CXO SAMVAAD

THE PLATFORM FOR INDIA'S TOP CXO

SEPTEMBER

2025

where AI meets IT, security, and technology

WWW.BHARATCXO.COM

CXO SAMVAAD

VOLUME LXIV, NO. 6

NAVIGATOR

HEAD OFFICE

23 , Shoppe Link , Dosti Acres, Wadala, Mumbai , Maharashtra 400037.

FROM THE EDITOR

K A U M U D I V A I D Y A

I am delighted to welcome you to the September edition of CXO Samvaad the flagship publication of BharatCXO, where leadership meets insight, collaboration, and vision. Over the past months, this platform has evolved into more than just a magazine; it has become a growing ecosystem where CXOs, thought leaders, and innovators come together to share ideas that shape the future of Indian business.

This edition is a testament to that spirit of collaboration. As industries continue to navigate disruption and transformation, we highlight stories of resilience, leadership, and forward-thinking strategies that are redefining how businesses operate in a digital-first world.

From thought-provoking features to leadership journeys, and from the growing conversations around artificial intelligence to the ever-pressing themes of innovation and sustainability, this issue captures the pulse of change. Our ongoing podcast series, Hum Tum Aur AI, further strengthens this dialogue by bringing together voices that explore how AI is transforming leadership and decision-making.

September marks an exciting phase for us, as we continue to deepen our community, foster new collaborations, and expand the conversations that matter most to CXOs. We hope this edition inspires you to look at challenges with fresh perspectives and opportunities with renewed optimism.

Thank you for being an integral part of the CXO Samvaad journey together, we are building not just a magazine, but a movement for purposeful leadership.

— Editor, CXO Samvaad

CXO SAMVAAD

CONTENTS

DISCOVER BALI – WHERE EVERY JOURNEY BECOMES A STORY

Let Bharat Trails plan your perfect Bali escape from stunning beaches to cultural wonders, with personalized tours and seamless travel services.

ESCAPE TO BALI – WHERE EVERY MOMENT BECOMES A MEMORY

Chase sunsets, swing over rice fields, and explore ancient temples Bali blends adventure with serenity. Let Bharat Trails craft your perfect getaway with seamless travel and concierge services.

AI + SECURITY + TRAVEL

INFO@BHARATCXO.COM

WWWBHARATCXO.COM

Evolution of Customer Expectations in Banking

S. P. Sudhakaran

Banking once meant visiting a branch and waiting in long queues. Technology shifted this experience to online, allowing customers to access services anytime, anywhere, now the banking is in our palm —ushering in the era of **“Line to On-line.”** Today, Artificial Intelligence is taking this a step further eliminating queues altogether by automating processes, anticipating needs, and delivering instant, personalized service. AI is enhancing it anywhere; it’s transforming the entire industry into a seamless, no-line experience.

The Inevitable Shift: Technology Adoption

In the rapidly evolving digital landscape, embracing technology is no longer optional it’s a necessity. "If you haven’t adopted the technology, the technology will make you to adopt it sooner or later." Indeed, technology plays a vital role in simplifying and optimizing processes. As industries digitize, those who resist transformation may find themselves forced to catch up, often under pressure. Artificial Intelligence is one of the most transformative forces leading this shift.

AI IN CYBERSECURITY DOMAIN

Artificial Intelligence (AI) is often described as a double-edged sword. On one side, AI brings remarkable advancements, boosting productivity through automation and enhancing daily life with smart technologies. It drives innovation, creates new opportunities, and solves complex problems faster than ever before. However, on the other side, this advantage is also available to attackers. This highlights the urgent need for cybersecurity professionals to stay ahead. "AI is being playing a vital role in Offensive and Defensive mechanisms, it can be used for cybersecurity & attackers, based on who’s own it." AI should be as a 360-degree view of the security landscape, enabling a proactive approach to threat detection and mitigation. Ultimately, AI’s impact depends on how it is developed and deployed. With thoughtful regulation, transparent systems, and ethical guidelines, society can harness the benefits of AI while minimizing its risks—ensuring that this powerful tool serves humanity, rather than undermines it.

How AI Enhances Cybersecurity

AI empowers organizations to strengthen their cyber defenses through:

1) Continuous monitoring of massive datasets.
2) Real-time detection of anomalies and potential threats.
3) Predictive analytics to foresee system failures before they occur.
4) Automated responses to minimize human error and reduce reaction time, which often serves as a primary entry point for attackers.

