunity for CISOs and enterprises to build trust, transparency, and customer loyalty, capabilities increasingly linked to competitive differentiation. By implementing strong consent management practices, enterprises can demonstrate respect for user autonomy, clearly articulate data usage, and provide seamless mechanisms for access, correction, and withdrawal.

For CISOs, this approach not only mitigates regulatory and financial exposure but also strengthens brand reputation, improves data quality for analytics and AI, and enhances operational efficiency by ensuring data collection aligns strictly with business objectives.



Transforming Consent Compliance into a Strategic Asset: CISO Action Agenda

By approaching DPDP compliance as a structured capability rather than a regulatory burden, CISOs can convert legal obligations into strategic assets, enhancing operational efficiency, strengthening customer trust, and creating long-term business value.

1. SYSTEM REDESIGN

- **Action:** Redesign apps, websites, and forms to capture granular, verifiable consent.
- **Impact:** Ensures compliance while generating clean, structured datasets that improve analytics, AI initiatives, and personalized customer experiences.

2. RETROACTIVE MANAGEMENT

- **Action:** Re-permission existing datasets to align with DPDP standards.
- **Impact:** Validates and refreshes data, reduces redundancy, and enhances data quality, supporting marketing, product innovation, and strategic decision-making.

3. RECORD-KEEPING & TRANSPARENCY

- **Action:** Maintain comprehensive, timestamped consent logs and processing records.
- **Impact:** Builds accountability and positions the organization as a trusted custodian of customer data, strengthening brand reputation and stakeholder confidence.

4. HIGH-STAKES & CROSS-BORDER SAFEGUARDS

- **Action:** Implement contractual and technical measures to manage penalties and regulate cross-border data transfers.
- **Impact:** Mitigates regulatory and reputational risks while building confidence with international partners and customers.

Purpose matters: keeping data use aligned with consent

Under India's DPDP Rules, purpose limitation is one of the core compliance pillars. It means an enterprise may collect, process, store, and share personal data only for a specific purpose clearly communicated to the individual at the time of collection. If a team later wants to reuse that data for a different purpose, for instance, marketing, analyt-

Key Compliance Actions for Data Fiduciaries Under the DPDP Act

Compliance Stage	Required Actions	Impact Area
Assessment & Planning	Conduct data mapping exercises; identify all data collection points; define clear purposes for processing data.	Legal, IT, Operations
System Redesign	Implement consent management platforms (CMPs); redesign user interfaces (websites/apps) for explicit opt-ins.	IT, Product Development
Policy Updates	Revise internal privacy policies and external notices to be transparent and DPDP-compliant.	Legal, Compliance
Training & Awareness	Train all staff (HR, Marketing, Analytics) on new data handling protocols and user rights.	HR, Compliance
Vendor Management	Review and update vendor contracts with data protection clauses for third-party sharing/ processing.	Procurement, Legal
Incident Response	Establish a clear breach notification protocol for reporting data incidents to the Data Protection Board of India (DPBI).	IT, Legal
Ongoing Monitoring	Conduct regular audits of consent records and data flows to ensure continuous compliance.	Audit, Compliance

ics, AI modelling, product evaluation, fresh consent is mandatory.

Purpose limitation goes hand-in-hand with data minimisation, which requires that organizations:

- Collect the minimum data needed
- Keep it only for the required duration
- Avoid storing unnecessary or unrelated attributes

For CISOs, the challenge is not understanding the rule; it is enforcing it across a complex organisation with multiple applications, data flows, teams, and vendors. The biggest risk is function creep, where data quietly migrates into new use cases—typically analytics, marketing automation, CRM enrichment, and AI training.

KEY RESPONSIBILITIES

- Translate "purpose limitation" into technical and procedural controls.
- Prevent silent "function creep" where teams start reusing data for new purposes without governance.

Collect less, retain only what's needed

Data minimisation and retention is another key requirement under DPDP. Organizations must ensure that they collect only the personal data necessary to achieve a clearly defined purpose and avoid gathering excessive or unrelated information. Personal data should be retained only as long as required for the stated purpose or to meet legal obligations.

Once the data is no longer needed, it must be securely deleted or anonymized. This principle not only reduces the organization's exposure to privacy risks and regulatory penalties but also limits the operational and security overhead of managing large volumes of sensitive data across enterprise systems.

For CISOs, the practical challenge lies in enforcing minimisation and retention policies consistently across multiple systems, applications, business units, and cloud platforms, while ensuring alignment with business objectives and legal mandates. Without robust controls, organizations risk data sprawl, increased breach liability, and non-compliance.

By integrating data minimisation and retention into enterprise architecture and workflows, CISOs can significantly reduce risk, simplify compliance, and demonstrate accountability under the DPDP Act.

> *"Security today isn't just protection—it's visibility, control, and making every investment count."*

-Dr. Sriranga Narasimha Gandhi,
Head-Infosec, Jio Platforms

CISO Action Points

CISO Action Area	Key Action Points
Data Inventory & Classification	Identify all personal data collected across the organization, classify it by sensitivity, and map each dataset to its business purpose.
Limit Collection at Source	Redesign forms, APIs, and data ingestion workflows to capture only required attributes. Avoid free-text fields or optional data that are not critical.
Retention Policy Implementation	Define retention schedules per data type and purpose; automate data deletion or anonymization once retention periods expire.
Monitoring & Auditing	Conduct periodic audits to ensure compliance with minimisation and retention policies; detect and remediate unnecessary accumulation of data.
Cross-Functional Alignment	Collaborate with legal, product, marketing, and analytics teams to ensure minimisation policies align with operational and regulatory requirements.
Vendor & Cloud Oversight	Ensure third-party processors and cloud providers comply with minimisation and retention rules; include contractual obligations and verification steps.
Employee Awareness & Training	Educate teams on why only necessary data should be collected and how retention policies affect day-to-day operations.
Access Mapping & Role Definition	Define access rights by specific use-case rather than broad roles; map every dataset to its approved purpose.
System & Application Controls	Implement purpose-based permissions in applications, databases, and analytics platforms; remove generic access wherever possible.
Policy Enforcement	Develop and enforce policies that prevent teams from repurposing data without documented consent.
Monitoring & Auditing	Track all data access, generate alerts for unauthorized or unusual usage, and conduct periodic reviews of access assignments.
Cross-Functional Coordination	Work with HR, product, marketing, analytics, and IT teams to ensure access rules are operationally feasible and compliant.
Vendor & Cloud Oversight	Ensure third-party processors follow purpose-based access rules; include contractual obligations and audit rights.
Employee Awareness & Training	Train staff on access limitations, the risks of function creep, and the importance of adhering strictly to declared purposes.

> *"Data sovereignty is no longer a choice—it has become a core regulatory expectation."*

-Vamsi Krishna Ithamraju,
CTO, Axis Mutual Fund

Grant access only for what matters

Under DPDP, personal data access must strictly align with its declared purpose. Generic role-based permissions are no longer sufficient, every system, application, and team member must have access rights mapped to a specific, approved use-case. This prevents inadvertent or unauthorized use of personal data, reducing compliance risk and function creep, particularly in large organizations with multiple departments, applications, and analytics workflows. For CISOs, the challenge lies in translating this principle into enforceable technical controls and operational processes across the enterprise.

Monitoring, Logging, and Accountability

Organizations must maintain comprehensive logs tracking who accessed what data, for which purpose, and when. Regular audits and automated alerts for unusual access patterns are required to ensure accountability. These measures enable demonstrable compliance and support investigations in the event of a data breach.

Third-Party & Vendor Oversight

The Act mandates that any third-party processors or vendors handling personal data operate strictly within the scope of defined purposes. Contracts must clearly delineate responsibilities, retention periods, deletion obligations,

CISO monitoring & accountability playbook under DPDP rules

Focus area	Objective	Key CISO actions	Tools / Implementation Notes
Comprehensive Logging	Capture who accessed which personal data, for what purpose, and when	• Implement centralized logging across apps, databases, and cloud systems • Ensure logs are linked to purpose and consent records	SIEM platforms, database audit logs, cloud-native logging
Real-time Monitoring	Detect anomalous or unauthorized data activity	• Set automated alerts for unusual downloads, access outside normal hours, cross-system queries • Monitor for deviations from purpose-based access	SIEM alerts, anomaly detection algorithms, AI-driven monitoring
Audit & Review	Periodically validate compliance and identify gaps	• Conduct regular reviews of access logs vs. consent and purpose • Reconcile user actions against internal policie	Quarterly audits, internal compliance dashboards
Accountability & Ownership	Assign clear roles for data access oversight	• Define responsibilities for IT security, data owners, and compliance teams • Establish escalation and remediation processes	Data Protection Officer (DPO), Security Operations Center (SOC) workflows
Integration with DLP / CASB	Prevent accidental or malicious data leaks	• Enforce data loss prevention rules linked to monitoring • Restrict unauthorized exports or transfers	DLP tools, CASB solutions, cloud security posture management
Reporting & Documentation	Ensure readiness for regulatory inspection	• Maintain structured, timestamped logs • Document purpose justification for every access • Keep evidence for potential audits or breach investigations	Regulatory-ready dashboards, automated compliance reports
Continuous Improvement	Evolve monitoring based on emerging risks	• Regularly update alert thresholds, access policies, and retention schedules • Incorporate learnings from audits and incidents	Threat intelligence feeds, periodic policy reviews

and liability clauses. This ensures that outsourcing or cloud services do not dilute compliance or introduce additional risks.

