

CIO Ledger



INDEX

AUGUST 2026 | EDITION -1 | ISSUE-2 | PAGES-28

4



AI AT SCALE:
THE CIO'S NEXT MOVE

15



**FROM CYBERSECURITY TO
CYBER RESILIENCE: THE NEW
ENTERPRISE IMPERATIVE**

10



**FROM AI HYPE TO
BUSINESS VALUE**

20

**THE HIDDEN
CYBERSECURITY RISKS
IN MODERN DATA
PLATFORMS**

26

CIO MOVEMENT

WELCOME TO CIOLEDGER

WHERE TECHNOLOGY LEADERSHIP MEETS BUSINESS STRATEGY

In every era of business, a defining force reshapes industries and technology trends. Today, that force is the convergence of Artificial Intelligence, Data, Cloud Computing, Cybersecurity, Automation, and Digital Engineering. Organizations are no longer competing solely on products or services—they are competing on turnaround time for data transformation into intelligence and intelligence into business value.

As enterprise technology writes a new chapter, the role of the Chief Information Officer(CIO) is not limited to managing technology infrastructure. Today's CIO is a leader with strategic business thinking, accountable for driving innovation, enabling growth, strengthening resilience, ensuring governance, and creating sustainable and competitive edge.

CIOLedger has been established with a singular purpose: to become the trusted knowledge platform for technology leaders navigating this transformation.

We are committed to delivering insightful, evidence-based, and vendor-neutral analysis that helps executives & leaders make informed decisions in an highly competitive digital landscape. Our mission extends beyond technology news. We decode emerging trends, evaluate enterprise technologies through a business lens, and bring practical strategies for organizational adoption.

Each edition of CIOLedger is carved to assist technology leaders:

- How Artificial Intelligence to be adopted for measurable business value?
- What defines a modern, secure, scalable, and governed data ecosystem?
- Enterprises readiness for Agent AI and autonomous operations?

- Which cloud or technology strategies maximize innovation at optimized cost?
- How can cybersecurity evolve from a defensive necessity into a strategic business enabler or accelerators?
- What leadership principles distinguish organizations that consistently outperform their competitors?

Organizations continue to face familiar challenges while technology advances — legacy modernization, fragmented data, governance, regulatory compliance, cybersecurity threats, talent shortages, and the pressure to demonstrate tangible returns on investments.

At CIOLedger, we believe successful digital transformation begins with informed leadership rather than technology adoption. Sustainable innovation is built on trusted data, responsible AI, automated and resilient architectures, disciplined governance, and a relentless focus on measurable business outcomes.

Five guiding principles aligned with our *editorial philosophy:

- Editorial Independence
- Every article is developed with objectivity and professional integrity. Editorial decisions remain independent of commercial influence, ensuring our readers receive balanced and unbiased perspectives.
- Business-First Perspective
- Technology is valuable only when it solves meaningful business problems. We evaluate innovations based on strategic impact, operational excellence, customer value, and measurable outcomes.

-Shreeti Verma

AI AT SCALE: THE CIO'S NEXT MOVE



From experimentation to execution, CIOs are under pressure to turn artificial intelligence into measurable enterprise value.

Artificial intelligence has moved beyond the innovation lab. Across industries, organisations are investing heavily in AI infrastructure, models, applications and increasingly autonomous agents. Yet the defining question for CIOs in 2026 is no longer whether the enterprise should adopt AI. It is whether AI can be scaled responsibly, economically and in a way

that produces measurable business outcomes.

The investment numbers underline the scale of the shift. Gartner forecasts worldwide AI spending to reach **\$2.59 trillion in 2026**, up 47% year on year. More than 45% of this spending is expected to go towards AI infrastructure, reflecting the enormous computing, networking and processing capacity required for emerging AI workloads.

IDC sees a similar acceleration. Its latest

research projects **\$409 billion in global IT spending on AI in 2026**, with spending expected to reach \$700 billion by 2029. IDC also estimates that around two-thirds of organisations were already using AI in live production environments at the beginning of 2026, but meaningful enterprise-wide scaling remains uncommon.