Yet, technology alone isn't enough. The human factor remains a critical line of defense."The most effective defense is employee awareness and training, empowering staff to recognize and respond appropriately to cyber threats."

Pros & Cons

With great power comes responsibility. AI decisions in both banking and cybersecurity must be:

- Transparent – Can we explain why a fraud detection system flagged a user?
- Fair – Are algorithms biased against certain groups?
- Regulated – Are there laws ensuring safe and responsible AI use?
- AI misuse or lack of governance could lead to invasion of privacy, discrimination, or overreach, especially in financial and security sectors.

Conclusion

As the digital world continues to evolve, AI isn’t just a tool—it’s a strategic partner in shaping the future of banking and cybersecurity. However, its success depends on balanced implementation:

- Technology + Human Insight
- Speed + Ethics
- Automation + Awareness

By investing in both AI innovation and human intelligence, organizations can build truly resilient systems ready to face both today's and tomorrow's threats.

Cybersecurity in Agile Product Development Cycle: Embedding Security by Design

by Dinesh Durai

Chief Digital Officer, Ideassion Technology Solutions

In today's fast-paced digital economy, organizations are under immense pressure to release products quickly, gain market share, and continuously deliver value to customers. Agile methodologies have become the standard approach to achieve this speed, allowing teams to break down work into smaller increments, collaborate effectively, and respond rapidly to changing requirements.

Yet, while Agile accelerates delivery, it also magnifies risks. Shorter release cycles mean there is less time for traditional, end-of-cycle security checks. Vulnerabilities that would have been detected in a waterfall model often go unnoticed in Agile until after deployment, when they are far more expensive and damaging to fix.

This is where embedding security by design becomes non-negotiable. Security can no longer be treated as a "bolt-on" or afterthought. Instead, it must be integrated into every sprint, user story, and release cycle. This shift requires organizations to adopt a DevSecOps mindset—where development, security, and operations are seamlessly aligned, and security becomes a continuous enabler of innovation, not a bottleneck.
Agility without security is fragile. Agility with security is unstoppable.

The Imperative of Security in Agile

Traditional models treated security as a separate gate that teams needed to pass after development. This created friction, delays, and often hostility between developers and security professionals. In contrast, Agile's core philosophy thrives on collaboration, iterative feedback, and shared responsibility. By embedding cybersecurity into Agile workflows, organizations achieve two critical outcomes:

1. Resilience by design – vulnerabilities are identified and addressed early, not after release.
2. Trust at scale – customers, regulators, and partners have confidence in the product's security posture.

Security in Agile Phases with Real-Life Lessons
To embed security into Agile, organizations must align it with each phase of the development cycle. Let's explore how this works in practice, along with real-world case studies that underline the consequences of neglecting security

Backlog & Planning
This is the foundation of secure Agile. If security is not considered at this stage, it is unlikely to be addressed later.

Key Practices:

- Define security user stories alongside feature stories (e.g., "As a system, I must encrypt sensitive data at rest").
- Include compliance requirements (GDPR, HIPAA,PCI-DSS) in the backlog.
- Conduct threat modeling workshops to anticipate risks from design to deployment.
- Prioritize backlog items with security impact through risk scoring.

Case Study: Capital One (2019)
Capital One's cloud misconfiguration exposed over 100 million customer records. Had security stories around firewall configurations and compliance checks been embedded in the backlog, this breach could have been prevented.
"Embedding security at the planning stage is cheaper than firefighting after a breach."

Cultural Shifts: Making Security Everyone's Job

Embedding security is not just about tools and processes—it requires cultural transformation. Agile thrives on cross-functional collaboration, and security must become a shared responsibility.
- Developers must treat security as part of coding craftsmanship.
- Product owners must balance customer value with compliance and risk reduction.
- Scrum masters must ensure security stories are not sidelined during sprints.
- Executives must champion security investment as a business enabler, not a cost center.

"Security isn't a speed bump—it's the guardrail keeping Agile on track."

Frameworks and Best Practices

Organizations can leverage established frameworks to embed cybersecurity into Agile:

- OWASP SAMM:- aligns security with development maturity.
- NIST DevSecOps Practices:- provides structured controls for integrating security into CI/CD.
- ISO 27034:- guidance on secure application development lifecycle.
- BSIMM:- benchmark for assessing security practices in Agile.