Under the DPDP Act, enterprises remain fully accountable for personal data even when it is processed by vendors, cloud providers, or other third parties. Organizations must ensure that external parties act strictly within the agreed purposes, comply with retention and deletion requirements, and maintain robust security standards. Failure to enforce these obligations can lead to regulatory penalties, reputational damage, and operational risk.

> ***"From requirement gathering to operationalization, privacy needs to be considered at every stage."***
>
> ***-Vikas Srivastva,*** *CTO, Mahindra Holidays & Resorts*

Think Before You Send: Cross-Border Data Compliance

DPDP restricts the transfer of personal data outside India. Organizations must implement contractual and technical safeguards to protect data during international transfers. Non-compliance can lead to heavy penalties and reputational harm, especially for global enterprises or those using cloud services.

> *"Businesses must obtain explicit, informed consent from individuals before collecting their data, and consent must be voluntary with a simple method for users to withdraw it at any time."*

***-Prashant Mali,** President & Founder, Cyber Law Consulting (Advocates & Attorneys)*

Key CISO Responsibilities

Focus area	Objective	CISO Action Points	Implementation Notes / Tools
Vendor Assessment	Ensure vendors can meet DPDP compliance standards	• Conduct due diligence before onboarding • Evaluate security controls, prior audit results, and regulatory awareness	Vendor questionnaires, security audits, compliance certifications
Contractual Governance	Clearly define data obligations and liabilities	• Include clauses specifying purpose limitation, retention, deletion, and breach reporting • Define liability and indemnity for non-compliance	Standardized contract templates, legal review
Data Flow Mapping	Track personal data across all third parties	• Map what data is shared, for what purpose, and who has access • Ensure alignment with consent records	Data inventory tools, flow diagrams, cloud access reports
Monitoring & Auditing	Validate ongoing compliance	• Periodically audit third-party processing against contracts and DPDP rules • Review logs, access patterns, and deletion procedures	Vendor audit reports, remote monitoring, SOC integration
Access Control	Limit data exposure	• Enforce least-privilege access for vendors • Segregate sensitive datasets where possible	Role-based access controls, encryption, tokenization
Incident Response Integration	Ensure prompt action for breaches	• Align vendor breach reporting timelines with internal DPDP incident response • Test joint response procedures	Run tabletop exercises, incident playbooks
Continuous Oversight	Maintain proactive risk management	• Update agreements as regulations evolve • Include regular compliance checkpoints and certifications	Periodic vendor reviews, automated compliance dashboards

2. Data Breach Notification

DPDP mandates that organizations report personal data breaches promptly to affected individuals and the Data Protection Board of India (DPBI), including incident details, mitigation measures, and remedies. Timely reporting is key to compliance and maintaining trust.

CISO Action Points			
Focus area	**Objective**	**Action Points**	**Notes / Tools**
Incident Detection	Quickly identify breaches	• Deploy monitoring and alerting systems for unusual access or exfiltration	SIEM, DLP, CASB
Response & Escalation	Structured, rapid response	• Establish breach notification protocols • Define internal escalation paths	Incident response playbooks, SOPs
Reporting & Documentation	Comply with legal mandates	• Prepare templates for DPBI and affected individuals • Record mitigation measures and timelines	Audit logs, automated reporting systems
Post-Incident Review	Reduce recurrence	• Analyze root causes • Update policies, controls, and training	Lessons learned sessions, risk registers

3. Legacy Data & Risk Management

Data collected before DPDP came into force may lack clear consent. Organizations must evaluate and manage historical datasets to reduce legal risk and ensure transparency.

CISO Action Points			
Focus area	**Objective**	**Action Points**	**Notes / Tools**
Data Inventory & Classification	Identify at-risk legacy data	• Map old datasets by type, purpose, and consent status	Data cataloging tools
Consent Management	Align past data with DPDP	• Reach out for fresh consent where possible • Document responses	Email/SMS/app notifications
Data Remediation	Reduce legal exposure	• Anonymize or securely delete data lacking consent	Automated deletion scripts, pseudonymization tools
Ongoing Monitoring	Ensure compliance continuity	• Periodic review of legacy datasets for proper usage	Audit logs, data governance dashboards

4. AI & Analytics Governance

OVERVIEW:

DPDP emphasizes that AI and analytics datasets must comply with consent and purpose requirements. Function creep, reusing personal data without consent, and processing sensitive data without safeguards are significant risks.

CISO Action Points

Focus area	Objective	Action Points	Notes / Tools
Dataset Review	Ensure lawful use of personal data	• Validate all datasets against consent, purpose, and sensitivity	Data catalogs, consent logs
Data Protection Techniques	Minimize regulatory and ethical risks	• Mask or anonymize data for analytics and model training • Limit access to approved personnel	Pseudonymization, masking, role-based access
Approval Workflows	Prevent function creep	• Require formal approvals for new use cases or model training with personal data	Workflow management tools, data governance policies
Monitoring & Audit	Demonstrate compliance	• Track AI training datasets and model outputs to ensure adherence to DPDP	Audit reports, automated compliance checks

5. Training & Awareness

DPDP requires organizations to educate all employees handling personal data about lawful processing, consent requirements, and security obligations. Embedding privacy principles across teams reduces violations and strengthens compliance culture.

CISO Action Points

Focus area	Objective	Action Points	Notes / Tools
Policy Dissemination	Ensure understanding of DPDP obligations	• Share clear policies, SOPs, and workflow guides	Internal portals, newsletters
Regular Training	Prevent inadvertent violations	• Conduct role-based DPDP and privacy training sessions	E-learning platforms, workshops
Decision Support Tools	Assist staff in day-to-day compliance	• Provide "Can I use this data?" decision trees • Include FAQs on consent, sharing, and retention	Interactive guides, intranet knowledge base
Awareness Campaigns	Reinforce culture of compliance	• Periodic updates on new regulations, reminders, and audit results	Audit reports, automated compliance checks

'Ask Me Anything on DPDP Rules'

During the CISO Forum Annual Conference, **Khushboo Jain, Managing Partner, Ark Legal & Satyanandan Atyam, Chief Risk Officer, TATA AIG General Insurance,** conducted a session addressing the key concerns of conference participants.

THE CISO Forum recently hosted an interactive "Ask the Expert" session on the Digital Personal Data Protection (DPDP) Rules. The session featured expert insights from Khushbu Jain, an Advocate at the Supreme Court of India and Founding Partner of Ark Legal, and Satyanandan Atyam, Chief Risk Officer, TATA AIG General Insurance.

CISOs and CIOs posed pertinent questions regarding the operational impact of the new regulations. Below are key questions and answers from that discussion to help guide your organization's compliance journey.

Q: If my privacy is breached under DPDP, do I get compensated, or does the money only go to the government?

EXPERT: You're right that the Act does not prescribe a fixed or formula-based compensation for the data principal. Penalties are framed as "up to" a certain amount – that could be as low as INR 10,000 or as high as ₹5 crore, depending on the case.

So, compensation will largely emerge through litigation and legal precedents. Courts and the Data Protection Board will interpret "harm", look at the facts of each case and gradually set benchmarks. Until then, this uncertainty is a genuine vulnerability in the ecosystem.

Q: Why did the government create an independent "Consent Manager"? Can an organisation itself act as one?

EXPERT: "Consent Manager" is a new, independent role created in the Act. These entities will have about 12 months to register and then demonstrate compliance on security, interoperability and technology standards.

However, many aspects are still unclear:

- What exactly are their obligations and liabilities?
- Will there be minimum/maximum pricing for their services?
- How will disputes between Consent Managers, Data Fiduciaries and data principals be handled?

Importantly, data fiduciaries are not obligated to use a Consent Manager. You can continue managing consent in-house.

Given the uncertainty, my advice is:

- Spend the next 12 months getting your own consent, data-mapping and governance processes in order.
- Wait for clearer rules on Consent Manager obligations and pricing before you rush to appoint one. For now, they will only be a front-end

CISO's DPDP Playbook: Quick Reference

Area	What It Means	CISO Actions / Controls	Examples
Purpose Limitation	Use personal data only for the purpose you told the user. For any new use, get fresh consent.	Map every data field to an approved purpose. Enforce purpose-based access rules.	Email collected for billing cannot be used for marketing.
Data Minimisation	Collect only the minimum data needed. Keep it only for as long as required.	Review forms, APIs, logs, and delete unnecessary fields. Automate retention deletion.	Don't collect DOB if age bracket works. Delete KYC scans after legal retention.
Purpose-Based Access Control	Access must match the declared use-case – not generic roles.	Shift from "department-based" to "use-case-based" permissions.	✓ Marketing can access email for retention campaign **X** But not for new AI model training
Dataset Segregation	Avoid giant "everything buckets." Split data by purpose.	Create filtered datasets/views with restricted fields per use-case.	billing_view, support_view, analytics_view (anonymised), marketing_view.
Monitoring & Logs	Track how data is used, by whom, and why.	Log dataset access + declared purpose. Auto-flag unusual actions.	Bulk downloads, cross-domain joins, wrong-system access.
Analytics & AI Guardrails	AI teams easily drift into "function creep."	Provide masked/aggregated data; require privacy review for raw data.	Share anonymised datasets; allow raw data only with documented approval.
DLP / CASB Controls	Prevent data going to wrong systems or people.	Configure rules for Aadhaar, PAN, health data, export limits.	Block Excel exports of PAN data; alert if uploaded to cloud drives.
Third-Party Controls	Vendors must follow your stated purpose.	Update contracts with allowed purposes, no secondary use, deletion obligations; audit regularly.	Cloud vendor can process data only for support—not analytics or ads.
Legacy Data Risk	Old datasets may not have clear consent or purpose.	Identify risky historic data; delete, anonymise, or re-seek consent.	Old CRM backup with fields not needed today.
Team Awareness	Most violations happen due to misunderstanding.	Train teams; share "Can I use this data?" decision-tree.	Product team asking to reuse phone numbers for a new feature → requires review.

to record consent and withdrawals; the heavy lifting at the back-end still remains with you.

