ManageEngine

VOICES, VISIONS, AND VICTORIES OF IT LEADERS

CIO Compass 2026

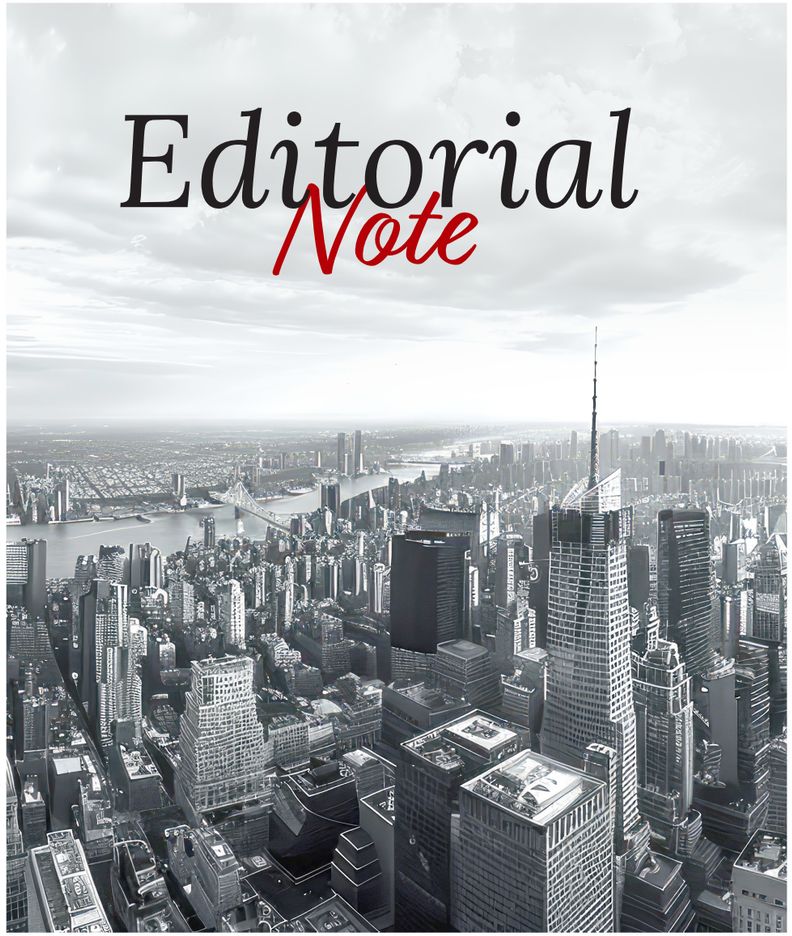
WHERE TECHNOLOGY MEETS LEADERSHIP

IDEAS, STRATEGIES, AND STORIES FROM **PEERS WHO LEAD**

ManageEngine

THIS IS AN

Editorial Note



FOR A MAGAZINE FOCUSED ON IT LEADERS

In the world of enterprise technology, we often speak in terms of systems, architectures, and frameworks. But the real story has always been about people—the leaders who hold the burden of decisiveness when the landscape shifts without warning. The pivots made in this space influence growth trajectories, shape organizational trust, and increasingly determine competitive advantage. This reality calls for leaders who make decisions that protect not just their organization's infrastructure, but reputation, culture, and continuity. This magazine is created for those decision-makers.

Within these pages, you'll find perspectives that move beyond surface-level commentary. There are stories of transformation—organizations that redefined their trajectory and the leadership mindsets that made that possible. There are explorations of cyber risk, identity, and data integrity, not merely as technical concerns, but as strategic imperatives that demand attention at the executive level.

Woven through the issue are thoughtful examinations of the vulnerabilities that warrant board-level focus, the governance frameworks that must evolve, and the strategic clarity required to make security a business enabler rather than a constraint. Alongside these discussions are insights from CIOs who are shaping culture, guiding innovation, and redefining what it means to lead in a world where technology decisions increasingly influence enterprise direction. Their perspectives serve as a reminder that today's technology leaders are not merely operators; they are stewards of continuity and architects of long-term value. Throughout this issue, we've also included lighter touchpoints to serve as reminders that curiosity and creativity remain essential tools in a leader's arsenal.

This issue is a companion for decision-makers—intended to equip, challenge, and sharpen—while reinforcing a central truth: the enterprises that will lead the next decade are those that treat technology decisions as business decisions, and security as a strategic pillar, not an operational afterthought. My aspiration is that this issue offers perspective that resonates not just with your expertise, but with the decisions you carry into the boardroom each day.

Jenny Suzanna J

Head of Enterprise Business and Strategy
ManageEngine

TABLE OF *Contents*



The big picture

From a telecom niche to an IT powerhouse: The ManageEngine evolution 04

Our commitment to cybersecurity 08



Shaping the future

Defining the CIO's next move 06

Leadership lens 10



Tech unwind

A day in a CIO's life 14

The curious case of Nyx Technology 15

Crossword challenge 20

CIO happiness index 21

Ready for a brain workout? 21

CIO archetypes 28

The secret life of a service account 34

Decoded: The answers you've been looking for 38



Resilience in action

How to make cyber risk matter in the boardroom 16

The business cost of fragmented identity architectures 22

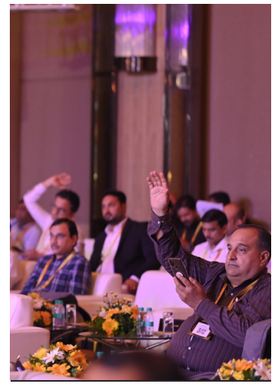
The DNA of DPDP compliance: Shaping trust through law and leadership 26



Risk made real

The Easter weekend breach: What CISOs can learn from M&S 18

Data under siege: Building cyber resilience in modern healthcare 24



From the front lines

Memory bytes: CIO Connect 30

From friction to focus: How leading enterprises have mastered identity management and IT security 36

The Strategy Seat: Tech talks for shaping the future 39



From a telecom niche to an IT powerhouse:

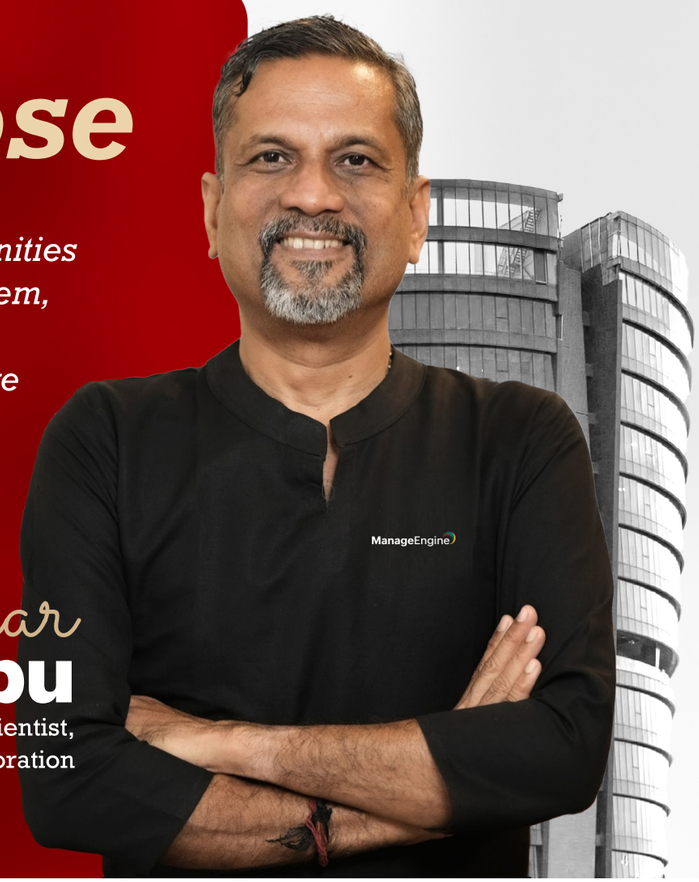
The ManageEngine evolution

Our purpose

has been to create opportunities for those who don't have them, build compelling products for our customers, and serve geographical locations that have not been served before.

Sridhar **Vembu**

Co-founder and Chief Scientist, Zoho Corporation



Our story

The foundation

Founded in 1996, when the internet was still emerging, Advent Network Management Inc. focused on delivering Java SNMP APIs and network management software for the telecommunications industry. Over the next two years, we expanded our expertise and in 1998 launched our first major product, WebNMS, which offered OEM solutions such as protocol adapters, software agents, and test and simulation toolkits. Our products solved real problems for a rapidly growing industry. Growth was strong, the market was booming, and our future looked secure—until everything changed.

The re-invention

In the late 1990s, internet startups surged with abundant funding and sky-high ambitions. Telecom manufacturers, fueled by this optimism, poured billions into fiber optics, network switches, and wireless infrastructure. The boom felt endless until it wasn't. By mid-2001, the dot-com bubble burst and wiped out most venture-backed firms through overspending and speculative investments. For AdventNet, the fallout was swift and severe. We lost most of our customers, and our market collapsed. Confronted with this crisis, we faced a choice: cling to a shrinking niche or reinvent ourselves. Leadership chose transformation, diversifying our technology to serve all businesses needing IT management.