The gap between adoption and value is therefore becoming the CIO's central challenge.



From Pilots To Production

The first phase of enterprise AI was dominated by experimentation. Teams tested copilots, generative AI assistants and individual use cases, often without fundamentally changing how work was performed.

That approach is reaching its limits.

McKinsey's 2025 State of AI survey found that nearly two-thirds of respondents

had not yet begun scaling AI across their organisations. While 62% said their organisations were experimenting with AI agents, only 39% reported an enterprise-level EBIT impact from AI.

The lesson is clear: deploying AI is not the same as transforming the business with AI.

For CIOs, scaling requires moving from isolated applications to connected workflows. An AI assistant that drafts a report may improve an employee's productivity. An AI-enabled workflow that connects customer data, decision-making, compliance checks and execution can change the economics of an entire business process.

This is where the next phase of enterprise AI will be decided.

The New CIO Mandate: Build For Outcomes

AI programmes need to begin with business problems rather than technology capabilities.

A successful AI-at-scale strategy should identify where AI can materially improve revenue, customer experience, productivity, risk management or operational resilience. Every major deployment should have clearly defined success metrics before significant

resources are committed.

This is particularly important as AI costs become more visible. Gartner forecasts worldwide spending on AI models and platforms at **\$64 billion in 2026**, up 63.4% from 2025, while noting that enterprise AI budgets are coming under greater scrutiny around usage efficiency, cost control and measurable outcomes.

The CIO therefore has to manage AI not simply as an IT investment, but as a portfolio of business investments.

Infrastructure Is Only The Foundation

Scaling AI also demands a rethink of the technology stack.

IDC forecasts global AI infrastructure spending to reach **\$487 billion in 2026**, representing approximately 53% growth from the previous year, with spending expected to exceed \$1 trillion by 2029.

But more infrastructure alone will not create competitive advantage.

Organisations need reliable data pipelines, modern cloud and hybrid architectures, strong integration layers, model evaluation capabilities and observability. They must also decide which workloads belong in public cloud, private environments or increasingly specialised

AI infrastructure.

The objective should be an AI foundation that can support multiple use cases rather than a collection of disconnected technology investments.



Governance Moves From Policy To Infrastructure

As AI becomes embedded in core operations, governance can no longer remain a document produced by the compliance team.

The rise of agentic AI makes this even more important. Systems that can make decisions, access enterprise data and execute actions require controls around identity, permissions, auditability, data protection, model behaviour and human oversight.

IDC reports that enterprises now allocate an average of **16.7% of planned AI spending to AI and agent security and governance, signalling that governance** is becoming a core investment layer

rather than an afterthought.

For CIOs, responsible AI must therefore be designed into the architecture from the beginning.

People Remain The Scaling Advantage

Technology can accelerate processes, but people determine whether those processes create value.

AI adoption changes job responsibilities, workflows and required skills. PwC's 2026 Global AI Jobs Barometer found that productivity growth is **40% higher in companies most exposed to AI** than in those least exposed. It also found that skills requirements for the most AI-exposed jobs are changing more than twice as quickly as those for the least exposed roles.

This makes workforce transformation a core CIO responsibility.

The organisations that gain the most from AI are unlikely to be those that simply automate the greatest number of tasks. They will be those that redesign work around a combination of human judgement, domain expertise and machine capability.

Training, change management and new operating models should therefore sit

alongside infrastructure and software on the AI roadmap.



The Move From Assistant To Agent

The next major shift is from AI that assists employees to AI that can execute defined tasks across workflows.

Agentic AI has the potential to connect systems, interpret information, make decisions within defined boundaries and initiate actions. IDC expects agentic systems to account for nearly half of AI spending by 2029, highlighting how quickly the enterprise AI stack is evolving.

But CIOs should resist the temptation to deploy agents simply because the technology is available.

The strongest starting point is a high-volume, well-defined process where the organisation can establish clear boundaries, measure performance and maintain human oversight. Scaling

should follow demonstrated value, not technology enthusiasm.