Q: We already hold large volumes of customer data collected in the past. Do we now need to go back and obtain consent again?

EXPERT: The law is not crystal clear yet, but here is a practical approach:

- Reach out once to existing customers—via email, SMS, app or website pop-up.
- Tell them what data you hold, for what purposes you use it, and ask for their consent under the new regime.
- Provide links to:
  - Your consent form, and
  - Your privacy policy, which should clearly list purposes and third-party sharing.

If they explicitly consent, you're safe. If they remain silent, you can reasonably argue later that:

- The data was already part of your ongoing business, and
- You proactively sought consent after the law came into force; since they did not object or withdraw, you continued processing.

However, do not stay silent. Sending that one consent request for old data is important both for transparency and future legal defence.

Q: Earlier we collected data mainly for business operations. Now we may want to use the same data for cross-selling. If we don't mention cross-selling in the consent, are we restricted?

EXPERT: Yes. Under DPDP, purpose specification is central.

- When you seek consent (including for old data), clearly state all purposes: servicing, billing, marketing, cross-selling, etc.
- Link to a detailed privacy notice with itemised purposes and list of third-party vendors. This list can change over time, so your notice should say that the policy will be updated periodically and indicate the last updated date.

If you collect consent only for "billing", you cannot later justify using the same data for marketing unless you have obtained separate, explicit consent for that purpose.

Q: How does DPDP distinguish between a Data Fiduciary and a Data Processor?

EXPERT: DPDP uses different terminology but similar concepts:

- **Data Fiduciary (like GDPR's Controller):** The primary entity that determines the purpose and means of processing. It is the first line of liability.
- **Data Processor:** Processes data strictly on behalf of the Data Fiduciary and within the contractual instructions.

A processor stops being a processor the moment it:

- Uses the data for its own purposes
- Processes it beyond the agreed scope
- Keeps it longer than instructed
- Shares it with other parties without a mandate

In such cases, it becomes a Data Fiduciary (or co-fiduciary) and inherits liability.

So, your contracts must:

- Clearly state what the processor can and cannot do
- Prohibit unauthorised duplication, retention and onward sharing
- Spell out deletion requirements.

Q: In insurance, mutual funds or auto sales, dealers and brokers source the client. Who is the Data Fiduciary and who is the Processor?

EXPERT: If dealers or brokers collect data in your name ("I am collecting this for XYZ Insurance Company"), then:

- You are the Data Fiduciary and first point of contact for the data principal.
- The dealer/broker is acting on your behalf, so they are typically Data Processors or agents.

However, if they also want to use customer data for their own independent purposes – for example, their own marketing – they must:

- Take separate, explicit consent for those purposes, and
- Your contract must reflect that they are acting as an independent fiduciary for that part.

Again, contractual clarity is crucial to avoid paying penalties for someone else's misuse.

Q: How should retailers take valid consent in physical stores with very little time?

EXPERT: Two key points:

CONSENT MUST BE VERIFIABLE.

- A tick on a tablet is not enough if you cannot later prove who gave it.
- After capturing a phone number or email, send the customer an SMS or email summarising the consent and explaining how they can exercise their rights (access, correction, withdrawal, etc.). Keeping this outbound record helps you in case of disputes.

PURPOSE LIMITATION STILL APPLIES.

- If you collect data only for billing or delivery, you should delete it once that purpose is fulfilled, unless there is a legal requirement (for example, to retain invoices for 12 months).
- Using that same data for marketing without consent is not permitted.

The Act even gives an example of a pharmacy to illustrate this "limited purpose" principle.

Q: In B2B relationships, suppliers often share their name, official email ID and phone number. Does this count as personal data under DPDP?

EXPERT: Yes. Anything that can identify a person is personal data: name + phone number, email, IP address, etc.

Essential Dos & Don'ts Under India's DPDP Rules 2025

A Practical Compliance Checklist for CISOs & CIOs

Data Protection Dos	Data Protection Don'ts
Obtain explicit, informed consent before collecting or processing any personal data.	Don't use vague, hidden, or confusing language to secure consent or explain data use.
Explain data purposes in clear, simple language that any user can understand.	Don't retain personal data longer than necessary unless legally required.
Allow users to withdraw consent easily, using the same simplicity as the opt-in process.	Don't delay grievance handling—respond within the mandated timelines (typically 90 days).
Implement strong security controls—encryption, role-based access, monitoring, and breach prevention.	Don't transfer personal data outside India without meeting government restrictions and safeguards.
Report data breaches immediately to both affected individuals and the Data Protection Board with clear remediation steps.	Don't process data of children or persons with disabilities without verified parental/guardian consent.
Erase personal data when no longer needed, with reminders to individuals before deletion (where applicable).	Don't outsource Consent Manager duties or create conflicts of interest without disclosure and Board approval.
Provide user-friendly channels for data access, correction, grievance redressal, and complaint escalation.	Don't skip audits or ignore record-keeping obligations mandated under the DPDP Rules.
Appoint a Data Protection Officer (or contact point) and display their contact details prominently.	Don't exceed the stated purpose—avoid processing data beyond what users were informed about.
Apply enhanced safeguards for children and vulnerable individuals, including age checks and lawful consent.	
Conduct annual audits and higher compliance checks if classified as a Significant Data Fiduciary.	

The fact that it's used in a business context doesn't change that.

However, you typically don't need a separate "consent management" flow if the data is processed purely to perform a contract (for example, service delivery, SLAs, invoices). Those obligations can be covered through contract clauses rather than customer-style consent journeys.

But don't assume it's outside DPDP. It is personal data; you must still protect it and process it fairly and lawfully.

Q: Are we giving "implicit" consent when we upload photos to apps that generate avatars?

EXPERT: Most of these apps actually take very explicit, very broad consent—if you read their privacy policies carefully. They often claim rights to:

- Use your images for research and model training
- Reuse and share them
- Retain them for long periods

The problem is not lack of explicit consent; it's that users often don't realise how much they're consenting to in the excitement of using a trendy app.

With DPDP, such platforms operating in India will need to rationalise and justify these permissions, and users (especially security professionals like you) should exercise their right to access to see what data is actually held.

Q: What about DPDP in the context of AI? We use first-, second- and third-party datasets. Some may turn out to include PII or infer personal information later. Could these become "tainted datasets"?

EXPERT: Yes, this is a genuine concern. With AI, the training dataset is often a black box. Once models are trained and reused across many organisations, tracing exactly which data point caused which outcome becomes very hard.

To protect yourself:

- Put strong contracts in place across the AI supply chain—between data providers, model developers and consuming enterprises.
- Ensure each link in the chain confirms that:
  - Proper consent has been taken,
  - DPDP and other applicable laws (including IP rights) have been complied with, and
  - Responsibilities are clearly allocated.

Remember, GDPR took nearly eight years from first draft to mature operational practice and is still evolving. DPDP is at a much earlier stage. No company will be "100% compliant" on day one. The goal is to demonstrate good-faith compliance and reduce risk, not to reach a mythical perfect state.

In both DPDP and AI governance, contracts and clarity of roles will be critical. The internet was once called a black box; AI is an even darker one. The more clearly you define who is doing what, on whose behalf, and with what legal basis, the better positioned you'll be when regulators and courts start testing these boundaries. ■

CISO Forum Annual Conference 2025: The new age of strategic cyber leadership

The CISO Forum Annual Conference 2025 united over 100 cybersecurity leaders to redefine the CISO's strategic role amid AI, regulation, and evolving cyber risks.

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

THE CISO Forum hosted its flagship annual conference on November 21–22, 2025, at the Athiva Resort & Spa, Khandala. The conference, themed "The Strategic CISO: Leading in the Age of AI," brought together over 100 senior cybersecurity leaders and Chief Information Security Officers (CISOs) from various industries to address emerging challenges and opportunities in an increasingly complex digital security landscape.

The sessions at the conference emphasized the transformation of the CISO into a strategic business leader equipped to harness emerging technologies like AI and automation to navigate complex regulatory landscapes, and foster resilient security ecosystems amid evolving cyber threats and digital disruption.

The two-day agenda featured impactful keynotes on critical security themes, panel discussions, the NextCISO awards and the CISO Samman recognition. Other highlights of the conference include a fireside chat with cricketer Sanjay Manjrekar, a comedy and musical performance byDr Sanket Bhosale and Sugandha Mishra, and a Cookathon with Sashi Cheliah (MasterChef Australia Season 10 winner, 2018).