Building for IT leaders

What we carried from those early years proved invaluable: deep technical expertise in network management, strong research and development capabilities, and a clear understanding of how complex systems should be monitored and managed. These strengths weren't limited to telecom; they were universal. Every enterprise faced the same challenge: managing growing IT complexity reliably and securely. This insight reshaped us. We began creating solutions for the broader enterprise IT market. We evolved from a niche vendor into a platform company—built for scale, resilience, and innovation.

ManageEngine now

Today, the ManageEngine platform supports IT operations for over 280,000 customers through 60+ enterprise IT solutions. With more than 12,000 employees, our mission remains the same: help IT leaders manage complexity, mitigate risk, and achieve operational excellence. Over the years, we've learned that enterprise IT does not have a one-size-fits-all approach. Today, as C-level executives and IT leaders navigate unprecedented complexity across hybrid environments, that same principle endures: listen to customers, invest in technology, and deliver measurable value in the real world, and not just in theory. Our platform empowers IT leaders to manage complexity with confidence and align technology with long-term business goals.

"It was never about building 90 products —it was about finding the right problem to solve for the market, for the customers."

Rajesh **Ganesan**

CEO, ManageEngine



"We are like a one-stop shop—whatever the IT management needs, we'll be there. From IT service management all the way up to IT security."

Shailesh **Kumar**

CEO, Zoho Corporation



DEFINING THE CIO'S NEXT MOVE

The CIO's responsibilities have evolved far beyond simply keeping systems running. Today's CIO is a catalyst for change, a guardian of trust, and a driver of growth. True impact doesn't come from adopting every technology trend—it comes from choosing the right tools and aligning them with real business goals.

3 CIO reflections for 2026

1 What's the one AI risk that isn't being talked about enough inside your boardroom?

2 Can your organization recover from a cyberattack faster than the headlines hit?

3 Are your teams building the future—or maintaining the past?



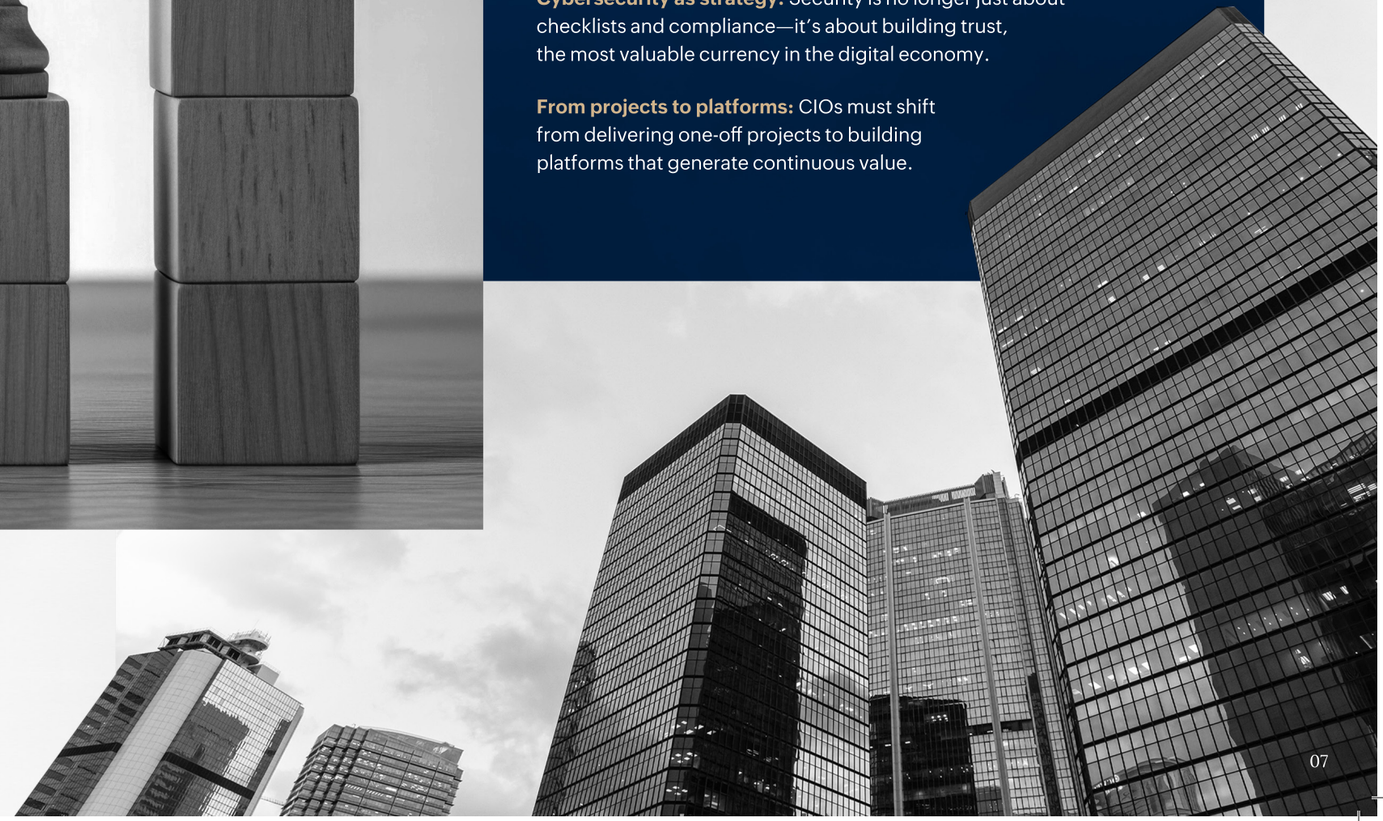
CIOs DON'T JUST PREDICT THE FUTURE —THEY PROTOTYPE IT.

For years, IT was seen as a support function. In 2026, technology is the business. CIOs are now shaping revenue, strengthening resilience, and influencing culture across the organization.

AI as a growth engine: AI is no longer just automating tasks. It's enabling new business models and unlocking opportunities once beyond our reach.

Cybersecurity as strategy: Security is no longer just about checklists and compliance—it's about building trust, the most valuable currency in the digital economy.

From projects to platforms: CIOs must shift from delivering one-off projects to building platforms that generate continuous value.



Our commitment to **cybersecurity**

"Continuing our tradition of prioritizing privacy and security, we're integrating our in-house Zia AI to transform enterprise security operations to deliver smarter detection, faster response, and greater resilience. By combining proactive and risk-based security with enhanced scalability and interoperability, we plan on ensuring our security platform adapts seamlessly to the evolving needs of enterprises across industries."



Manikandan Thangaraj
Vice President, ManageEngine

Cybersecurity today is not just about protecting systems. It is about preserving credibility, the trust that connects businesses with their customers, partners, and people. For ManageEngine, that trust is our foundation. We have always believed that security is not a single solution, but a journey that evolves with every new challenge the digital world brings.

Over the years, we have strengthened this commitment through continuous innovation, close collaboration with enterprises, and an unwavering focus on understanding how technology and risk intersect. Our roadmap reflects that spirit of evolution, adapting to the pace of modern business while keeping security at its core.

INNOVATING FOR A *Secure* TOMORROW

Evolution of our IAM and SIEM suites over the years

2005
Centralized log management

2006
AD management and reporting

2007
AD self-service management

2009
AD auditing and reporting

2010
Exchange auditing and reporting

2013
Unified identity and access management

2015
Enterprise backup and recovery

2016
Unified SIEM with DLP and CASB

2017
Cloud security management

2022
Birth of MSSP editions

2023
Cloud-based IAM platform

Our journey began with a simple mission: to help organizations gain control of their digital environments. As enterprises expanded, their digital ecosystems became more complex, with growing numbers of users, applications, devices, and points of vulnerability. We focused on helping IT teams manage access intelligently, automate routine tasks, and gain a clear, unified view of who has permission to access what, ensuring that security becomes easier to implement and harder to compromise. We also understand that prevention alone is not enough. Modern enterprises need deep visibility into what is happening across their systems, early detection of unusual behavior, and the agility to respond before a risk turns into a breach. Our analytics-driven security solutions bring these capabilities together by consolidating event data, correlating behavior patterns, and highlighting threats that would otherwise remain unnoticed. Through user and entity behavior analytics, we help organizations strengthen their posture and move from reactive defense to a proactive, intelligence-led approach to security.

Today, more than 280,000 organizations worldwide trust ManageEngine to secure their digital ecosystems. From financial institutions and healthcare providers to government agencies and technology companies, our solutions help protect the systems that drive innovation and growth.

Trusted By

IBM · Disney · hp · EY · NASA · TOSHIBA Leading Innovation

Our commitment to security goes beyond building robust technology. We cultivate a culture where compliance and accountability are part of daily operations. Routine audits, continuous assessments, and adherence to globally recognized security and privacy standards ensure that we not only meet industry benchmarks, but also uphold the highest levels of trust and integrity.