Challenges in Embedding Security

Despite best intentions, organizations face hurdles:

- 1. Speed vs. Security tension:– teams resist added steps in fear of slowing delivery.
- 2. Tool overload:– Integrating multiple scanners and tests can overwhelm developers.
- 3. Skill gaps:– not all developers are trained in secure coding.
- 4. Budget constraints:– security seen as a cost rather than a value.
- 5. Change resistance:– cultural inertia against shifting responsibilities.

Solutions include automation, training, leadership buy-in, and incremental adoption.

Future Trends: Where Agile Security is Headed

- AI-driven threat detection integrated into Agile pipelines.
- Automated compliance validation embedded into backlog items.
- Shift-left observability monitoring from the development phase onwards.
- Security as code codifying policies directly into pipelines.
- Quantum-safe cryptography future-proofing Agile security against emerging risks.

Enabling Innovation, Safely

Cybersecurity in Agile is not about slowing down innovation; it's about enabling it safely. Organizations that embed security by design deliver software that is resilient, compliant, and trusted by users. Each phase of Agile, from backlog planning to retrospectives, provides opportunities to strengthen security posture. The lessons from Capital One, Uber, Toyota, SolarWinds, and Equifax underscore one truth: neglecting security at any stage can have catastrophic consequences. But when security becomes part of Agile DNA, organizations can move fast without breaking trust.

"Speed wins the market. Security wins the customer."

The Bitter Truth: Global Data Governance & Security, Harmonization, Issues, and a Comparative Maturity Model

Umang Mehta

Founder - World AI Governance (WAIG)

Around the world, governments and regulators have been busy enacting privacy, cybersecurity, and AI governance frameworks. On paper, it looks like progress, GDPR in Europe, PIPL in China, DPDP Act in India, APPI in Japan, LGPD in Brazil, and so on. Each country wants to protect data, ensure security, and enable digital growth.

But here's the bitter truth: global data governance and security policies are not harmonized. They are fragmented, sectoral, sometimes contradictory, and often politically motivated. This creates compliance nightmares for businesses, weakens global cooperation against cybercrime, and leaves critical gaps in protection.

The time has come to confront this reality and build a comparative maturity model that highlights where nations stand, what misalignments exist, and how researchers, policymakers, and industry leaders can move toward genuine harmonization.

Global Approaches to Data Governance

From our comparative analysis of 50+ countries, three dominant approaches emerge:

1. **Adoption (Global Standards)**

- Countries like Kenya, Uganda, Seychelles, and Nepal align heavily with ISO/IEC, ITU, and OECD principles.
- Pro: Easy interoperability for international firms.
- Con: Limited local enforcement and weak cultural adaptation.

2. **Hybrid (Localized + Global Mix)**

- Seen in the US, Canada, India, UK, Brazil, Australia, Israel, and South Africa.
- Pro: Balances international standards with local priorities.
- Con: Creates sectoral gaps (e.g., US HIPAA/CCPA but no federal privacy law).

3. **Own Principles (Sovereignty-First)**

- Adopted by China, Russia, Saudi Arabia, UAE, Japan, Singapore, Qatar
- Pro: Strong national control, tailored to local policy objectives.
- Con: Data localization, sovereignty restrictions, and incompatibility with global norms.

The Misalignment Problem

The most striking misalignments include:

Data Localization vs. Data Flow:

- China's DSL & CSL require strict localization, while GDPR allows controlled cross-border transfer.
- India's DPDP Act initially leaned toward localization, now softened but confusion remains.

Privacy vs. Security Trade-offs:

- EU's GDPR maximizes individual privacy, but countries like Singapore and UAE balance privacy with state-led AI ethics and national security.

Sectoral Fragmentation:

- The US relies on sectoral rules (HIPAA, GLBA, CCPA), leaving gaps compared to comprehensive laws like GDPR or LGPD.

Maturity Gaps in Emerging Economies:

- Many African nations (Rwanda, Mali, Somalia, Sudan) have nascent or draft frameworks, heavily dependent on ISO/ITU guidance, with weak enforcement.