The conference was hosted in collaboration with industry partners like Kaspersky, Microsoft, and Securiti, Claroty, Proofpoint, Versa, Netskope and SentinelOne. It also featured exhibition partners like ANA Cyber Forensic, Armis, Barracuda Networks, Cotelligent, Cyber Vigilens, Morphisec, NeoSoft, Protechmanize, Aquila, Sophos, Magnanimous Systems, and Trellix.

The conference commenced with Jatinder Singh, Editor, 9.9 Group, presenting insights from the State of Enterprise Security Survey 2025, followed by keynote talk on the evolving role of "The CISO in the AI Era"byDavid Gee, International CIO, CISO & Board Advisor. Vamsi Ponnekanti, Regional Business Leader – India, Securiti.ai made a presentation on "How DSPM Unifies Security, Privacy and AI Governance in the Cloud Era." This set the stage for the opening panel discussion on"Managing the Risks of AI and Agentic AI."

Following a tea break, the conference featured a fireside chat with the well-known Indian cricket commentator and former member of the Indian cricket team,Sanjay Manjrekar.

The afternoon sessions then dived deeper into technical, operational, and regulatory perspectives through four keynote sessions by Vishal Salvi, Global Cybersecurity Practice Head at Cognizant (Evolving Cybersecurity Through AI); Priyadarshi Achar, Sales Engineering Leader – India & SAARC, Proofpoint (Rethinking Data Loss Prevention); Khushboo Jain, Managing Partner, Ark Legal (DPDP and India AI Guidelines: Implications for Technology Leaders); and Satyanandan Atyam, Chief Risk Officer, Tata AIG General Insurance (A Practitioner's View on AI Risk and DPDP Readiness). This was followed by a panel discussion on "Building Next-Gen Cybersecurity Teams Amid Talent Shortages."

The evening featured an innovative Ideas Café, with rapid roundtable discussions hosted by leading security vendors, followed by concurrent CISO mixers and closed-door roundtables.

Day one concluded with the NextCISO Awards, recognising emerging security leaders, followed by the second CISO Samman felicitation, honouring Agnelo D'Souza, Adani Arports; Muralidhar Nambiar, State Bank of India; Jacxine Fernandez, Bangalore International Airport; and Lucius Lobo, Tech Mahindra for their exemplary leadership and contributions to the cybersecurity community.

The evening wrapped up with cocktails, dinner, and a high energy performance by Dr Sanket Bhosale and Sugandha Mishra.

Day Two

Day two opened with an "Ask Me Anything" session featuring Khushboo Jain and Satyanandan Atyam, offering attendees direct access to expert perspectives on navigating the DPDP Rules and AI Governance Guidelines. This was followed by a panel discussion on the topic "Third-Party Tsunamis: Managing IT Supply Chain and Vendor Risk," roundtable discussions, case-study workshops, and booth visits by delegates.

The annual CISO Forum conference concluded with the felicitation of "AI Visionary CISOs,"which recognised leaders who have championed innovative approaches to AI security.

An interactive cooking session with Sashi Cheliah, MasterChef Australia Season 10 winner, sponsored by Securiti.ai and Kaspersky, provided a fitting finale that reinforced the forum's emphasis on community-building alongside professional development.

Delegates departed after a power lunch, carrying insights from two days of intensive discussions on navigating one of the most transformative periods in cybersecurity history. ■

Vikas Gupta, CEO & Editorial Director, B2B Tech and Co-Founder, 9.9 Group delivered the welcome address. He set the tone by positioning the CISO as a strategic business architect grappling with accountability and AI complexity—questioning whether organizations can truly rely on the trustworthiness of their AI models.

State of Enterprise Security
Top Cybersecurity Threats: 2025 Reality Check
17th Annual Conference
CISO FORUM
#TheCISOForum

In his presentation on the State of Enterprise Security 2025, **Jatinder Singh, Editor, 9.9 Group,** highlighted how Indian cybersecurity leaders are tackling complexity, enabling innovation, and reclaiming control in uncertain times.

The CISO in the AI Era–A Strategic Enabler's Digital Workforce
CISO FORUM

David Gee, International CIO, CISO & Board Advisor explained why CISOs must transform from security gatekeepers to strategic business enablers who serve as the "HR department for AI"—ad how they will need to manage digital employees through comprehensive lifecycle governance, identity management, and performance monitoring.

How DSPM Unifies Security, Privacy and AI Governanc in the Cloud Era
Vamsi Ponnekanti
17th Annual Conference
CISO FORUM

How DSPM Unifies Security, Privacy and AI Governance in the Cloud Era: **Vamsi Ponnekanti, Regional Business Leader - India, Security.AI**

The Panel Discussion on Managing the Risks of AI & Agentic AI examined how AI and AI agents are reshaping India's enterprise landscape, introducing new security challenges. It underscored the need for CISOs to balance risk mitigation with responsible innovation. (Left to Right) **Abhishek Jha,** Tata Technologies; **Dr Pawan Chawla,** Tata AIG Life Insurance; **Hitesh Sachdeva,** ICICI Bank; **Jayjit Biswas,** Tata Motors; **Himachal Jothinarasimhan,** Ashok Leyland. The discussion was moderated by **Jatinder Singh,** CISO Forum.

Sanjay Manjrekar, Indian cricket commentator and former member of the Indian cricket team in conversation with **Sachin Mhashilkar, COO, 9.9 Group**

Evolving Cybersecurity Through AI: Stages of Adoption and Maturity
CISO FORUM

Vishal Salvi, Senior Vice President & Global Cybersecurity Practice Head, Cognizant Technology Solutions Corp discussed the evolution of Cybersecurity and the impact of AI

proofpoint
Rethinking Data Loss Prevention
Priyadarshi Achar
Sales Engineering Leader, India
CISO FORUM

Priyadarshi Achar, Sales Engineering Leader - India & SAARC, Proofpoint spoke about "Rethinking Data Loss Prevention."

India's AI Guidelines and the Implications for Technology Leaders
Khushboo Jain
CISO FORUM

Khushboo Jain, Managing Partner, Arklegal discussed the implications of the DPDP Rules and India's AI Guidelines for technology leaders.

The panel discussion on "Building Next-Gen Cybersecurity Teams Amid Talent Shortages" focused on India's cybersecurity talent gap, and the avenues for upskilling and AI augmentation. It also covered talent retention strategies that are essential for building resilient, future-ready security teams. (Left to Right) **Dinesh Shrimali,** Tata Steel; **Lucius Lobo,** Tech Mahindra; **Pradipta Patro,** KEC International; **Avinash Tiwari,** Pidilite. The discussion was moderated by **R Giridhar,** CISO Forum

Satyanandan Atyam, Chief Risk Officer, TATA AIG General Insurance made a detailed presentation on the practical issues surrounding AI Risk and DPDP Readiness.

Ideas Café - Rapid Roundtables: Structured, closed-door discussions enabling CISOs to exchange insights and co-create actionable strategies.

Roundtable Discussion on the"Evolving Role of AI in Data Security"hosted by **Priyadarshi Achar,** Sales Engineering Leader - India & SAARC, Proofpoint. Discussion moderated by **Jatinder Singh,** Editor, 9.9 Group

Roundtable Discussion on "Cyber Security in the Age of AI: Data Defense & Intelligent Protection" hosted by **Anujh Tewari,** Chief Cybersecurity Advisor & Field CISO, Microsoft India. Discussion moderated by **R Giridhar,** Group Editor, 9.9 Group

Roundtable Discussion on "Cyber Security in the Age of AI: Data Defense & Intelligent Protection" hosted by **Aman Malhotra,** Security Global Black Belt - Securing AI & Agents, Microsoft India. Discussion moderated by **Sachin Mhashilkar,** COO, 9.9 Group

NEXTCISO 2025 award winners felicitated by **Kaspersky India, Claroty and Microsoft**

NextCISO 2025 Jury members felicitated by **Vikas Gupta**, CEO & Editorial Director, B2B Tech and Co-Founder, 9.9 Group

CISO Samman 2025 recipients **Agnelo D'Souza,** Adani Airport Holdings and Lucius Lobo, Tech Mahindra are felicitated by senior CISOs **Uday Deshpande,** L&T and **Rajesh Thapar,** NSE India

CISO Samman Committee members, **Uday Deshpande** and **Rajesh Thapar** felicitated by **R Giridhar** and **Jatinder Singh,** 9.9 Group

Ask Me Anything on DPDP Rules and AI Governance Guidelines hosted by **Khushboo Jain,** Managing Partner, Arklegal and **Satyanandan Atyam,** Chief Risk Officer, TATA AIG General Insurance

Music and entertainment program by **Dr Sanket Bhonsale** & **Sugandha Mishra**

Panel Discussion on "Third-Party Tsunamis—Managing IT Supply Chain and Vendor Risk," examined the need for continuous vendor risk assessments and stronger supply-chain security monitoring. (Left to Right) **Agnelo D'souza,** Adani Airport Holdings; **Deepak Bhonsale,** Asian Paints; **Divan Raimagia,** Adani Green Energy; **Dr Yusuf Hashmi,** Jubilant Group; and **Vamsi Krishna,** Axis Mutual Fund. Discussion moderated by **R Giridhar,** 9.9 Group

Roundtable discussion on "Why Cyber-Physical Systems Require Unique Security," hosted by **Joshua Kathiravan,** Solution Engineer, Claroty. Discussion moderated by **R Girdhar,** Group Editor, 9.9 Group.