Our Certifications

PRIVACY FEEDBACK Powered by TRUSTe · AICPA SOC · GDPR · CCPA · STAR LEVEL ONE · bsi ISO/IEC 27001 Information Security Management CERTIFIED IS 642819 ISO/IEC 27001

What drives us forward is our community. The insights of CIOs and IT leaders guide our roadmap and keep our solutions aligned with real-world challenges. Through ongoing conversations and initiatives like CIO Connect, we continue learning from those leading digital transformation.

As the threat landscape grows more complex, our promise remains the same: to innovate, evolve, and partner with enterprises to strengthen their resilience. Cybersecurity is not just a feature we deliver, it is a responsibility we share.

Leadership lens

In this special edition, we shine a light on the brightest minds within our CIO community: leaders who are shaping the future of technology with vision, resilience, and heart. We asked them a range of questions that offer a closer look at the people behind the role and the perspectives that influence how they lead. Their insights reflect not only deep expertise but also the values and experiences that guide their decisions every day. With each perspective, this feature celebrates the depth, diversity, and spirit of a community that continues to inspire progress across industries.

Q. What's a CIO myth you've heard that you've found isn't true?

A common myth is that CIOs spend most of their time experimenting with cutting-edge tech, as if we're running a futuristic gadget lab. Reality is far less cinematic. Most days are about translating business needs into something technology can actually deliver while ensuring the wheels don't come off in the process. We're part negotiator, part strategist, and part advisor. The idea that a CIO can just upgrade the system overnight is charming, but it's also spectacularly untrue. If anything, the real magic trick is keeping innovation moving forward without breaking what already works. Anyone who's lived through a major migration knows: Stability is the unsung hero, not the myth.



Hilal Ahmad Lone
CISO & VP
Liminal Custody

Q. If you had a magic wand to fix one recurring IT challenge instantly, what would it be?

I would permanently close the gap between technology execution and business expectations. Even with rapid digital adoption, IT is still largely judged on stability, cost control, and delivery timelines, while the business looks to technology for speed, insight, and innovation. This disconnect often leads to friction, rework, and lost opportunities.

Bridging this gap means building systems that are adaptive by design; data platforms that provide real-time, decision-ready insights; and security that is seamlessly embedded into everyday operations. IT should function as a strategic partner, not just a service provider, anticipating business needs, enabling growth, and converting technology into tangible outcomes. When this alignment is achieved, technology becomes an invisible yet powerful driver of trust, agility, and competitive advantage.



Sanjay Jaiswal
Deputy VP
ISG Application & Network Security,
Nuvama Group

Q. How did you balance human intuition versus automated systems in key decisions this year?

As a CTO, I believe the right balance between human intuition and automation comes from clarity of ownership and trust in people. Automated systems played a critical role in providing real-time insights, risk indicators, and performance metrics, enabling faster and more informed decisions. However, leadership judgment remained central for strategic priorities, cultural alignment, and long-term technology vision. I followed a human-in-the-loop approach, where automation augmented decision-making but did not replace accountability. By empowering teams with data while preserving human oversight, we ensured decisions were not only efficient but also responsible, ethical, and aligned with business outcomes.



Gaurav Mishra
CTO
Bluspring Enterprises Limited

Inside the minds shaping tomorrow's enterprises

Q. How do you balance long-term strategy with the urgency of day-to-day crises?

Balancing long-term strategy with day-to-day operational urgency requires discipline, structure, and clear ownership. With over 30 years of experience across global manufacturing, SAP environments, and Industry 4.0 ecosystems, I have learned that the key lies in creating a governance model that protects strategic priorities while ensuring high responsiveness to immediate risks.

My approach begins with empowering strong operational teams who manage incidents, cybersecurity alerts, and production system stability, allowing me to remain focused on transformation initiatives such as S/4HANA migration, cloud modernization, automation, and digital transformation. At the same time, I apply strict prioritization frameworks to distinguish between truly business-critical issues and noise, ensuring rapid response without derailing long-term goals.

Every crisis is treated as a source of insight, often revealing process gaps, vulnerabilities, or technical debt, which I incorporate back into strategic planning. This dual mindset enables organizations to remain resilient, maintain innovation momentum, and continue progressing toward a future-ready digital enterprise.



Ajitsingh Nawale
Head - Information Technology
Advik Hi-Tech Pvt. Ltd.

Q. If you could bet on one emerging technology to redefine business in the next five years, what would it be, and why?

In the pharmaceutical sector, the most transformative emerging technology for IT and security over the next five years is an AI-driven Zero Trust Architecture (ZTA). ZTA replaces legacy perimeter defenses with continuous identity verification, micro-segmentation, and least-privilege access, while AI algorithms monitor user behavior, detect anomalies, and automatically remediate threats in real time. For pharma, this means secure sharing of sensitive genomic, clinical, and proprietary data across research consortia, cloud platforms, and IoT devices, without exposing intellectual property or violating regulatory mandates. AI-guided policy enforcement reduces false positives, preserves productivity, and ensures compliance with FDA, GDPR, and even the DPDP Act of India. By embedding ZTA into the drug-development pipeline, companies can accelerate collaboration, protect trade secrets, and mitigate ransomware risks, ultimately shortening time-to-market and safeguarding patient safety. Thus, adopting an AI-powered Zero Trust model will redefine how pharmaceutical firms manage risk, innovate, and deliver value. It also streamlines audit trails, speeding regulatory reviews, and building stakeholder trust.



Chitti Babu
Group CIO
Aurobindo Pharma

Q. Looking at the major cyber incidents of 2025, which one genuinely shook your view on security, and why?

The Jaguar Land Rover (JLR) cyberattack in August–September 2025 really altered my perspective on security. It wasn't just a data breach; it was an operational catastrophe. The attack, attributed to the Scattered LAPSUS$ Hunters group, forced JLR to shut down production for five weeks, halting output at major United Kingdom (UK) plants and disrupting 5,000 suppliers. The financial impact was staggering: £196 million in direct costs and an estimated £1.9 billion hit to the UK economy made it the costliest cyber incident in British history.

What shook me most was how deeply IT and operational technology are intertwined. The cascade from a single compromise to the halting of assembly lines, empty dealerships, and national economic consequences was a real shock. This incident has underlined the fact that cybersecurity is no longer an IT issue; it's a core business continuity challenge. For manufacturers like JLR, resilience planning and supply chain security must now be treated as existential priorities.

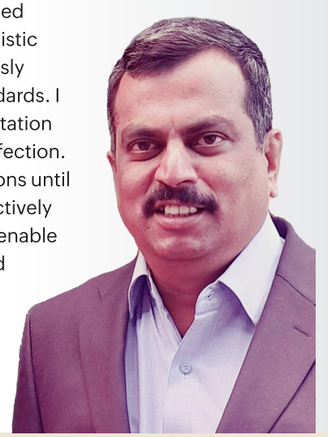


Piyush Joshi
Head of Global Business Service Centre India
Brose India Automotive Systems Pvt. Ltd.

Q. Which quality do you value most in your IT team and how do you nurture it?

The single most important quality I value in my IT team is customer commitment—a principle that applies not only to IT but to every business function. For IT, customers include both internal users of infrastructure and applications as well as external partners, such as service providers, system integrators, and vendors.