What CIOs Should Do Now

The AI-at-scale agenda can be distilled into five priorities:

1. **Start with value.** Tie every major AI initiative to a measurable business outcome.
2. **Build a reusable foundation.** Invest in data, integration, infrastructure, security and AI platforms that can support multiple use cases.
3. **Redesign workflows.** Do not simply add AI to existing processes; rethink how work should be performed.
4. **Make governance continuous.** Embed security, risk management, evaluation and human oversight into the AI

lifecycle.

5. **Prepare the workforce.** Build AI literacy while strengthening the human skills that become more valuable as automation increases.

The Next Competitive Divide

The AI race is entering a more demanding phase. The winners will not necessarily be organisations with the largest models or the biggest technology budgets. They will be organisations capable of repeatedly converting AI investment into better decisions, faster operations, stronger customer experiences and new sources of growth.

The evidence already points towards this transition. IDC projects that AI could generate **\$22.5 trillion in cumulative economic value between 2025 and 2031**, while warning that the opportunity depends on organisations overcoming gaps in maturity, governance and measurable business outcomes.

For CIOs, this changes the role of AI from an innovation programme into an enterprise operating priority.

The next move is not to deploy more AI.

It is to scale the right AI, across the right workflows, with the right controls—and prove that it creates value.

ADVERTISE WITH US

- CONNECT
- INFLUENCE
- GROW

Promote your brand through CIO Ledger and reach a highly engaged audience of business leaders, entrepreneurs, and industry professionals.

Start your advertising journey with us today.



+91 9599522011



cioledger@gmail.com



FROM AI HYPE TO BUSINESS VALUE



Why the CIO's 2026 mandate is shifting from AI experimentation to measurable enterprise impact.

Artificial intelligence has crossed the adoption threshold. The harder challenge now is proving that the investment is creating business value.

Global AI spending is forecast to reach **\$2.52 trillion in 2026**, a 44% year-on-year increase, according to Gartner. Yet Gartner's research also points to a more pragmatic phase of AI adoption, where

organisations are increasingly demanding predictable outcomes and clearer returns before scaling further.

This marks an important change for CIOs. The question is no longer ***"What can AI do?"*** but ***"Where can AI create measurable value for our business?"***

The ROI Reality

AI adoption is widespread, but enterprise-level impact remains uneven.

McKinsey's 2025 global survey found that nearly two-thirds of organisations had not yet begun scaling AI across the enterprise. While 62% were experimenting with AI agents, only 39% reported any enterprise-level EBIT impact from AI.

The message for technology leaders is straightforward: a successful pilot is not necessarily a successful business transformation.

The gap often emerges between demonstrating that an AI system works and redesigning the surrounding process so that the organisation can actually capture its benefits.

From Pilots To Business Outcomes

The next phase of AI adoption will require CIOs to become **value orchestrators**, connecting technology investments with strategic business priorities.

Gartner recommends moving towards a structured approach that prioritises AI use cases according to business value and feasibility, establishes clear value metrics and continuously tracks whether AI initiatives are delivering their intended outcomes. Gartner also notes that CIOs should look beyond the technology itself and consider the organisational and behavioural changes required to sustain value.

This means an AI project should not begin

with a model. It should begin with a business problem.

Is the objective to reduce processing time? Improve customer retention? Increase sales conversion? Detect fraud earlier? Accelerate software development?

Improve decision-making? Once the outcome is defined, technology becomes an enabler rather than the destination.



The Cost Of Scaling

The economics of AI are also becoming more complex.

IDC forecasts **\$409 billion in global AI spending in 2026**, with spending expected to reach \$700 billion by 2029. At the same time, IDC warns that many organisations are struggling to move

from targeted deployments to broad operationalisation, with unclear business benefits and weak data foundations remaining significant barriers.

For CIOs, this makes AI economics a board-level issue.

The cost of models, cloud infrastructure, data preparation, integration, cybersecurity, talent and ongoing inference must be measured against the value generated. A use case that looks inexpensive during a pilot can have a very different cost profile once deployed across thousands of employees or millions of customer interactions.

The new discipline is therefore **AI unit economics**: understanding what each AI-enabled process costs and what measurable value it generates.