Round table discussion on "Data Risk - Evolving Paradigm and Challenges" hosted by **Vamsi Ponnekanti,** Regional Business Leader – India, Securiti.ai. Discussion moderated by **Jatinder Singh,** Editor, 9.9 Group.

Case Study Workshop by Versa. Moderator: **Sachin Mhashilkar,** COO & Associate Publisher, B2B Tech, 9.9 Group

Cookathon with **Sashi Cheliah** (MasterChef Australia Season 10 winner 2018), sponsored by **Securiti.ai and Kaspersky**

Data encryption and protection

Encryption is becoming essential for protecting sensitive data, reducing breach impact, and meeting rising cybersecurity and compliance demands.

By **Dr. Sunil Kr Pandey** | Director (IT), Institute of Technology & Science com

IN TODAY'S digital landscape, data breaches and cyber attacks pose significant threats to organizations' sensitive information. Data encryption and protection have emerged as critical components of a robust cybersecurity strategy. This article explores the imperative of data encryption and protection in preventing data breaches and ensuring the confidentiality, integrity, and availability of digital assets. We delve into the latest encryption technologies, including homomorphic encryption and quantum encryption, the latest industrial trends, the market in Data encryption, cyber security and in what direction is it heading towards, It also discusses some of the best practices. Furthermore, we examine the growing demand for encryption as a service and the importance of implementing a comprehensive data protection strategy to mitigate the risk of data breaches and cyber-attacks.

Introduction

The encryption process involves converting readable plaintext into unreadable ciphertext to prevent unauthorized access to sensitive information. To safeguard against data breaches, organizations widely adopt encryption as a critical component of their data security strategies. Encryption algorithms scramble data into an indecipherable format, ensuring that only authorized parties with the decryption key can access the information. Notably, encryption protects data in various states, including at rest, in transit, and during processing, whether stored on-premises or in the cloud.Given its effectiveness, encryption has become a cornerstone of cloud security and broader cybersecurity efforts. According to the IBM 2023 Cost of a Data Breach report, organizations that implement encryption can reduce the financial impact of a data breach by over $220,000. Moreover, encryption is increasingly necessary for complying with regulatory requirements, such as PCI DSS and GDPR.

The growing investment in encryption by organizations underscores the escalating threat landscape. In fact, the global encryption software market is projected to reach $20.1 billion by 2025, with a compound annual growth rate (CAGR) of 15.1% from 2020 to 2025 further to with the market size anticipated to reach USD 60.7 billion by 2033. Likewise, the global encryption as a service market is poised for significant growth, projected to surge from USD 1.57 billion in 2024 to USD 5.98 billion by 2030, at a remarkable Compound Annual Growth Rate (CAGR) of 24.9%. Key drivers of this growth include the accelerating adoption of cloud services and escalating concerns over critical data loss. In recent years, modern encryption algorithms have largely replaced outdated standards like the Data Encryption Standard (DES).

The emergence of artificial intelligence (AI) has also transformed the encryption landscape, with organizations exploring AI's potential to optimize key management and enhance encryption algorithms.As organizations increasingly adopt cloud and hybrid cloud environments, encryption has become a crucial safeguard for sensitive data. However, this shift also introduces data complexity, characterized by data sprawl and expanding attack surfaces. Consequently, data breaches are becoming more frequent and costly. A recent report revealed that the global average cost of remediating a data breach in 2023 was $4.45 million, marking a 15% increase over three years. Encryption plays a vital role in deterring or mitigating the severity of data breaches by rendering sensitive data, such as social security numbers and credit card information, inaccessible to hackers. Furthermore, organizations in regulated industries like healthcare and finance rely on encryption to meet stringent compliance standards and protect sensitive personally identifiable information (PII). With current nature of security, the following projections related to Cyber Security present an interesting directions in which the market is moving forward:

Dr. Sunil Kr Pandey
Director (IT),
Institute of Technology & Science

- **Encryption as a Service Market:** Expected to grow from USD 1.57 billion in 2024 to USD 5.98 billion by 2030, at a CAGR of 24.9%.
- **Network Security Market:** Projected to grow from USD 78.2 billion in 2024 to USD 111.0 billion by 2029, at a CAGR of 7.2%.
- **Zero Trust Security Market:** Expected to grow from USD 36.5 billion in 2024 to USD 78.7 billion by 2029, at a CAGR of 16.6%.
- **Incident and Emergency Management Market:** Projected to grow from USD 137.45 billion in 2024 to USD 196.20 billion by 2030, at a CAGR of 6.1%.
- **Data Protection as a Service Market:** Expected to grow from USD 26.04 billion in 2024 to USD 74.91 billion by 2030, at a CAGR of 19.2%.
- **Artificial Intelligence in Cybersecurity Market:** Projected to grow from USD 22.4 billion in 2023 to USD 60.6 billion by 2028, at a CAGR of 21.9%.
- **DDoS Protection & Mitigation Security Market:** Expected to grow from USD 5.17 billion in 2024 to USD 9.63 billion by 2029, at a CAGR of 13.2%.

Advances in encryption algorithms have led to the development of robust security solutions that not only protect data confidentiality but also ensure integrity, authentication, and nonrepudiation. These principles guarantee that data remains tamper-proof (integrity), verify the authenticity of data sources (authentication), and prevent users from denying legitimate transactions (nonrepudiation).Current encryption trends focus on enhancing algorithms and protocols to counter emerging cyber threats and technologies. Two notable examples are:

- **Quantum Encryption:** Leveraging quantum mechanics principles to create cryptographic keys that are theoretically resistant to brute-force attacks.
- **Homomorphic Encryption:** Enabling organizations to perform computations on encrypted data without decryption, ensuring confidentiality and individual privacy. This approach facilitates the use of sensitive data for applications like AI model training and analysis, without compromising security.

These innovations mark significant strides in encryption technology, offering organizations robust protection against evolving cyber threats

“Encryption has become a cornerstone of cloud security and broader cybersecurity efforts.”

while preserving data utility and privacy.Recent developments in encryption revolve around homomorphic encryption for secure data processing in use, Post-Quantum Cryptography (PQC) for resilience against quantum attacks, and advancements in algorithms like AES and RSA for enhanced security. The homomorphic encryption allows computations to be performed directly on encrypted data without decryption, ensuring data privacy during processing.This is crucial for tasks like secure cloud storage and outsourced computations, where sensitive data needs to remain protected during use.This ability to process data in use or data in motion is a key feature of homomorphic encryption.

However, as technology evolves, especially with the potential rise of quantum computers, new encryption challenges arise. Quantum computers pose a significant threat to asymmetric cryptography or public key encryption, like the RSA algorithm.

Data breaches are becoming increasingly common, with hackers and cybercriminals using sophisticated techniques to gain unauthorized access to sensitive information. According to a report by IBM, the average cost of a data breach is around $3.9 million. Moreover, data breaches can also lead to reputational damage, loss of customer trust, and even legal liabilities.

Best Practices for Data Encryption and Protection

- **Use Strong Encryption Algorithms:** Use widely accepted and reviewed encryption algorithms, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).
- **Implement End-to-End Encryption:** Ensure that data is encrypted from the moment it's created to the moment it's deleted.
- **Use Strong Encryption Algorithms:** Use widely accepted and reviewed encryption algorithms, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).
- **Use Secure Key Management:** Implement a secure key management system to generate, distribute, and manage encryption keys.
- **Regularly Update and Patch Software:** Regularly update and patch software to prevent vulnerabilities and exploits.
- **Use Two-Factor Authentication:** Use two-factor authentication to add an extra layer of security to your data protection strategy.
- **Conduct Regular Security Audits:** Conduct regular security audits to identify vulnerabilities and weaknesses in your data protection strategy.
- **Train Employees on Data Protection:** Train employees on data protection best practicesand ensure they understand the importance of data encryption and protection.

Conclusion

Data encryption and protection are essential for safeguarding of sensitive information in today's digital age. By implementing a robust data protection strategy that includes strong encryption algorithms, secure key management, and regular security audits, we can protect our data from unauthorized access and ensure the confidentiality, integrity, and availability of your digital assets.As encryption technology advances, so must our understanding and skills. We must invest time and resources into understanding and adapting to the promising advancements in encryption technologies in preparation for the future. These mechanisms offer transformative potential for safeguarding our digital assets and privacy, yet also present unique challenges and complexities that need to be surmounted. Navigating the future of encryption requires a delicate balance of harnessing these new technologies while also preparing for their associated challenges. By doing so, we can hope to foster a future where data security and privacy are not just assured but also accessible and user-friendly. ■

Guarding the skies: How cyber resilience keeps airports safe

Neehar Pathare, Managing Director, CEO & CIO of 63SATS explains how cyber resilience, zero trust, and OT security are critical to safe, resilient aviation operations.

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

IN AN industry where every second of uptime can mean the difference between safety and chaos, cybersecurity in aviation isn't optional—it's existential. In this exclusive conversation with CISO Forum, Neehar Pathare, Managing Director, CEO & CIO of 63SATS, delves into the complex cybersecurity landscape underpinning aviation and airport operations. He emphasizes that the modern CISO's role goes far beyond protecting data—it's about safeguarding the interconnected web of operational technologies keeping airports running: from air traffic systems to fuel management and baggage handling.