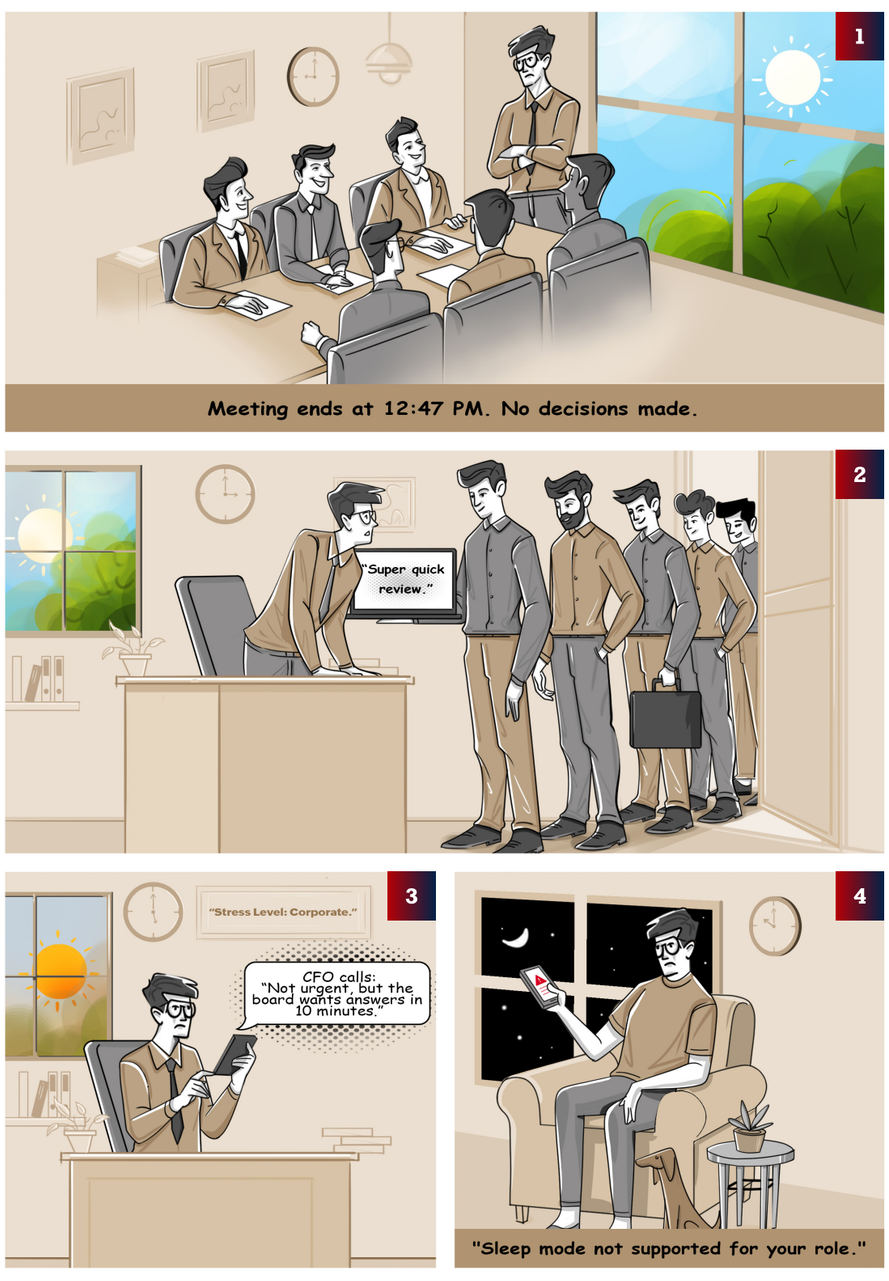
I nurture this commitment by encouraging teams to deeply understand business needs before designing user-friendly solutions, distinguish between hyped and justified requirements, and set realistic timelines while continuously raising performance standards. I believe phased implementation is better than delayed perfection. We closely monitor solutions until stability is achieved, proactively address user pain points, enable business power users, and continuously explore new technologies to drive business outcomes.



Dr. Madhav Bhole
Head - ERP & IT
Fleetguard Filters Pvt. Ltd.

Scan the QR code to get featured in Leadership Lens!

A DAY IN A CIO's LIFE



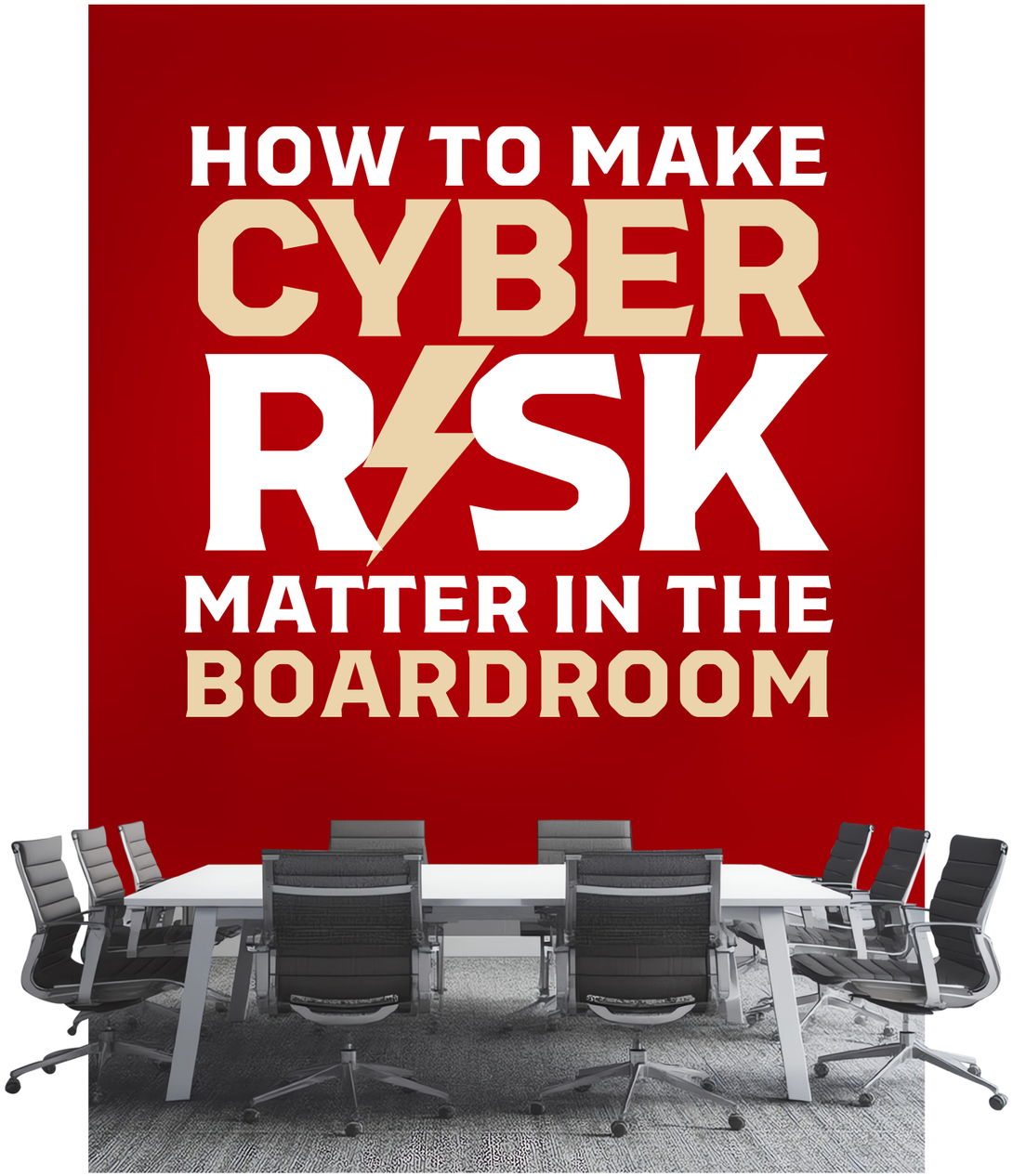


Thursday dawned like any other, until chaos struck Nyx Technology. This rising force in the cloud services market suddenly found itself in the midst of a catastrophic cybersecurity fallout.

Confidential data was exposed, revealing internal documents, client records, and sensitive information that were never meant to see the light of day. Contracts with clients and partners were suddenly at risk, with potential violations of strict data-handling agreements. As details of the breach surfaced, the company's reputation took a visible hit, trust wavered, and market confidence slipped. Meanwhile, the recovery process required significant time and effort as teams worked to revoke access, audit systems, and rebuild security controls they once thought unshakable.

Your mission begins now! Follow the scattered digital crumbs, hidden across different pages of this magazine to uncover how Nyx Technology's defenses broke down, and who was secretly pulling the strings all along.

HOW TO MAKE CYBER RISK MATTER IN THE BOARDROOM



CISOs can sometimes feel like pundits of frameworks like the NIST and ISO, reveling in establishing security metrics that help them understand the security and compliance posture of their organization. But when it comes to engaging business leaders, many hit a wall. Why? Because technical jargon and security intricacies rarely make an impact in the boardroom—an arena that is more concerned with big picture items: market pressures, bottom lines, and reputation risks. The issue isn't that the board lacks technical expertise, but rather that cyber risk is often not communicated to them in a way they can easily grasp.

Business leaders don't want to hear about cloud misconfigurations or vague references to credential stuffing. They want to understand how these specific risks hurt their bottom lines and how often. So as a CISO, how you present these technical risks matters the most. Instead of dropping abstract numbers like a "40% chance of a DDoS occurrence," tell them DDoS attacks happen about once every two to three years, and share the range of potential losses in dollars following these attacks. This helps turn statistical buzzwords into impactful narratives that matter.

A CISO mantra when dealing with the board is, **"stories anchor risk in reality."**

To your security team, a phrase like "lax third-party access control" feels relevant to their roles. But to the board, it's just jargon. Instead, tell the story in plain language: "Imagine a contractor with temporary access quietly manipulating claims data. Later, fraudulent claims are submitted and reimbursed. Now we've got regulatory violations, financial losses, and insurers questioning our integrity."

Mapping risk to business processes is crucial. Don't just say "there's insider fraud risk in billing operations." Demonstrate how temporary staff could bypass approval checks to push inflated or duplicate claims during peak processing season, revealing a clear threat to revenue and compliance with healthcare regulations.

It's equally crucial to **differentiate risk from operational issues.** An unpatched picture archiving and communication systems (PACS) server means nothing to the board. Instead, highlight the potential exploit that alters diagnostic images, delaying patient care and inviting legal action.