Case Studies

1. **Cross-Border Business Compliance (US–EU Data Transfers)**

- Case: Schrems II ruling invalidated Privacy Shield. Companies like Facebook faced billion-dollar fines.
- Lesson: Misaligned frameworks cripple international business.

2. **AI Governance (Singapore vs. EU)**

- Case: Singapore's IMDA AI Toolkit vs. EU AI Act draft.
- Lesson: Singapore focuses on industry adoption, EU on risk classification, hard for multinationals to comply with both.

3. **National Security & Sovereignty (China vs. India vs. EU)**

- Case: China enforces data localization; India oscillates; EU balances free flow with adequacy agreements.
- Lesson: Sovereignty-first models increase friction in supply chains.

GLOBAL DATA & CYBER GOVERNANCE MATURITY LEVELS

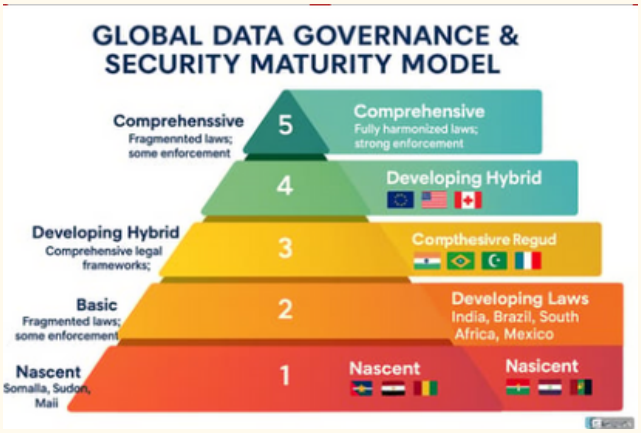
Level 1 – Nascent
- Draft laws, weak enforcement, ISO/ITU reliance.
- Example: Somalia, Sudan, Mali.

Level 2 – Basic
- Formal privacy/cyber laws exist but fragmented; no integrated enforcement.
- Example: Nepal, Pakistan, Bangladesh.

Level 3 – Developing Hybrid
- Combination of international standards and national frameworks; stronger institutions but gaps remain.
- Example: India, Brazil, South Africa, Mexico.

Level 4 – Advanced Hybrid
- Comprehensive legal frameworks, strong regulators, AI/sectoral guidelines.
- Example: US, UK, Canada, Singapore, Australia.

Level 5 – Sovereign Global Shapers
- Countries with extraterritorial reach and influence over global norms.
- Example: EU (GDPR, NIS2), China (PIPL, CSL), Japan (APPI), Russia (GOST).



For Researchers

Researchers should explore comparative studies that examine the impact of hybrid versus sovereign-first policies on innovation. There is also a need to create more comprehensive maturity benchmarking metrics that go beyond legal presence, incorporating factors such as enforcement strength, awareness levels, and the effectiveness of penalties.

For Policymakers

Policymakers should prioritize interoperability agreements—similar to the EU adequacy model or initiatives like the ASEAN Digital Pact to ensure smoother global data flows. Establishing regulatory sandboxes for testing alignment between local laws and international frameworks can also help. At the same time, they should avoid the pitfalls of "policy nationalism," which risks fragmenting digital ecosystems and hindering global collaboration.

For Industry & Practitioners

Industry leaders and practitioners should adopt "compliance by design" models, building modular frameworks that are adaptable to multiple jurisdictions—for example, GDPR-ready or HIPAA-ready structures. Leveraging maturity model mapping can support more effective planning for cross-border operations. In addition, investing in skilled Data Protection Officers (DPOs) and AI governance specialists with multi-jurisdictional expertise will ensure organizations remain agile, compliant, and future-ready.

The Bitter Truth

The world cannot afford data governance silos. Cyber threats, AI risks, and privacy violations don't respect borders. Yet, nations continue to treat data like oil, guarding it for sovereignty instead of enabling safe flows.

The bitter truth is this: we don't have a global standard, we have a global patchwork. Until harmonization efforts move from theory to enforcement, businesses will bleed resources in compliance battles, citizens will face uneven protections, and adversaries will exploit the weakest links.

The comparative maturity model isn't just an academic tool, it's a call to action. Harmonization is no longer optional; it's a prerequisite for a secure, trusted, and innovative digital future.