Data Is The Differentiator

The quality of an AI strategy is ultimately constrained by the quality of the data

supporting it.

Enterprises may have access to powerful foundation models, but fragmented, outdated or poorly governed data can undermine their effectiveness. IDC describes a growing “intelligence gap” between the speed at which AI-driven decisions need to be made and the quality of verified intelligence available to support those decisions.

This places data governance, architecture and integration firmly on the CIO agenda.

The organisations most likely to extract sustained value will not necessarily be those with access to the most sophisticated model. They will be those that can connect trusted enterprise data to the right workflows while maintaining security, compliance and governance.

Redesign The Workflow, Not Just The Tool

AI creates limited value when it is simply added on top of an inefficient process.

McKinsey’s research shows that organisations seeing greater value from AI are more likely to redesign workflows and pursue broader business transformation. Its 2025 survey found that only around 7% of respondents reported that AI had been fully scaled across their organisations.

This is where the CIO’s role becomes

more strategic.

Instead of asking employees to use another AI tool, organisations need to rethink how work gets done. Human judgement, AI assistance and increasingly autonomous agents should be combined into redesigned operating models.

The objective is not simply automation. It is ***better work, faster decisions and stronger business outcomes.***



The Human Equation

Technology alone cannot deliver AI transformation.

Gartner estimates that by 2030, 75% of IT work will be performed by humans working with AI, while 25% will be performed by AI alone. The research

highlights the importance of balancing AI readiness with human readiness.

That makes workforce transformation a core component of AI strategy.

Employees need more than access to AI tools. They need training, clear operating guidelines and confidence about where human judgement remains essential. Managers also need to understand how performance metrics, roles and responsibilities change when AI becomes part of everyday work.

The New AI Scorecard

Traditional technology metrics such as adoption, licences and system availability are no longer sufficient.

CIOs should build AI scorecards around business outcomes:

- **Revenue:** What new revenue or growth has AI enabled?
- **Productivity:** How much time or effort has been eliminated?
- **Customer:** Has satisfaction, retention or response time improved?
- **Risk:** Has AI reduced errors, fraud or operational exposure?
- **Cost:** What is the total cost per AI-enabled transaction or workflow?

- **Innovation:** Has AI accelerated new products or services?

Deloitte's 2025 research illustrates why this discipline matters. Its survey found that 85% of organisations increased AI investment over the previous 12 months, yet most respondents reported that satisfactory ROI from a typical AI use case could take two to four years. Only 6% reported payback within a year.

Investment is accelerating. Value realisation must accelerate with it.

From Hype To Advantage

The AI conversation is entering a more mature phase. The early race was about experimentation and access. The next race will be about execution.

CIOs who continue to measure success by the number of pilots launched may find themselves with a large AI footprint but limited business impact. Those who build disciplined portfolios around measurable

outcomes can turn AI from an expensive technology programme into a strategic growth engine.

The opportunity is significant. IDC estimates that AI could generate **\$22.5 trillion in cumulative economic value between 2025 and 2031**, driven by productivity gains and workforce transformation. But realising that opportunity depends on organisations closing the gap between investment and execution.

The mandate for CIOs in 2026 is therefore clear:

Stop measuring how much AI the organisation has adopted. Start measuring how much value it creates.

AI will eventually become embedded in the technology estate. The competitive advantage will belong to enterprises that embed it into the way they create, deliver and capture value.



FROM CYBERSECURITY TO CYBER RESILIENCE: THE NEW ENTERPRISE IMPERATIVE



Why enterprises are shifting from preventing every attack to ensuring they can withstand, recover from and continue operating through disruption.

Cybersecurity has traditionally been built around a simple objective: keep attackers out. But as digital ecosystems become more interconnected and threats become faster, more adaptive and increasingly

AI-enabled, prevention alone is no longer enough.

For CIOs and CISOs, the strategic question is changing from “Can we stop the attack?” to “Can the business continue if the attack succeeds?”

That shift is driving the move from cybersecurity to cyber resilience.

Beyond The Perimeter

Modern enterprises operate across cloud platforms, SaaS applications, remote endpoints, third-party ecosystems and increasingly autonomous AI systems. This has made the traditional security perimeter far less meaningful.