To bridge the gap between the technical outcome and the business impact even better, **instead of heat maps cluttered with technical controls, use business impact maps** that highlight zones of revenue loss, operational disruption, or reputational damage. Boards rarely respond to red-yellow-green severity labels. They're more likely to respond to a visual that shows how a ransomware attack could freeze claims processing systems for three days, delaying reimbursements, disrupting cash flow, and triggering penalties from payers. That downtime translates into millions in lost revenue, strained provider relationships, and reputational damage with patients and insurers alike.

Cyber maturity, when framed and demonstrated correctly, can also become a strategic brand asset. Beyond risk reduction, a well-secured ecosystem signals operational discipline, resilience, and trustworthiness—qualities that accelerate partnerships and attract investors. Boards are keenly aware that trust drives growth, and in sectors like healthcare, finance, or manufacturing, demonstrating robust cyber practices can be the differentiator in winning contracts or securing funding.

That's why cybersecurity leaders must move beyond abstract risk lists and instead tell business-driven stories. When risks are framed around profits, growth, and reputation, security investments shift from being seen as a technical expense to a strategic imperative.



An excerpt from a security assessment report during the internal audit reads: "*Permission reviews were completed for less than half of all external integrations, this quarter.*"

THE EASTER WEEKEND BREACH: WHAT CISOs CAN LEARN FROM M&S

April 2025 marked a turbulent period for the retail sector, with several major chains—Co-op, Harrods, and Marks & Spencer (M&S)—falling victim to cyberattacks. M&S bore the brunt of these incidents when Scattered Spider launched a high-impact ransomware attack over Easter weekend. By manipulating the service desk through social engineering, the attackers bypassed MFA, accessed Active Directory (AD), deployed DragonForce ransomware, and encrypted VMware ESXi hosts. This disrupted critical online operations and impacted payment and customer services.

The fallout was extensive: M&S temporarily shut down its online operations, reverted to manual processes, and paused its click-and-collect service for months. Estimated weekly losses reached £43 million, with overall disruption costs potentially surpassing £300 million. Compromised customer data—such as names, birth dates, addresses, phone numbers, and purchase histories—added reputational and regulatory strain to the crisis.

For CISOs, the incident highlights several priorities. First, service desk security needs renewed attention. Attackers exploited human trust, proving the importance of strict identity verification, frequent social engineering drills, and controlled credential reset workflows.



Attack type -
Ransomware (DragonForce)

Threat actors -
Scattered Spider group

Attack vector -
Service desk social engineering, MFA bypass

Targeted assets -
Active Directory, VMware ESXi hosts, payment and customer services

Data compromised -
Names, DOB, addresses, phone numbers, purchase histories

Financial impact -
£43M/week; projected >£300M total

Duration of disruption -
~4 months (Click & Collect and online ops)

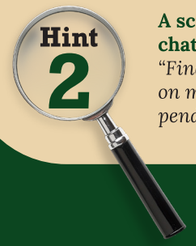
MARKS & SPENCER

Second, AD security must be hardened. Protecting NTDS.dit files, implementing Just-in-Time privileged access, and enforcing phishing-resistant MFA help prevent privilege escalation and lateral movement. Third, continuous endpoint and threat monitoring is essential. Fileless attacks and misuse of built-in tools often slip past traditional defenses. A combined approach using SIEM, UEBA, and EDR improves contextual detection and response speed.

Beyond internal systems, CISOs must address the third-party attack surface. Retail environments depend on multiple vendors, each with varying cyber hygiene. Zero Trust principles, vendor audits, and access controls are crucial to prevent supply chain exploitation. Additionally, proactive incident response and clear communication strategies are necessary to maintain brand trust during disruptions. Pre-drafted breach communication templates and rapid containment protocols reduce reputational and operational damage.

Finally, segmented, immutable backups and alignment of cybersecurity with business continuity plans are vital. Ransomware groups often target backups, and the M&S disruption illustrates how downtime can cost hundreds of millions in lost revenue. Ensuring backup systems for payment processing and order fulfillment mitigates operational risk.

The M&S ransomware attack is a stark reminder that even mature security frameworks can be circumvented by social engineering and privileged account abuse. For CISOs, the lessons are clear: strengthen human-focused defenses, monitor critical assets continuously, enforce strict identity controls, and integrate security into business continuity planning.

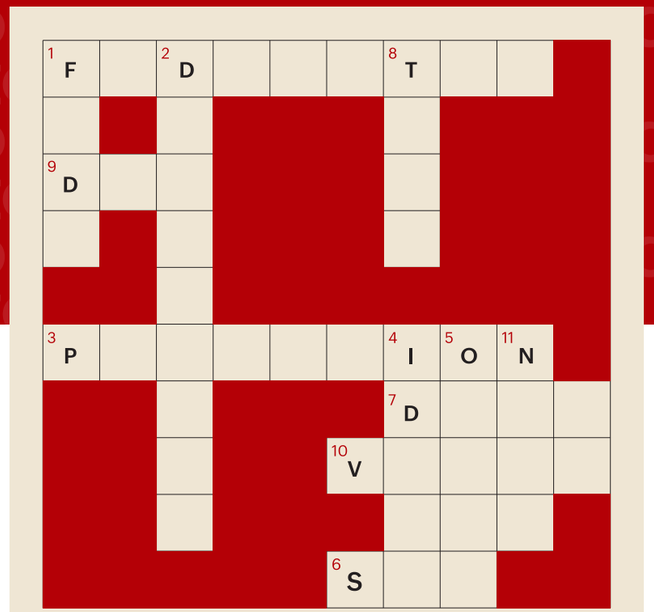


A screenshot of an internal team chat shows a sales rep saying, *"Finally set up the new CRM on my own. IT approval is still pending."*

CROSSWORD CHALLENGE

“Decode this, CIO!”

Test your IAM & SIEM smarts



Across

1 Single login across multiple platforms

3 Create user accounts and access

6 Secure remote access to servers and devices

7 What every breach aims to steal

9 Internet’s phonebook

10 Secure digital password storage

Down

1 Passwordless authentication standard

2 Central view for monitoring cyber threats and systems

4 Cloud-based identity management service

5 SSO protocol granting secure access to apps

8 Time-based one-time code

11 Old Microsoft challenge-response auth, replaced by Kerberos

CIO HAPPINESS INDEX



READY FOR A BRAIN WORKOUT?

1

I assume nothing,
even when everything looks familiar.
I ask again, verify again,
even when nothing seems wrong.

What security model am I?

2

I arrive only when needed
and disappear before I’m missed.
I reduce risk not by restriction,
but by timing.

What access strategy am I?

3

Alone, each signal is meaningless.
Together, they reveal intent.
I connect moments across systems
to expose what no single alert can.

What capability am I?

4

I don’t wait for damage.
I look for patterns, anomalies,
and behaviour that doesn’t belong.

What security outcome am I?

The business cost of **fragmented identity** architectures



Enterprise systems power operations worth thousands of crores each year, and their value is measured through uptime, performance, and return. As these enterprise systems become more siloed, identity has become the layer that connects users, applications, and data across the organization. For any organization, having a central and consistent view of identity is now essential because it determines how quickly teams can provision access, resolve issues, and understand who can reach sensitive information.

Fragmentation affects how reliably an organization can meet the expectations of the DPDP Act. The Act requires purpose-bound access, timely breach notification, and clear evidence of how personal data is handled. These obligations become more resource-intensive when identity information is inconsistent. The Act permits penalties up to ₹250 crore for inadequate safeguards, up to ₹200 crore for delayed or lack of breach notifications, and up to ₹50 crore for other violations.

Beyond compliance, fragmentation introduces practical delays across the business. It slows projects, delays revenue initiatives, and increases the time required for incident response when a unified identity view is missing. Containment efforts that should take minutes stretch into days, increasing downtime and public exposure. Over time, these delays accumulate, raising compliance costs and weakening trust in the organization's digital systems.

IAM can be used as a control panel to increase resilience

A strong identity architecture starts with visibility, accountability, and measurable control over who has access, why they have it, and how long it lasts. Here are a few steps that can help you get there.

1. **Improve access visibility and reduce reconciliation effort:** A unified view streamlines access reviews and helps identify excessive or unused permissions early. This reduces audit workload and improves overall governance.
2. **Strengthen access hygiene to control exposure:** Regular cleanup of inactive accounts and overlapping permissions keeps the attack surface predictable.
3. **Reduce login friction and password fatigue:** Consistent authentication lowers help desk load and improves day-to-day productivity.
4. **Automate identity workflows to improve efficiency:** Shortening onboarding from days to minutes reduces manual effort and ensures timely access.
5. **Enhance threat detection through behavioural insight:** Analysing user patterns helps surface unusual activity sooner and supports faster response.
6. **Replace standing privileges with time-bound access:** Limiting elevated rights to the duration of a task reduces unnecessary exposure.
7. **Simplify audit preparation with centralized evidence:** Consolidated records make audit cycles faster and reduce the need for manual reconstruction.