THE IMPORTANCE OF CYBER-SECURITY

~ Bantesh Singh

Cybersecurity is the foundation of digital resilience, essential for protecting IT systems against malicious attacks that can disrupt business operations and expose sensitive information. Without a robust cybersecurity strategy, organizations are left vulnerable to cybercriminals who exploit weaknesses for financial, political, or personal gain. In today's hyperconnected world, every device, application, and user account can become a potential entry point for attackers. As businesses adopt digital transformation at scale, the stakes are higher than ever where even a single breach can cascade into massive operational, financial, and reputational damage. Effective cybersecurity not only defends against threats but also builds trust, enabling innovation and sustainable growth in the digital economy.

Rising Threats in the Digital Age

Cyberattacks are escalating worldwide. In 2025, organizations face an average of 1,673 attacks each week a staggering 44% increase over the previous year. The global cost of cybercrime is expected to reach $10.5 trillion this year, making it one of the greatest economic threats to businesses and governments alike. This surge results from expanding digital footprints and increasingly sophisticated cybercrime tactics that create new opportunities for criminals.

The Modern Cybercrime Ecosystem

The cybercrime landscape has evolved dramatically. Sophisticated hacker groups and state-sponsored actors leverage advanced techniques, while the proliferation of Malware-as-a-Service allows less-skilled attackers to launch campaigns at scale. In 2025, more than 300,000 new pieces of malware are created daily, and nearly 2,244 daily cyberattacks threaten global organizations. Phishing, credential theft, and social engineering are still common, preying on weak organizational defenses and untrained staff.

Conversely, strong cybersecurity delivers

- Protection of sensitive data and reduced breach risks
- Improved business continuity and fewer disruptions
- Enhanced compliance with data security regulations
- A trusted brand image and secure adoption of modern work model
- A cyber-aware workforce trained in best practices

The Expanding Attack Surface

Adoption of cloud services, IoT devices, SaaS applications, and remote work models has created a complex web of assets and connections. Each innovation opens up new vulnerabilities, requiring organizations to constantly update their security posture. Notably, cloud-targeted attacks surged by 136% in just the first half of 2025, and identity-based intrusions remain a leading cause of breaches.

The digital workplace has blurred traditional network boundaries, meaning security teams must now defend not only data centers but also home offices, mobile devices, and distributed cloud environments. IoT sensors, smart devices, and third-party integrations often lack strong protections, making them easy targets for attackers seeking a backdoor into corporate systems. Moreover, the rapid adoption of SaaS applications while driving efficiency creates shadow IT challenges, where unauthorized apps bypass security controls and expose sensitive data.

This ever-growing digital footprint expands the "attack surface," giving adversaries more entry points to exploit. To counter this, organizations must embrace a proactive security model prioritizing identity protection, continuous monitoring, and zero-trust architectures that limit access and verify every interaction.

The Cost of Neglect

Ignoring cybersecurity can lead to-:

- Severe reputational damage and loss of customer trust
- Major financial losses from downtime, remediation, and regulatory fines
- Operational disruptions caused by data breaches or halted services
- Increased risks when adopting new technologies or digital business models

Conclusion

As digital dependence grows, cybersecurity is no longer optional it is a fundamental requirement for safeguarding both business continuity and reputation.

Aligning IT and Business in the Age of AI-Driven Digital Transformation

by - Gaurav Vyas

(Head of Information Technology at SPGPrints India)

In today's hyper-connected, AI-powered world, digital transformation is no longer a choice—it's a strategic imperative. But transformation without alignment is chaos. For organisations to thrive, the alignment of IT and business objectives must be intentional, continuous, and deeply integrated. This alignment becomes even more critical when considering the growing complexities of risk and cybersecurity in the digital era.

The New Paradigm: AI as a Catalyst for Transformation

Artificial Intelligence (AI) is transforming industries by automating processes, enhancing decision-making, and enabling the development of new business models. From predictive analytics in manufacturing to personalised customer experiences in retail, AI is the engine driving digital transformation.

However, AI's potential can only be fully realised when IT and business leaders collaborate to define shared goals. IT must evolve from a support function to a strategic partner—co-creating value, not just enabling it.

Strategic Alignment: More Than Just Communication

True alignment goes beyond regular meetings or shared dashboards. It requires:

- Shared Vision: Business and IT must co-develop a digital roadmap that reflects both technological capabilities and business aspirations.
- Integrated Governance: Joint decision-making frameworks ensure that technology investments are prioritised based on business impact.
- Cross-Functional Teams: Embedding IT professionals in business units fosters agility and innovation.