Gartner's 2025 cybersecurity research identifies resilience as a central priority for security leaders, alongside the challenges created by generative AI, expanding cloud adoption, regulatory requirements and persistent talent shortages.

The implication is significant: security can no longer operate as an isolated technical function. It must become part of business continuity and operational strategy.

Assume Breach, Prepare To Recover

Ransomware illustrates the limitation of a prevention-only approach. Even organisations with mature security controls can face compromised credentials, exploited vulnerabilities or attacks through suppliers.

Gartner's research on ransomware resilience emphasises the importance of secure recovery environments, while its 2025 research warns that conventional disaster-recovery strategies may not

be sufficient for modern ransomware incidents.

Cyber resilience therefore requires organisations to prepare for the moment when prevention fails.

That means maintaining clean and recoverable data, isolating critical systems, testing recovery procedures and establishing clear business priorities for restoring operations.



Recovery Is A Security Capability

Recovery is often treated as an IT continuity issue. It increasingly needs to be treated as a security capability.

IDC research highlights the financial and operational consequences of

ransomware, including downtime, productivity losses, reputational damage and regulatory exposure. Its research also points to the importance of clean, redundant and immutable backups because attackers frequently attempt to compromise or destroy recovery data. For CIOs, this changes the architecture of resilience.

Backups cannot simply exist.

Organisations must know whether they are clean, whether they can be restored and how quickly critical applications can return to service.

Recovery time is now a security metric.

The Cost Of Downtime

The business case for resilience is becoming harder to ignore.

IBM's 2026 Cost of a Data Breach research puts the global average cost of a data breach at **\$4.99 million**, while breaches involving AI-enabled attacks are increasingly adding complexity and cost. IBM reported that one in four malicious breaches in its 2026 study were AI-enabled, with those incidents costing an average of **\$6 million**.

The Indian picture is equally significant. IBM's 2026 research puts the average cost of a data breach in India at **₹25.5 crore**,

up 15.9% from ₹22 crore in 2025.

These figures demonstrate why resilience should not be viewed simply as another cybersecurity expenditure. It is an investment in protecting revenue, customer trust and operational continuity.



AI Changes The Risk Equation

Artificial intelligence is creating a dual challenge.

Enterprises are embedding AI into applications and workflows while attackers are using the same technology to improve phishing, impersonation, malware and social engineering.

IBM's 2026 research found that **26% of malicious breaches in India were AI-generated**.

This makes AI governance inseparable from cyber resilience. Organisations need visibility into AI assets, appropriate access controls, secure data pipelines and mechanisms to detect abnormal behaviour.

The objective is not to slow AI adoption. It is to ensure that AI becomes part of the enterprise's secure operating model.



Designing For Resilience

A resilient enterprise needs several capabilities working together:

- **Identify:** Understand critical assets, dependencies and risks.
- **Protect:** Secure identities, endpoints, applications, data and infrastructure.
- **Detect:** Identify suspicious activity quickly.
- **Respond:** Contain incidents without

unnecessarily disrupting operations.

- **Recover:** Restore trusted systems and data rapidly.
- **Learn:** Convert every incident into stronger controls and processes.

This approach moves security from a defensive perimeter into a continuous organisational capability.

The CIO's New Scorecard

Cybersecurity performance has traditionally been measured through indicators such as vulnerabilities patched, incidents detected and compliance requirements met.

Cyber resilience demands broader metrics.

CIOs should also measure:

How quickly can critical services be restored?

How much business can continue during an attack?

Can the organisation recover without relying on compromised infrastructure?

How frequently are recovery plans tested?

How quickly can teams make decisions during a crisis?

These measures connect cybersecurity directly to business performance.



Resilience As Competitive Advantage

The objective of cyber resilience is not to promise that an organisation will never be breached. That is increasingly unrealistic. The objective is to ensure that an incident does not become a business-ending event.

Organisations that can detect attacks early, contain damage, recover trusted systems and maintain essential services will be better positioned to withstand disruption than those focused exclusively on prevention.