Securing identity enables business

As enterprises become more interconnected, identity becomes the map and the compass, the only layer with visibility across cloud infrastructures, application layers, and data boundaries in real time. When IAM matures into an identity fabric, it shifts from a set of controls to an adaptive network of trust that continuously verifies access and withdraws it as context changes.

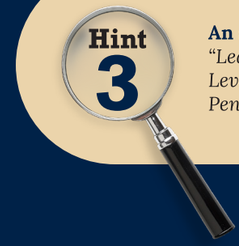
The question **who has access, why, and until when** becomes the foundation for any enterprise that intends to remain secure and trusted.

The operational gains delivered through strong identity foundations

100% consistency in multi-domain identity management for Royal Cosun through a single console.

10× faster user management at New Process Metal Solutions with automation.

$26,000 saved annually at CAMH by removing password-reset calls through self-service.



An admin panel entry reads: *"LeadGrid CRM — Permission Level: Full | Review Status = Pending."*

Data under siege



Building cyber resilience in modern healthcare

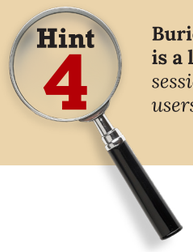
Healthcare has always been an attacker's favorite, but it's become staggeringly clear in recent months, with threat actors leaving no stone unturned to access and exfiltrate sensitive health information. Threat actors are targeting hospitals, insurers, and clinics with ruthless precision, exploiting patient data as leverage for ransom. No healthcare organization—big or small, public or private—is immune to a breach.

The siege of healthcare intensified at the end of 2024 during the Star Health breach, when attackers used compromised credentials, spread a disinformation campaign, and leaked the personal and medical data of 31 million customers. This continues into 2025 with the Episource data breach, in which the healthcare delivery organization suffered a ransomware attack that exposed data of 5.4 million individuals. Even emergency and specialized care aren't spared: Bell Ambulance was targeted by the Medusa ransomware group that affected 114,000 people, while Vitenas Cosmetic Surgery fell victim to Kairos ransomware through a simple brute force attack, and allegedly had 734 GB of sensitive medical records and patient images stolen.

In addition, the 23andMe data breach—first reported in 2023—returned to headlines when regulators fined the company £2.31 million in June 2025 for inadequate data protection. This demonstrates that even genetic testing firms, which hold some of the most sensitive human data, are within attackers' reach.

The recent breaches have sent a clear message to healthcare CISOs: cybersecurity can't be an afterthought—it's a boardroom imperative. These incidents didn't just expose data; they exposed strategic vulnerabilities in how healthcare organizations manage trust, continuity, and risk.

Star Health's breach revealed the dangers of insecure APIs and unencrypted data, underscoring the need for proactive security assessments and robust encryption protocols. With scrutiny escalating, reputational damage from delayed disclosures—like Star Health's 11% stock dip—can be swift and unforgiving. Episource highlighted the fragility of vendor ecosystems, in which third-party access can become a silent entry point for attackers. Bell Ambulance's ransomware attack reminded us that clinical continuity hinges on resilient backup and recovery strategies.



Buried in the help desk queue is a low-priority ticket: "CRM *sessions stay active even after users log in from different IPs.*"

For CISOs, the mandate is clear: Adopt Zero Trust as a foundational principle, not just a feature. Identity must be continuously verified, access tightly controlled, and networks segmented to prevent lateral movement. Real-time security monitoring, threat hunting, and dark web monitoring must be embedded into daily operations—not reserved for post-incident analysis. Genomic data adds a new layer of complexity. With its permanence and sensitivity, protecting it demands quantum-resistant encryption, blockchain integrity, and privacy-preserving AI.

Cybersecurity leadership today means anticipating threats, orchestrating rapid response, and embedding resilience into every layer of the enterprise. CISOs must understand that cyber resilience is clinical resilience, and building robust healthcare security means combining visibility, verification, and vigilance into every system that touches patient data. Protecting data is no longer just about compliance; it's about preserving trust and safeguarding lives.

Leave no room for attacks with **Log360**!

The DNA of DPDP compliance: Shaping trust through law and leadership

Where governance and leadership actions encode the living code of organizational integrity.

The genetic code of compliance decoded for the modern CISO.

Section 5
Purpose limitation
Data must be collected and processed only for specific, lawful, and consented purposes.

Make data usage visible and accountable

Section 6
Consent and lawful processing
Valid consent must precede data processing; withdrawal must be honored.

Consent must remain a continuous, non-negotiable imperative

Section 7
Rights of data principals
Individuals have rights to access, correction, and erasure of their personal data.

Build data principal rights into system workflows

Section 8
Security safeguards
Fiduciaries must maintain controls to prevent unauthorized access or breaches.

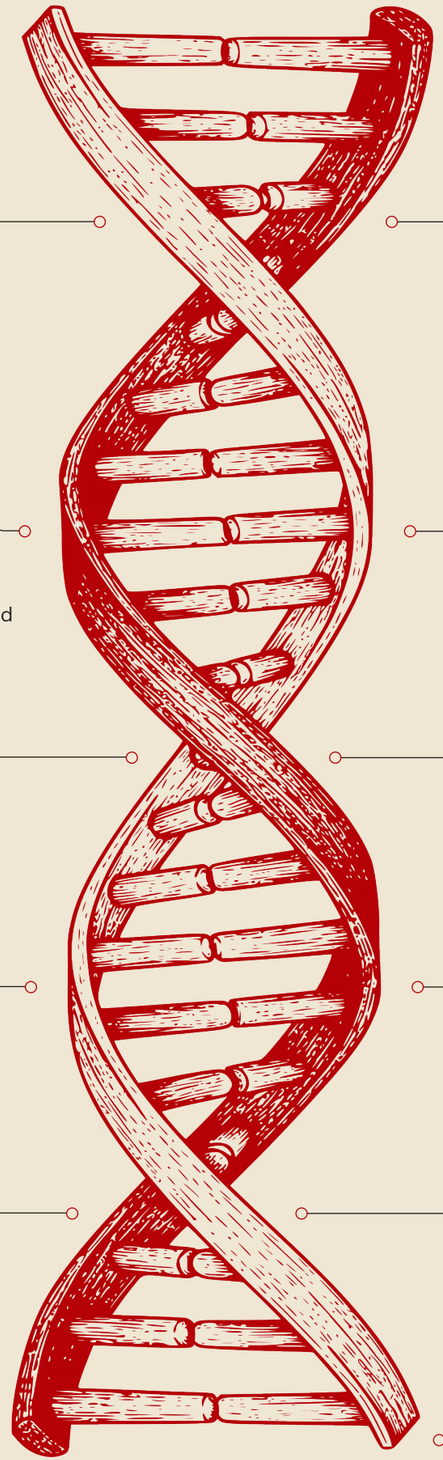
Prove security through live controls

Section 9
Breach notification
Breach disclosure is mandatory to the Data Protection Board and affected individuals.

One chain from alert to report

Section 10
Accountability and governance
Organizations must conduct audits and ensure ongoing compliance oversight.

Turn compliance into real-time data



Purpose limitation
Build a registry linking each data collection process to its approved purpose.
Set up filters to block data without declared purpose.
Review APIs to catch usage outside intended scope.
Key metric: Percentage of data with verified purpose tags

Data purpose governance

Consent and lawful processing
Configure IAM and API gateways to check consent tokens before granting data access.
Integrate real-time consent checks in data pipelines and backend workflows.
Enforce a deny-by-default policy when consent is missing, withdrawn, or expired.
Key metric: Consent revocation latency

Consent verification at access gate

Rights of data principals
Tag datasets with owner information.
Automate deletion or correction requests.
Keep audit records of changes.
Key metric: Average time to complete data deletion requests

Erasure and access automation

Security safeguards
Monitor encryption and access controls in real time.
Use behavior tracking for anomalies.
Apply Zero Trust principles to sensitive flows.
Key metric: Percentage of systems with active security checks

Continuous control validation

Breach notification
Create a breach response guide integrated with incident response.
Automate notifications for regulators and privacy officers.
Track deadlines for reporting (for example, 72 hours).
Key metric: Time from breach detection to disclosure

Disclosure orchestration

Accountability and governance
Build dashboards for audit logs and compliance reports.
Link privacy KPIs to risk and performance metrics.
Set quarterly reviews with legal and security teams.
Key metric: Rate of automated evidence generation

Evidence automation

Section 5
Data purpose governance
Data discovery and classification, DLP, data tagging solutions

Section 6
Consent verification
IAM systems, consent management platforms

Section 7
Erasure and access automation
SOAR and workflow automation solutions

Section 8
Continuous control validation
SIEM, UEBA, endpoint detection, Zero Trust platforms, cloud security posture management solutions

Section 9
Disclosure orchestration
SOAR, SIEM, incident response platforms, automated email and alert systems, regulatory communication modules

Section 10
Evidence automation
Audit dashboards, compliance solutions

QUIZ

THE CIO ARCHETYPES

1. Over the next year, what will be your top IT priority?

a. Ensuring technology initiatives complement broader business objectives.
b. Exploring new approaches to stay ahead of technology trends.
c. Upgrading internal capabilities and workflows for better business outcomes.
d. Fortifying defenses and maintaining vigilance amid evolving threats.