He outlines a pragmatic framework for building cyber resilience through segmentation, zero-trust security, and recovery readiness, while emphasizing the importance of trust, compliance, and innovation by design. As AI-driven threats rise and operational systems become increasingly connected, Pathare makes a compelling case for unifying governance, automation, and human preparedness—transforming cybersecurity into a strategic enabler of safe, efficient, and intelligent aviation.

CISO Forum: In a sector where operational continuity is critical, how do CISOs address cyber risks across aviation and airport services?

NEEHAR PATHARE: In aviation, operational continuity isn't just a business goal; it's a core safety imperative. The primary challenge is the deep convergence of IT and OT. We're no longer just protecting data; we're also safeguarding critical physical systems, including baggage handling, air traffic control, runway lighting, and fuel management.

The CISO's approach must be built on cyber resilience:

- **Deep Segmentation:** We must strictly segment critical OT networks from the corporate IT environment and the public-facing internet. This prevents a breach in one area (like guest Wi-Fi) from cascading into a critical operational system.
- **Zero Trust for OT:** Assume a breach is possible. Every connection request to a critical system must be authenticated and authorized, regardless of whether it's "internal" or "external."
- **Resilience and Recovery:** Because you cannot always patch OT systems (which may require a complete system shutdown), the focus shifts to rapid detection and recovery. We must have well-practiced playbooks to isolate a compromised system and failover to redundant controls immediately, ensuring the airport continues to function safely.

CISO Forum: How does protecting passenger and operational data support both trust and operational efficiency in highly regulated environments?

NEEHAR PATHARE: This is a dual-pillar strategy

- **Protecting Passenger Data (PII):** This forms the foundation of trust. Passengers exchange personal data—passport information, travel itineraries—for service. Any breach critically erodes public confidence in airlines or airports, causing brand damage and severe regulatory penalties (like GDPR). Robust data encryption, strict access controls, and data minimization are non-negotiable.
- **Protecting Operational Data:** This ensures efficiency and safety. Consider the impact of corrupted flight manifests, maintenance logs, or cargo weight and balance data. It could ground entire fleets or create direct safety risks. Protecting data integrity ensures operations run smoothly, on time, and safely. In regulated environments, strong data protection provides competitive advantage, demonstrating maturity and stability to partners and regulators alike.

> **"In aviation, operational continuity isn't just a business goal; it's a core safety imperative."**

CISO Forum: What frameworks are effective in managing cyber risk across multiple airport facilities or operational sites?

NEEHAR PATHARE: A "one-size-fits-all" framework doesn't work. The most effective strategy is a hybrid, risk-based model combining centralized governance with decentralized execution

- **Centralized Governance:** A central team establishes the "what" and "why" using a standard framework like the NIST Cybersecurity Framework (CSF). It provides a common language—Identify, Protect, Detect, Respond, Recover—that all facilities can understand and map to.
- **Decentralized Execution (IT):** For IT systems (booking, corporate email), ISO 27001 is excellent for building a robust Information Security Management System (ISMS) that can be certified and audited across sites.
- **Decentralized Execution (OT):** For critical operational technology, the ISA/IEC 62443 series is the gold standard. Purpose-built for Industrial Control Systems (ICS), it helps each facility apply specific controls relevant to its unique machinery and risk profile.

This federated model allows a central CISO to manage aggregate risk scores while empowering local teams to address specific, on-the-ground threats.

CISO Forum: How can innovation in passenger services be balanced with stringent security and compliance requirements?

NEEHAR PATHARE: Innovation and Security must be partners, not adversaries. The "move fast and break things" mentality is unacceptable in critical infrastructure.

The balance is achieved through "Security by Design" and a DevSecOps culture.

- **Embed Security Early:** Security teams must be involved from the inception of a new service (such as a biometric boarding app or a new IoT-based baggage tracker), not just at the final testing phase. This "shift-left" approach identifies and mitigates risks when they are cheapest and easiest to fix.
- **Risk-Based Controls:** Instead of applying a blunt, "maximum-security" policy to everything, we use controls proportionate to the risk. A new digital information kiosk has a different risk profile than an app that touches the flight control system.
- **Secure API Gateway:** Most new passenger services are built on APIs. A robust API security strategy—focusing on authentication, rate limiting, and anomaly detection—is essential to enable innovation without exposing the core systems behind it.

CISO Forum: Which metrics or KPIs best capture the effectiveness of cybersecurity initiatives in critical infrastructure sectors?

NEEHAR PATHARE: Vanity metrics, such as "number of attacks blocked," are useless. In critical infrastructure environments, the most meaningful KPIs are tied to resilience and operational uptime. Security effectiveness must be measured by how quickly systems recover, how early threats are detected, and how well critical assets are protected.

- **Mean Time to Recover (MTTR)** is the most critical KPI. When an incident occurs, how fast can full, safe operations be restored? This is the ultimate test of cyber resilience.
- **Mean Time to Detect (MTTD)** measures how long an adversary remains in the network before detection. Faster detection limits damage and business impact.
- **Percentage of Critical Asset Visibility** tracks how much of the organization's IT and OT environment is fully monitored. You cannot protect what you cannot see.
- **Patching and vulnerability cadence** measures how consistently critical vulnerabilities are remediated within defined SLAs.

Finally, a control efficacy score, measured through Breach and Attack Simulation (BAS), shows how often security controls stop realistic attacks.

> "Innovation and Security must be partners, not adversaries."

CISO Forum: How are teams being prepared to anticipate and respond to emerging threats, including AI-driven attacks on critical infrastructure?

NEEHAR PATHARE: AI is a dual-use tool. Attackers are using it, and so must we

- **Threats from AI:** We're preparing for AI-driven threats, including hyper-realistic deepfake voice calls for social engineering, polymorphic malware that rewrites itself to evade detection, and AI-powered swarm attacks identifying vulnerabilities faster than any human team.

OUR PREPARATION STRATEGY:

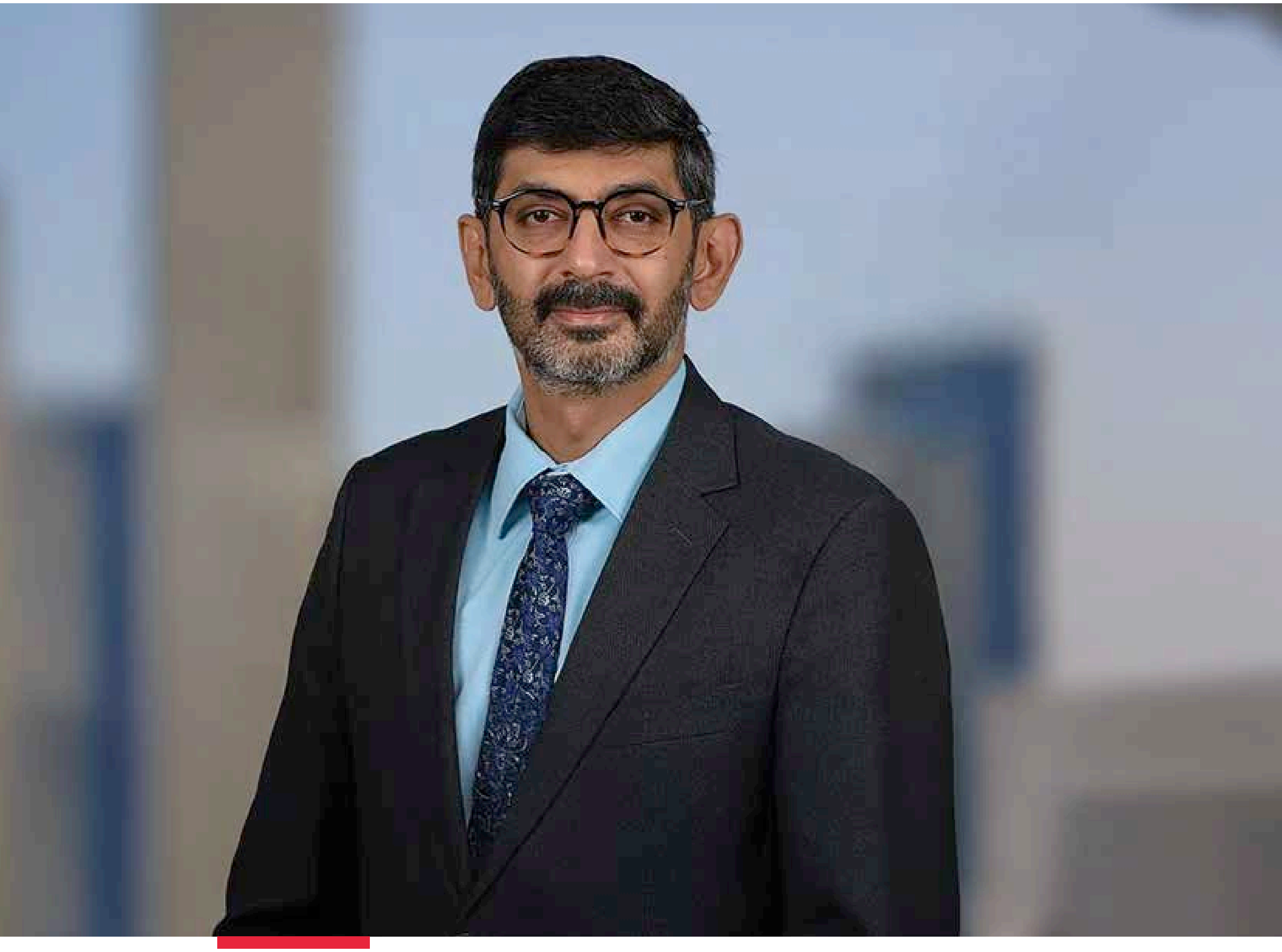
- **AI for Defense:** We're implementing AI and Machine Learning in our Security Operations Centers (SOCs). These tools detect anomalies and subtle network traffic patterns signaling sophisticated attacks that human analysts might miss.
- **Training the "Human Firewall":** The human element remains key. We're moving beyond simple phishing drills to advanced simulations training staff to recognize AI-driven social engineering like deepfake audio.
- **Resilience-Based War Gaming:** We run regular "war game" scenarios based on emerging threats, assuming AI-driven attacks will breach our perimeter, testing our response playbook to build muscle memory for rapid containment and recovery.