For CIOs, the strategic shift is therefore clear: ***cybersecurity protects the enterprise from threats; cyber resilience prepares the enterprise to keep moving when threats get through.***

In an environment where disruption is no longer a possibility but an operational reality, resilience is becoming the more meaningful measure of security maturity.

CONTRIBUTE TO THE CIO LEDGER UPCOMING EDITION

A great opportunity to share your expertise with the global technology leadership community!

You're invited to contribute an article, interview, case study, thought leadership piece

WRITE TO US:
cioledger@gmail.com

THE HIDDEN CYBERSECURITY RISKS IN MODERN DATA PLATFORMS

Author by

Ramesh Raju C

Technology Advisor &

Enterprise Architect

What every CIO, CTO, and Enterprise Architect should know - before an attacker does

Executive Summary

Organizations spend millions securing networks and endpoints. Yet the most dangerous exposures today live inside data pipelines — invisible to traditional security tools.

The six biggest blind spots:

- Excessive service account privileges
- Unsecured Kafka & streaming
- Data lakehouse misconfigurations
- Shadow data pipelines
- AI-driven data leakage
- Missing data lineage

The Core Problem

Why data engineering is security's new blind spot

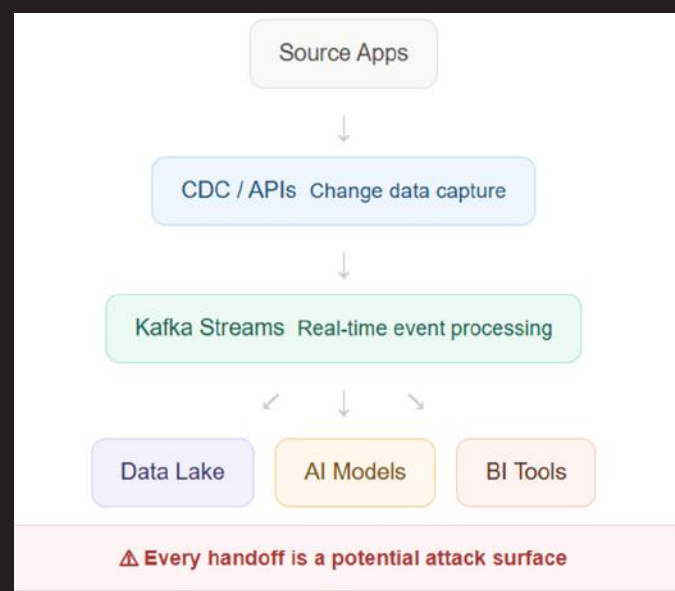
Traditional security was built around clear network boundaries — firewalls, monitored servers, tightly controlled access. Today's enterprise looks nothing like that.

A modern data platform connects cloud storage, data lakes, Kafka streams, CDC systems, ETL pipelines, AI models, SaaS APIs, and BI tools. Data flows constantly between all of them. ***Every handoff is a potential attack surface.***

The core mistake

Organizations invest heavily in data innovation while assuming traditional security controls automatically extend to modern architectures. They do not.

Diagram 1 — Modern Data Engineering Attack Surface



The Six Risks:

What attackers are already targeting

1. Service accounts with excessive privileges - Critical

Data pipelines run on service accounts — not human users. These accounts often carry database admin rights, broad cloud storage access, and long-lived credentials. Because they operate silently in the background, they escape regular access reviews.

Compromising one service account can expose the entire enterprise data platform — without triggering a single user-based security alert.

- Least-privilege access
- Auto-rotate credentials
- Continuous monitoring
- Eliminate hardcoded secrets

2. Unsecured data streaming platforms - Critical

Platforms like Apache Kafka process millions of events in real time. Most implementations prioritise speed over security — leaving weak authentication, overly permissive topic access, and unencrypted data transmission as standard issues.

A compromised streaming platform exposes customer data, financial transactions, and operational metrics — and can cascade

across dozens of downstream systems.

- Strong auth on all topics
- Encrypt in transit
- Segregate environments

3. Data lake and lakehouse misconfigurations - High

Cloud data lakes offer scale and flexibility — but governance rarely keeps up. Excessive storage permissions, misconfigured bucket policies, and missing encryption mean sensitive records are often accessible far beyond their intended audience.