2. When you first encounter a breakthrough technology, how do you typically respond or adapt?

a. Consider how it could influence the organization's overall direction and future positioning.
b. Explore its potential through contained use cases or test environments.
c. Examine its viability, integration challenges, and impact on current workflows.
d. Review its compliance, risk exposure, and resilience within existing frameworks.

3. How do you embody your role as a leader?

a. By setting clear direction and inspiring the team to achieve shared goals.
b. By encouraging new ideas and processes within the workforce.
c. By cultivating commitment to results and emphasizing consistency.
d. By anticipating challenges and threats while taking preventive actions.

4. What is the key benchmark you use to define IT success?

a. Progress toward sustainable growth and future-readiness of the organization.
b. Tangible outcomes from new initiatives and impactful deployments.
c. Reliable systems and stable processes that save time and boost overall performance.
d. Improved resilience that aligns with security standards and minimizes operational risks.

5. After resolving a major business challenge, your first instinct is to...

a. Revisit the roadmap and realign goals.
b. Identify tools that can directly prevent or disrupt similar issues in the future.
c. Implement learnings into existing processes to avoid recurrence.
d. Analyze risk exposure and strengthen safeguards around critical systems.

6. What's your preferred approach to decision-making?

a. Relying on intuition and long-term vision.
b. Using innovation and experimentation to discover new approaches.
c. Prioritizing safety, adherence to guidelines, and careful risk assessment.
d. Prioritizing rules, risk management, and compliance.

7. Your IT investments primarily focus on...

a. Digital transformation initiatives that drive competitiveness.
b. New-age technologies enhancing customer experience.
c. Tools that improve efficiency, reliability, and resilience.
d. Cyberdefense systems and compliance automation.

8. Which statement best aligns with your IT philosophy?

a. IT is the backbone that shapes business direction.
b. Technology is our catalyst for innovation and customer delight.
c. Consistency and reliability define IT excellence.
d. Security and compliance are the foundations of trust.



Strategic Visionary

Future-focused and transformational - the leader who turns vision into long-term business advantage.



Technology Evangelist

Passionate and persuasive - the champion who drives tech adoption to redefine customer and employee experiences.



Operational Innovator

Reliable and efficient - the master of stability who ensures IT runs like a well-oiled machine.



Cybersecurity Sentinel

Cautious yet confident - the protector who builds resilience through vigilance and control.

After answering, add up the points based on the scoring below, then use your total score to find your archetype.

Range	Archetype
40–69	Strategic Visionary
70–99	Technology Evangelist
100–129	Operational Innovator
130–160	Cybersecurity Sentinel

Scores							
Qn. 1	Qn. 2	Qn. 3	Qn. 4	Qn. 5	Qn. 6	Qn. 7	Qn. 8
						Total	

a - 5 points; b - 10 points; c - 15 points; d - 20 points

A LOOK BACK, A LOOK AHEAD



In an industry that moves as fast as ours, it is easy to forget the true value of coming together, sharing ideas, and learning from one another. CIO Connect was created with a simple belief at its core: When great minds meet, great progress follows. Across four cities, we had the privilege of bringing together some of the brightest cybersecurity and technology leaders, individuals who shape the way organisations think, operate, and stay secure.

Each edition of CIO Connect was more than an event; it was a conversation, a collaboration, and a reminder that community matters. As hosts, we listened, learned, and grew alongside our guests. This series reflects that spirit of connection, curiosity, and collective commitment to strengthening India's cybersecurity future.







Memory Bytes:

CIO Connect

Four cities, one conversation, countless insights

Bangalore

Where innovation met insight

Our first CIO Connect event in Bangalore set the tone for what would become a truly memorable series. Hosted in the city often called India's tech capital, the event reflected the same cool composure and intellectual energy that Bangalore is known for. With over 80 CIOs and IT leaders from diverse sectors, the evening was an engaging mix of knowledge exchange and meaningful connections.

From **Madhusudan Kohli's** [CIO & CBO, ACPL Systems Pvt. Ltd.] keynote on shaping security strategies to **Dr. Dhruv Pandit's** [Co-Founder & CEO, Drona Cyber Solutions Pvt. Ltd.] insights into digital forensics, the sessions sparked thought-provoking discussions on cybersecurity leadership. The panel on building resilient frameworks and the fireside chat on industry-specific challenges brought together CIOs from different industries who shared their first-hand experiences and practical perspectives. The musical interlude and networking dinner added warmth to the cool Bangalore evening, making it a fitting start to our CIO Connect journey that was premium, purposeful, and perfectly in sync with the city's innovative spirit.

Delhi

A royal gathering of cybersecurity leaders

The CIO Connect Delhi edition was grand in every sense, hosted at the majestic Leela Palace, which lent a royal charm befitting the nation's capital. The event drew more than 150 distinguished guests, including senior delegates from the Government of India, making it our largest and most prestigious gathering yet. The highlight of the evening was our Experience Center, where live product interactions brought our cybersecurity solutions to life, showcasing our unwavering commitment to safeguarding digital India.

The sessions were rich with insight and leadership. **Shri Narendra Nath Gangavarapu's** [Joint Secretary, National Security Council Secretariat, Govt. of India] keynote on securing India's digital frontier and **Mr. Vinayak Godse's** [CEO, Data Security Council of India] address on cybersecurity excellence set the tone for a thought-provoking evening. The panel discussion, featuring CIOs from large enterprises, provided an in-depth look into how industries are addressing evolving threats, while the fireside chat saw our cybersecurity evangelists present real-world solutions and best practices. Surrounded by Delhi's grandeur and driven by purpose, the evening celebrated the strength, pride, and vision of India's cybersecurity community.







Pune

Defending the digital fort

Known for its rich history and culture of leadership, Pune provided an inspiring backdrop for our CIO Connect event. With over 140 participants, the evening combined premium networking with deep, practical insights into cybersecurity. The city's legacy of foresight and resilience mirrored the discussions on protecting modern enterprises in an era of rapidly evolving threats.

The sessions were engaging and highly interactive. **Shri Amitesh Kumar** [IPS, Police Commissioner of Pune] set the stage by emphasising our responsibility as citizens in the cybersecurity ecosystem.

Dr. Prashant Mali [Cyber & Privacy Law Expert] highlighted key aspects of data privacy and compliance, giving participants actionable takeaways. The panel discussion, featuring CIOs from leading enterprises, offered real-world perspectives on challenges and strategies, while the fireside chat, led by our cybersecurity evangelists provided practical solutions for identity management, endpoint security, and threat detection. The event celebrated Pune's spirit of vigilance and learning, connecting the city's historic resilience to the modern need for robust digital security.

Hyderabad

The cybersecurity capital in the making

The CIO Connect Hyderabad brought together 148 CIOs for an evening of collaboration, learning, and insight. As a city with a tech legacy dating back to the mid-90s, Hyderabad seamlessly blends rich culture, vibrant talent, and forward-looking innovation. Its energy and warmth created the perfect backdrop for conversations on the future of cybersecurity, reinforcing its position as a mature technology powerhouse and a committed champion of digital resilience.

The sessions offered both strategic vision and practical guidance. **Shri Sridhar Babu Duddilla** [Minister of Information Technology, Electronics, Communications, Industries & Legislative Affairs] shared Telangana's bold ambition to become India's cybersecurity capital, while **Dr. Pavan Duggal** [Founder & Chairman of the International Commission on Cyber Security Law] unpacked the DPDP Act with a deep dive into emerging cyber trends and compliance challenges. The industry panel, featuring CIOs from leading enterprises, shared real-world lessons and strategies from breaches to boardrooms, while the fireside chat with ManageEngine evangelists explored integrated solutions for staying ahead of evolving threats. The evening concluded with **Yogesh Gupta's** [Editorial Director – Events, India & META, Foundry] closing keynote on AI-driven resilience, tying leadership, technology, and strategy together. Much like Hyderabad's vibrant culture and rich culinary heritage, the event blended diverse perspectives, deep insights, and forward-looking discussions into a truly memorable experience.



Scan the QR code to join our exclusive CIO community, your space to network with peers, share cybersecurity perspectives, and stay engaged in ongoing CIO collaborations.

FICTION



Hint 5

Monitoring dashboards reveal a sudden spike in outbound data from the CRM integration, reaching levels ten times higher than usual.

THE SECRET LIFE OF A SERVICE ACCOUNT

A CAUTIONARY TALE, BE WARNED

Manish Bhatia lay wide awake in the vigil hours. For the past week, rest had come only in fragments, which was again chased away by calls bearing nothing but bad news. This night felt no different, almost as if he were bracing himself for the next inevitable blow.