CISO Forum: How do your solutions help enterprises address current cybersecurity challenges while balancing risk, compliance, and operational efficiency?

NEEHAR PATHARE: Enterprises face a challenging balancing act: defending against a rapidly evolving threat landscape, navigating complex compliance mandates, and maintaining operational efficiency—all simultaneously. Our solutions address this trifecta, helping security leaders move from constant firefighting to confident, resilient operations.

- **To manage risk,** we provide [e.g., unified threat intelligence platforms / advanced breach detection solutions] moving beyond simple prevention, giving CISOs real-time visibility across the entire attack surface—from traditional IT to complex OT systems—enabling them to identify, contextualize, and prioritize vulnerabilities representing genuine business risk.
- **To streamline compliance,** our [e.g., automated GRC module] maps controls across frameworks like NIST, ISO, and PCI simultaneously, replacing costly manual audits with continuous, verifiable compliance posture.
- **To drive operational efficiency,** our solutions [e.g., leverage AI and SOAR] automate repetitive tasks, reducing analyst fatigue, accelerating response times, and lowering MTTR.

Ultimately, we help organizations evolve from reactive defense to proactive, predictive cyber resilience. ■



Cyber resilience in the age of generative AI

Gautam Kapoor, Managing Director & Lead—Cybersecurity, Accenture, explains why cyber resilience must evolve to protect AI-driven enterprises.

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

AS ORGANIZATIONS race to harness the power of AI and digital transformation, Cybersecurity has become both a business imperative and a strategic differentiator. India's rapid digital acceleration—fueled by cloud adoption, generative AI, and public digital infrastructure—has opened new frontiers of innovation but also amplified the complexity of managing risk across industries.

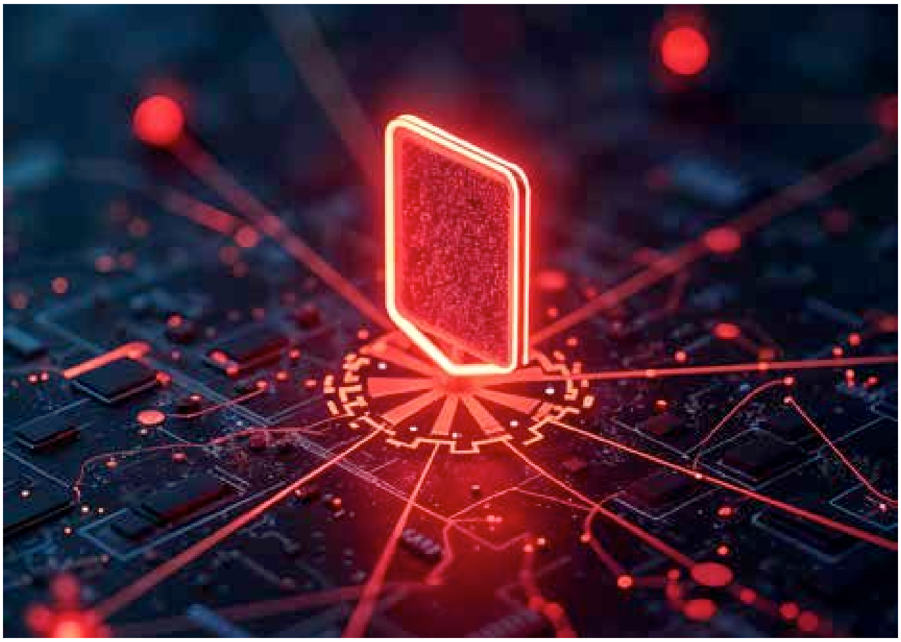
In this exclusive conversation with CISO Forum, Gautam Kapoor, Managing Director & Lead – Cybersecurity, Accenture in India, sheds light on how enterprises can navigate this evolving threat landscape. From AI-powered attacks and compliance challenges to secure-by-design frameworks and predictive defense models, Kapoor outlines the new rules of resilience in an era where trust and transformation must go hand in hand.

He explains why Cybersecurity is no longer a back-office control function but a growth enabler—one that can power secure innovation, safeguard AI adoption, and redefine digital confidence for the enterprise of the future.

CISO Forum: What challenges do organizations face in managing cyber risk across sectors with vastly different regulatory and operational profiles?

GAUTAM KAPOOR: Organizations face mounting challenges in managing cyber risk as they scale AI-driven initiatives across diverse sectors. Many lack foundational security practices – 81% of organizations in India fall short of protecting critical data pipelines and cloud infrastructure, according to our latest research. Some of the contributing factors include the absence of AI security policies, weak implementation of security controls, limited monitoring, and a shortage of skilled professionals.

At the same time, organizations have to navigate diverse compliance requirements while maintaining a consistent security posture. The core challenge is unifying controls across legacy systems, modern cloud-native platforms, and diverse third-party environments. Without these safeguards, organizations remain vulnerable to data breaches, regulatory penalties, and advanced threats, including adversarial attacks, data poisoning, and model manipulation.



“Cybersecurity is no longer about simply ticking boxes or meeting the bare minimum controls; it is a growth enabler.”

CISO Forum: What unique cyber risks are emerging in India's fast-growing digital economy?

GAUTAM KAPOOR: India's digital economy is booming, propelled by the adoption of AI, cloud technologies, and robust digital public infrastructure. However, this rapid growth is exposing organizations to increasingly sophisticated cyber threats. AI-powered attacks are becoming quicker and more challenging to detect. According to our recent report, only 8% of Indian organizations are currently prepared to defend against these advanced threats. Foundational digital platforms face mounting attacks, making cyber resilience an urgent priority.

A significant challenge adding to the risk landscape is the lack of strong AI governance. According to the report, only 19% of companies in India have clear policies and training in place for the secure use of AI. Many organizations still rely on reactive cybersecurity models, which are ineffective in dealing with today's dynamic threat landscape. As Indian enterprises build proprietary AI, securing these models against theft and manipulation is critical. Cyber resilience must be considered at the forefront of every digital initiative.

CISO Forum: How can Cybersecurity be embedded end-to-end across large-scale enterprise transformation programs, particularly in AI and gen AI-led initiatives?

GAUTAM KAPOOR: Cybersecurity by design is essential for successful AI-driven enterprise transformations. Security must be integrated at every stage, from data ingestion and model training to deployment and governance, rather than added as an afterthought. Our research highlights that 81% of Indian companies remain vulnerable due to a lack of cohesive cybersecurity strategies and insufficient technical capabilities. As cyber threats become increasingly sophisticated, especially with the adoption of gen AI by bad actors, traditional defenses are often inadequate, making it imperative to adopt secure-by-design architectures, continuous threat modeling, and AI-specific risk controls to ensure resilience throughout innovation.

The rapid evolution of generative AI brings both new challenges and significant opportunities for enterprise security. Initiating threat modeling early in the design process enables organizations to identify and address vulnerabilities before development, allowing them to detect threats early and take proactive measures to mitigate risks. By building AI systems with robust security foundations and maintaining continuous monitoring and updates, enterprises can stay ahead of emerging threats. This proactive stance not only safeguards digital transformation initiatives but also enhances competitiveness and customer trust, positioning Cybersecurity as a key business enabler.

CISO Forum: How can Cybersecurity shift from compliance to becoming a driver of digital growth?

GAUTAM KAPOOR: Cybersecurity is no longer about simply ticking boxes or meeting the bare minimum controls; it is a growth enabler. When embedded into a digital strategy, it builds trust, accelerates innovation, and opens new markets. In fact, it can act as a differentiator in transformation programs, helping organizations reduce pursuit cycles and enhance customer experience through secure innovation. The shift requires reframing security from a cost center to a value creator.

As organizations accelerate their AI transformation, they must rebalance cybersecurity investments to stay reinvention-ready through four critical actions:

- Develop and deploy a fit-for-purpose security governance framework and operating model that accounts for the realities of an AI-disrupted world, establishes clear accountability, and aligns AI security with regulatory and business objectives.
- Design a digital core to be generative AI secure from the onset by embedding security into AI development, deployment, and operational processes.
- Maintain resilient AI systems with secure foundations that proactively address emerging threats, enhance detection capabilities, enable AI-model testing, and improve response mechanisms.
- Reinvent Cybersecurity with gen AI by leveraging it to automate security processes, strengthen cyber defenses, and detect threats sooner.

By placing security at the core of their AI journey, organizations can safeguard their investments while driving sustainable growth.

CISO Forum: What immediate cyber priorities must enterprises act on in the next 12–18 months?