As data volumes grow, visibility decreases. This is the perfect environment for insider threats and silent data exposure.

- Data classification
- Audit logging
- Bucket policy review

4. Shadow data pipelines - High

Most CIOs know about Shadow IT. Far fewer track Shadow Data Engineering — business teams quietly building their own API integrations, self-service pipelines, and spreadsheet-based automation outside of any security review.

These pipelines move sensitive data through systems that have never been assessed for risk. Traditional security programs rarely detect them.

- Discovery scanning
- Data governance policy
- Integration registry

5. AI and machine learning data exposure
- Critical

Generative AI adoption has introduced a new category of data risk. Teams focus on model performance while overlooking what data is being fed in — and whether third-party AI providers are retaining it.

Ask your teams now:
What data trains our models? Is sensitive information exposed? Can proprietary data be extracted from model outputs?

- AI data inventory
- Third-party data contracts
- Model access governance

06. Weak data lineage and visibility - High

When a breach occurs, most security teams

spend the first hours simply figuring out what was exposed. Without data lineage, incident response is slow and incomplete.

If your team cannot answer “where did this data come from, who touched it, and who can see it now?” — you cannot respond effectively to a breach.

- #End-to-end lineage
- #Data observability
- #Access audit trails

Security Maturity

Where most organisations are — and where attackers strike

Most enterprises have moved through infrastructure and application security. Cloud security is now maturing. But data security and AI governance — the layers where modern attacks concentrate — remain largely undeveloped.

Diagram 2 — Security Maturity Model



The maturity gap is the attack window.
While most organisations secure Levels 1–3, the most valuable enterprise data sits at Levels 4 and 5 — largely unprotected.

CIO Action Checklist

What to do now

Designed for immediate sharing with your security, data, and architecture teams.

Priority	Action	Category
High	Audit all service accounts — review permissions, rotate credentials, eliminate hardcoded secrets	Identity
High	Review Kafka and streaming platform security — auth, encryption, topic access	Streaming
High	Validate data lake permissions — bucket policies, encryption, classification	Storage
High	Establish AI governance — data inventory, third-party contracts, model access controls	AI
Medium	Implement data lineage and observability across all pipeline stages	Visibility
Medium	Conduct shadow data pipeline discovery — scan for unapproved integrations	Governance
Medium	Review third-party SaaS integrations and API access scopes	3rd Party

Strategic Recommendations

Seven actions for technology leaders

1	Adopt data-centric security Protect the data itself, not just the infrastructure around it.	3	Strengthen identity governance Apply strict controls to service accounts, APIs, and applications.
2	Implement Zero Trust for data Verify every access request regardless of location or user type.	4	Invest in data lineage Gain full visibility across every stage of the data lifecycle.

5	Secure streaming architectures Treat event streams as critical enterprise assets — not utilities
6	Establish AI governance early Embed security controls into every AI initiative from day one.
7	Align security, data, and architecture teams Cybersecurity can no longer operate as a separate function. Data engineering and security must plan together from the very start.

The bottom line:

The most successful organisations will be those that integrate cybersecurity directly into their data architecture strategy — not as an afterthought, but as a founding principle.

Ramesh Raju Ch

Technology Advisor and Enterprise Architect specialising in cybersecurity, enterprise architecture, cloud transformation, data platforms, and AI governance. He helps organisations build secure, scalable, and resilient technology ecosystems while driving digital transformation and business innovation.

CONTRIBUTE TO THE CIO LEDGER UPCOMING EDITION

A great opportunity to share your expertise with the global technology leadership community!

You're invited to contribute an article, interview, case study, thought leadership piece

WRITE TO US:
cioledger@gmail.com

SPAN Inspection Systems Names Gaurav Vyas as New Chief Information Officer



SPAN Inspection Systems Pvt. Ltd. has designated Gaurav Vyas as Chief Information Officer (CIO) of the firm, in a strategic move to bring a technology expert with a strong

track record in digital transformation, IT infrastructure, enterprise applications and cybersecurity into its leadership team.