His phone buzzed with a high-priority escalation alert. The ball had dropped, and his face drained of color. Whatever it was, it was serious enough to drag him, the CTO of Bionautics, out of his bed at 3:12am. Manish grabbed his coat and headed out. Street lights flickered over the empty roads, and the night air felt dense as he drove toward the Bionautics campus. Every few minutes he glanced at his phone, hoping the screen would remain silent and no alerts would pop up.

The biometric scanner hesitated for a moment before accepting him, and he immediately noted the authentication latency. The network was still struggling. Inside the office, the corridors were unnervingly quiet. There was none of the usual muted conversations or soft clicking of keyboards. He entered the war room, where a handful of cyber analysts, SOC officers, and administrators stood with pale faces.

Since the breach, his team had been working nonstop. They had contained most of the damage, but the effortless way the intrusion had moved across trust zones kept them puzzled. The breach didn't match any known attack pattern.

At first, a cluster of inactive employee accounts, disabled days ago, had suddenly come back to life. Logging in from cities across the world, they drifted through systems, opening files, checking permissions, and quietly existing. They weren't stealing data or causing damage, only wandering through the network like ghosts. But the true horror behind those resurrected identities revealed itself before anyone could react.

A sprawling network of unauthorized apps had been quietly woven across the systems. Dozens of unknown services had been syncing data, escalating permissions, and slipping past alerts. Then reports of phantom logins surged, with employees accessing systems from impossible locations. As they watched helplessly, privileged accounts across the company were hijacked. It became clear someone had been inside Bionautics' network for months, wearing the identities of former employees.

Over the next two days, the systems were collapsing, the board was demanding an explanation, and the team was drawn into a grim pursuit for answers. All the while, Manish couldn't shake the feeling that something was lurking just beyond his sight.

Today, the room felt smaller as he realized that the feeling had been right all along. The SOC officer pointed to the large LED monitor displaying the activity logs of one of the company's senior DevOps engineers, Raghav Menon, who had resigned just a week earlier. His credentials were supposed to be revoked the moment he walked out of Bionautics' glass doors. But the logs told a different story.

Manish's stomach tightened as the officer walked him through how he had traced the pattern. There were short bursts of access, each lasting only fractions of a second. The access was always coming through a previously dormant service account:

SVC_CORE_MAINT_09.

An account that had already been deactivated. But it was active again.

"Raghav had embedded implants months before his resignation," the officer said. They were hidden inside routine scripts, camouflaged behind service accounts, and tucked into harmless-looking configuration files that no automated scanner ever flagged. He had spent years learning the company's architecture, and months dismantling it from within.

"And he's still inside." Manish's expression twisted in shock as the realization hit him.

"He knew exactly what we'd do. He anticipated every countermeasure."

Suddenly, every screen went black. Somewhere in the server hall, alarms began blaring in warped, broken tones, as if the machines were trying to speak. One by one, every device around Manish rebooted. Systems, tablets, company-managed phones, even the large LED monitor.

They all flashed the same message:

I NEVER LEFT.

*77% of organizations experienced insider-driven data loss in the past 18 months, and *41%* reported financial impact between $1M and $10M for their most significant incident.

If your current approach falls short against insider risk, it's time to act. Reach out to us to gain deeper visibility and strengthen your organization's security with our solutions.

From friction to focus:

How leading enterprises have mastered identity management and IT security

India's enterprises, along with organizations around the world, are navigating technology stacks that continue to grow in complexity. As digital expansion accelerates, enterprises must balance rapid growth with the critical need for a hardened security posture. When identity management and security intelligence operate as distinct disciplines, the challenge for the CIO is to ensure that each function possesses the operational maturity required to protect modern digital assets. Resilience is achieved not through one tool, but by fortifying these individual pillars as part of a multi-layered defense strategy. ManageEngine addresses this by providing robust, dedicated solutions for both IAM and SIEM, allowing organizations to tackle identity governance and threat intelligence with precision.

Pine Labs · novobanco · adani · RBL BANK · George Clinical (Science. Service. Solutions.) · INTERGLOBE · SUNDARAM BUSINESS SERVICES

This strategy begins by mitigating the high-stakes risks inherent in manual infrastructure. For **InterGlobe Enterprises,** manual provisioning was a source of administrative delays and a catalyst for human error. In an environment where every access point represents a potential entry for attackers, critical lapses such as misconfigured permissions create immediate, high-impact security gaps. By implementing AD360, ManageEngine's unified IAM solution, **InterGlobe** automated AD management and standardized user life cycles. This transformed identity management into a governed, audit-ready framework, protecting the organization's data and its long-term operational integrity from the massive financial fallout of a compromise.

Hardening this perimeter further requires rigorous entry controls. **Adani Group** demonstrates this proactive stance by using AD360 to enforce strict password policies and adaptive MFA. By preempting unauthorized access at the source, they have transformed identity from a potential vulnerability into a hardened shield. Crucially, this proactive security does not have to hinder productivity. **George Clinical** balances these strict access controls with a seamless user experience. By streamlining password management and implementing SSO, they ensure that while access remains tightly regulated to meet global standards, the daily workflow remains efficient.

Even the strongest perimeter requires constant vigilance. When a threat does breach the surface, the focus must shift to reactive intelligence. **Sundaram Business Services (SBS)** uses Log360, ManageEngine's comprehensive SIEM solution, to move beyond passive logging into active threat hunting. By gaining real-time insights into network changes, they identify unauthorized access attempts and the use of unapproved remote tools. This monitoring transforms security into an active process, preventing the unauthorized access lapses that often lead to catastrophic breaches.

As operations scale, this reactive focus deepens into comprehensive visibility and forensic accountability. **RBL Bank** utilized Log360 to address security log retention gaps, enabling the exhaustive, system-wide reporting required for deep-dive audits. And, **Pine Labs** leveraged AD360 to fortify the identity layer, ensuring granular tracking of user permissions even during infrastructure downtime. By deploying these specialized tools, these organizations proved that security and uptime can coexist—building a framework capable of satisfying the most rigorous data-handling investigations.

The final stage of a resilient strategy is the ability to recover when the unthinkable happens. True resilience requires a fail-safe for the identity backbone itself. For the investment banking firm **Novobanco**, AD serves as the nerve center of the organization. Recognizing that even hardened systems face risks of accidental deletion or corruption, they implemented Recovery Manager Plus, ManageEngine's enterprise backup and disaster recovery solution. This specialized solution allows for surgical restoration of identity objects without requiring a full domain controller reboot. By ensuring they can undo changes instantly, the firm has secured its business continuity, proving that high-stakes operations require not just a shield to prevent entry, but a fail-safe for immediate recovery.

The success of these enterprises—from the banking-grade compliance at RBL to the proactive threat intelligence at Sundaram Business Services—demonstrates that enterprise security relies on the depth and strength of its individual defensive pillars. Enterprises are finding that the most effective way to manage an evolving threat landscape is to deploy specialized, robust capabilities across automation, analytics, and identity management. By fortifying both identity governance and security intelligence as distinct but essential components, these organizations have transformed their security posture from a reactive obligation into a proactive, resilient defense.

Try our unified **IAM platform** today!

DECODED:

The answers you've been looking for

The curious case of Nyx Technology

All evidence now points to one name—LeadGrid CRM. When a sales rep installed the app without waiting for IT approval, it quietly opened a backdoor into Nyx Technology's systems. No one had verified its permissions, and deep within its code lay a hidden flaw. Attackers found the crack and slipped through, hijacking sessions, moving laterally across connected platforms, and extracting data. Dashboards displayed alerts about sudden surges of outbound traffic as confidential files slipped out unnoticed.

A perfect example of a poisoned chalice.
*Hints: page **17**, page **19**, page **23**, page **25**, and page **34**.*

Technical crossword

1 F	E	2 D	E	R	A	8 T	E	D	
I		A				O			
9 D	N	S				T			
O		H				P			
		B							
3 P	R	O	V	I	S	4 I	5 O	11 N	
		A				7 D	A	T	A
		R			10 V	A	U	L	T
		D				A	T	M	
					6 S	S	H		

Ready for the brain workout answers?

1

I assume nothing,
even when everything looks familiar.
I ask again, verify again,
even when nothing seems wrong.
What security model am I?
Answer: Zero Trust security

2

I arrive only when needed
and disappear before I'm missed.
I reduce risk not by restriction,
but by timing.
What access strategy am I?
Answer: Just-in-Time access

3

Alone, each signal is meaningless.
Together, they reveal intent.
I connect moments across systems
to expose what no single alert can.
What capability am I?
Answer: Log Correlation

4

I don't wait for damage.
I look for patterns, anomalies,
and behaviour that doesn't
belong.
What security outcome am I?
Answer: UEBA

ManageEngine
The Strategy Seat



Born from ManageEngine's commitment to understanding enterprise security priorities, The Strategy Seat is a video podcast series where C-level executives and IT leaders share strategic insights, leadership lessons, and real-world experiences that are shaping cybersecurity. Each episode provides a practical look at today's security challenges and the people driving solutions.

Scan the QR code to take your place in The Strategy Seat.