GAUTAM KAPOOR: In the era of accelerating digital transformation and AI adoption, enterprises must make a decisive shift from reactive to predictive security models. This starts with redefining governance frameworks, as the traditional approach is no longer sufficient in an AI-driven world. Organizations require governance that is fit for purpose, enabling them to identify and address emerging risks, particularly those associated with generative AI, data pipelines, and cloud infrastructure. Security must be integrated from the start, rather than being considered at a later stage, to ensure that adequate controls are part of the digital core from ideation to execution.

Equally critical is developing and maintaining a resilient core. Enterprises must strengthen identity and access management for hybrid workforces, invest in AI-powered threat intelligence, and embed cyber resilience into boardroom agendas. As most organizations remain unprepared for AI-enabled threats, the future of Cybersecurity depends on generative AI enabling automated detection, response, and recovery to outpace adversaries and sustain business operations.

CISO Forum: How does Accenture help enterprises address current cybersecurity challenges while balancing risk, compliance, and operational efficiency?

GAUTAM KAPOOR: Over the past two decades, Accenture has developed one of the most comprehensive and trusted portfolios of security services in the industry, enabling clients to navigate an increasingly complex threat landscape with confidence and scale.

What truly differentiates us is our end-to-end approach from strategy and architecture to implementation and managed services, all delivered through an industry-specific lens. This ensures solutions are tailored to each sector's unique needs, accelerating maturity across cyber risk, compliance, and operational resilience.

Our expertise spans six key areas: cyber strategy, protection, resilience, industry-focused services, cyber-physical security, and emerging technologies, including quantum and space security. Through our Cybersecurity as a Service (CaaS) model, we provide flexible, modern, and automated defenses that offer clear visibility and control, empowering clients to strengthen their security posture while enhancing efficiency and driving growth. ■

Cybersecurity workforce faces growing pains as industry ages

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

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

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

The Aging Workforce Crisis

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

Stress Levels Remain High

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

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

Adaptability Tops the Wishlist

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

Soft Skills Are the Biggest Gap

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

Budget Pessimism Grows

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

AI Adoption Increases

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

The microsegmentation mandate: why 2025 is the year of cyber resilience

Enterprises are prioritizing microsegmentation in 2025 to control lateral movement, boost visibility, and build resilient zero-trust environments.

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

AMAI'S SEGMENTATION Impact Study 2025 highlights how global enterprises are racing to secure sprawling hybrid environments through microsegmentation. This fine-grained security model isolates workloads, preventing attackers from moving laterally across networks. While more than 90% of organizations claim to use some form of segmentation, only 35% have reached microsegmentation maturity, revealing a significant gap between intent and execution.

From Legacy Defenses to Layered Control

Traditional network segmentation focuses on "north–south" traffic—data moving in and out of the network. But as hybrid and cloud infrastructures grow, threats increasingly move "east–west," spreading internally after an initial breach. Microsegmentation provides control at this level, enforcing security at the workload, application, or user layer. This capability is critical for Zero Trust architectures, which assume compromise and verify every interaction.

Why Visibility Matters

The study identifies visibility as a key driver of adoption. Without understanding how workloads and systems communicate, segmentation efforts remain superficial. Microsegmentation provides real-time observability, enabling organizations to map dependencies, close blind spots, and enforce more intelligent access policies. According to the report, 85% of security leaders say that poor visibility undermines their segmentation efforts, underscoring the need for granular monitoring to precede control.

> "85% of security leaders say that poor visibility undermines their segmentation efforts."

Barriers to Maturity

Despite growing awareness, organizations face persistent hurdles. Network complexity is the biggest challenge, cited by 44% of respondents, followed by limited expertise, cultural resistance, and fear of disruption. Many enterprises still struggle to define ownership for segmentation projects, slowing progress. However, large organizations with dedicated Security Operations Centers and regulatory pressure—particularly in finance, energy, and the public sector—are leading the maturity curve.

The Business Case for Microsegmentation

Microsegmentation is not just a cybersecurity tool—it's a financial risk reducer. Akamai's research shows that it helps contain ransomware 21–33% faster, reduces insurance premiums, and simplifies audits. About 75% of insurers now assess segmentation during underwriting, with 60% offering premium reductions for mature practices.

From Optional to Essential

Half of all non-adopters plan to implement microsegmentation within two years, signaling a shift from experimentation to strategic deployment. As cyberattacks become more automated and insurers tighten standards, the study concludes that microsegmentation is no longer optional—it's foundational to enterprise resilience, financial agility, and long-term digital trust.. ■

The strategic shift: how identity became the heart of digital trust

Identity has evolved into the core of digital trust and automation, as AI and machine identities reshape enterprise security strategy.

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

SAILPOINT'S HORIZONS of Identity Security 2025–2026 report underscores a profound transformation: identity has moved from a basic access control mechanism to the strategic core of digital business. In today's AI-accelerated economy, identity orchestrates access, automates decision-making, and enables real-time threat detection across both human and machine users.

A Growing Maturity Divide

The report reveals a widening gap between mature and lagging organizations. Nearly 63% of enterprises remain in early stages of maturity (Horizons 1 and 2), where manual processes dominate and automation is limited. Only a small fraction have reached Horizons 4 and 5, characterized by AI-driven identity automation and adaptive access controls. For every three organizations that advance, two regress—primarily because rising AI and cloud complexities raise the bar for maturity.

AI and Machine Identities Reshape Risk

A striking insight from the study is the explosive growth of non-human identities—AI agents and machine accounts now outnumber human users in many enterprises. Yet fewer than 40% of organizations govern AI agent identities effectively, despite these systems carrying high privileges. SailPoint warns that unmanaged machine identities can become the weakest link in enterprise defense.

Data-Driven Identity is the New Differentiator

Organizations that adopt AI-enabled identity and data capabilities—such as real-time synchronization, behavior-based access, and cloud data governance—are seeing up to 90% productivity gains and 2.8x cost savings. Mature enterprises use identity not only for security, but also for business agility—fueling intelligent automation, streamlined onboarding, and faster decision cycles.

> "Identity has moved from a basic access control mechanism to the strategic core of digital business."

Deployment and Data Quality: The Biggest Roadblocks

Despite rising investments, only 14% of organizations report fully successful IAM deployments. Most struggle with inconsistent rollouts, data fragmentation, and limited expertise. SailPoint finds that companies prioritizing identity data hygiene before migration are 1.6 times more likely to achieve successful implementations.

Quantifying ROI: From Compliance to Growth

The report urges CISOs and CIOs to measure identity not just by risk reduction, but by business impact. Identity investments deliver the highest ROI among all cybersecurity domains—driving cost reduction, compliance, and even revenue uplift by automating processes, improving user access, and enabling faster innovation.

The Future: Adaptive Trust and Unified Governance

Looking ahead, SailPoint envisions identity as the foundation of zero trust and AI governance. Future-ready enterprises will integrate identity telemetry with security operations, automate threat response, and move toward continuous adaptive access—where every interaction is verified in real time.

In essence, The Horizons of Identity Security 2025–2026 is a wake-up call: identity is no longer just about who gets access—it's about enabling secure, intelligent, and measurable business growth in the age of AI.. ■

Building trusted digital experiences in a complex tech landscape

IN TODAY'S digital-first world, user experience has become a defining factor in how organizations serve employees and customers. Technology choices are no longer just about systems or infrastructure. They now revolve around creating secure, resilient, and seamless interactions where even small delays can erode confidence.

To deliver this consistently, organizations need clear visibility across their digital environment. When every layer of the technology stack is well understood, monitored, and secured, it becomes possible to ensure smooth experiences at every touchpoint.

Customer journeys are also becoming more complex. A single interaction can move across multiple applications, channels, and back-end processes. Keeping this effortless on the surface requires strong orchestration, disciplined processes, and the ability to maintain security and reliability at scale. When done well, it turns operational efficiency into real customer satisfaction and a genuine competitive advantage.

Artificial intelligence is accelerating this transformation. Predictive insights, intelligent automation, and personalized interactions are helping organizations anticipate needs and respond faster. At the same time, the growing use of AI highlights the importance of responsible data practices, strong governance, and secure system design to preserve trust.

Across industries, technology leaders are rethinking how digital resilience, experience management, and data-driven intelligence come together to shape their customer strategy. As expectations evolve, one principle holds true. In a digital-first world, experience is not just an outcome. It is a core element of business value and organizational credibility. ■

> "Organisations that get it right can turn operations into meaningful customer delight and a tangible competitive edge."

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 @CISO Forum

Scan the QR code to follow

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

17th Annual Conference

CISO FORUM

India's Leading Cybersecurity Summit

Thank You

for making 17th edition of The CISO Forum a Grand Success.

Our Partners

GOLD PARTNERS

kaspersky Microsoft securiti

SILVER PARTNERS

CLAROTY proofpoint. VERSA

ASSOCIATE PARTNERS

netskope SentinelOne Secure Tomorrow™

EXHIBIT PARTNERS

ANA Cyber Forensic ISO 27001:2022 Certified Company ARMIS® Barracuda. Your business, secured. Cotelligent A TechDemocracy Company

Cyber Vigilens SECURE • MONITOR • DEFEND MORPHISEC NeoSOFT®

ProTechmanize | AQUILA I AQUILA I SOPHOS | MAGNAMIOUS SYSTEMS CONNECTING AIMS TO SOLUTIONS Trellix

MEDIA PARTNER

CNBC TV18

CONCEPT BY

CISOFORUM Security For Growth And Governance

#TheCISOForum