An experienced technology leader, Gaurav Vyas brings a strong track record in IT management, strategic planning, and digital transformation. He has expertise in cybersecurity, IT infrastructure, network management, cloud computing, and the implementation of technology best practices aimed at improving operational efficiency and strengthening cybersecurity resilience. Known for his strong leadership and communication skills, Vyas focuses on building high-performing teams and delivering technology solutions that support business growth and long-term organisational goals.

Vishal Rathod Joins as AMFI's Chief Technology Officer (CTO)



The Association of Mutual Funds in India (AMFI) has chaired Vishal

Rathod as its

Chief Technology Officer (CTO), in a strategic move to strengthen its technology leadership in a progressing mutual fund industry, aiming to get an edge on digital platforms, Vishal Rathod cybersecurity cloud infrastructure, and technology-based regulatory frameworks.

Vishal Rathod is a seasoned leader with over two decades of experience in IT leadership, and has expertise in driving digital transformations across NBFC and Banking sectors. He possesses a passion about augmenting cutting-edge technology with strategic business goals, fostering innovation, and championing robust cybersecurity measures to drive sustainable growth.

Birlasoft Chairs Krishna Thiagarajan as its Senior Vice President & Global Head of Data & AI

Birlasoft has designated Krishna Thiagarajan as its Senior Vice President & Global Head of Data & AI, as a strategic decision to strengthen its focus on fastest-growing area of technology industry. In this role, Mr. Thiagarajan will bring along extensive experience across analytics, data, artificial intelligence (AI), generative AI (genAI), technology advisory and digital transformation to firm's global Data & AI initiatives.

Krishna brings extensive leadership experience from a career spanning multiple leading technology companies. Before joining Birlasoft, he served in senior positions at Virtusa, Tech Mahindra, NTT DATA and Satyam Computer Services, Infosys, Compuware, and other multinational companies at senior positions, where he focused on driving data-led transformation initiatives and building and scaling technology capabilities across organisations.



Swiggy Reshuffles Leadership With Appointment Of New CTO, CGPO & COO

Swiggy has reshuffled the leadership of its Food Marketplace and Instamart businesses, appointing three senior executives to key roles.

Himavant Kurnala has become Chief Growth & Product Officer

at Instamart, Saurav Goyal has been named COO of the Food Marketplace, and Nitesh Garg has taken charge as CTO of Instamart. The changes follow several recent

leadership appointments, including Nandita Sinha as CEO and Gautam Swaroop as CBO of Instamart. Swapnil Bajpai was also elevated to CEO of Dineout & Scenes. Kurnala has led Instamart's product since 2024, Garg has been with Swiggy for over seven years, and Goyal joined in 2020.



Himavant Kurnala



Saurav Goyal



Nandita Sinha

Lohia Corp Appoints Jagdip Kumar as Chief Digital & Information Officer



Lohia Corp Limited has elevated Jagdip Kumar from Chief Information Officer (CIO) to Chief Digital & Information Officer (CDIO), strengthening its

digital and technology leadership. The expanded role reflects the company's increasing emphasis on digital transformation, artificial intelligence, data-driven innovation and technology-led growth. As CDIO, Kumar will oversee a broader enterprise-wide digital strategy, moving beyond traditional IT operations. His responsibilities will include driving AI and GenAI adoption, enabling data-driven decision-making, enhancing digital experiences and supporting technology-led business transformation. The elevation underscores Lohia Corp's focus on leveraging emerging technologies to improve business agility, innovation and long-term competitiveness.

CONTRIBUTE TO THE CIO LEDGER UPCOMING EDITION

A great opportunity to share your expertise with the global technology leadership community!

You're invited to contribute an article, interview, case study, thought leadership piece

WRITE TO US:
cioledger@gmail.com

ADVERTISE WITH US

- CONNECT
- INFLUENCE
- GROW

Promote your brand through CIO Ledger and reach a highly engaged audience of business leaders, entrepreneurs, and industry professionals.

Start your advertising journey with us today.



+91 9599522011



cioledger@gmail.com