Risk and Cybersecurity: The Invisible Thread

As organisations digitise, they expose themselves to new vulnerabilities. AI systems, while powerful, introduce unique risksdata poisoning, model drift, and adversarial attacks, to name a few. Cybersecurity can no longer be an afterthought; it must be embedded into the digital fabric.

Key considerations include:

- Zero Trust Architecture: Assume breach and verify everything. This model is essential in a perimeter less, cloud-first world.
- AI Governance: Establish ethical and operational controls around AI usage, including explainability, fairness, and accountability.
- Cyber Resilience: Go beyond prevention. Build capabilities to detect, respond, and recover from cyber incidents swiftly.

The Role of Leadership

Leadership plays a pivotal role in driving alignment. CIOs and CISOs must speak the language of business, while CEOs and CFOs must understand the strategic value of technology. This mutual literacy fosters trust and accelerates transformation.

Moreover, boards must evolve their oversight to include digital and cyber risks as core components of enterprise risk management.

A Unified Approach

Consider a manufacturing firm implementing AI-driven predictive maintenance

Without alignment:

- IT might deploy a cutting-edge solution that business users don't adopt.
- Businesses might expect ROI without understanding data quality requirements.
- Cybersecurity might be bypassed, exposing critical infrastructure to threats.

With alignment:

- Business defines the problem and success metrics.
- IT selects and integrates the right AI tools.
- Cybersecurity ensures data integrity and system resilience.

The result? Reduced downtime, improved efficiency, and a secure, scalable solution.

THE FUTURE OF TECHNOLOGY NAVIGATING THE INTERSECTION OF AI, IT AND CYBERSECURITY

Kunal Chakraborty

IT HEAD AT GKB OPTICALS

The rapid evolution of technology has brought Artificial Intelligence (AI), Information Technology (IT), and Cybersecurity to the forefront of modern business. As these fields converge, organizations encounter both exciting opportunities and pressing challenges. This article explores how AI, IT, and Cybersecurity intersect, highlighting the benefits, risks, and strategies needed for long-term success.

AI is transforming the IT landscape by reshaping operations and enabling smarter decision-making. From predictive maintenance that anticipates issues before they cause downtime, to chatbots and virtual assistants that provide round-the-clock customer support, AI is creating efficiency and improving service quality. In software development, AI-powered DevOps and automation are accelerating testing, deployment, and monitoring, ensuring faster delivery and higher reliability. Collectively, these innovations are revolutionizing how IT teams work, freeing professionals to focus on strategy and innovation rather than repetitive tasks.

Cybersecurity in the AI Era

With the rise of AI comes a new wave of cybersecurity concerns. Cyber attackers are increasingly leveraging AI to develop sophisticated methods such as AI-generated phishing campaigns and intelligent malware. At the same time, the vast amounts of data required for AI systems introduce heightened risks around privacy and compliance. Another emerging challenge is adversarial AI, where attackers deliberately manipulate AI models to compromise their accuracy and reliability. These risks demand that businesses not only embrace AI but also rethink their security posture to safeguard digital assets effectively.

Strategies for Success

Successfully navigating this landscape requires a balance between innovation and protection. Organizations must invest in AI-driven security solutions that can detect and respond to threats in real time. Developing strong data protection policies is equally critical to ensure compliance and safeguard sensitive information. Close collaboration between IT and cybersecurity teams can bridge gaps, ensuring seamless integration of AI tools without compromising security. Equally important is investment in AI literacy and training, equipping professionals with the knowledge to harness AI's potential while staying alert to its risks.

Maximizing the benefits of AI in cybersecurity depends on disciplined practices. Organizations should continuously monitor AI system performance to ensure accuracy and detect anomalies early. Embracing explainable AI helps bring transparency to decision-making processes, building trust and accountability. Regular security audits remain vital, providing ongoing assurance that systems are resilient and compliant with evolving standards. Together, these practices establish a foundation for sustainable growth in an AI-driven world.

Beyond these measures, it is also important to establish clear governance frameworks that define how AI is implemented and managed across the enterprise. Continuous training and awareness programs can empower teams to identify emerging threats and adapt quickly. Partnering with industry experts and leveraging threat intelligence networks further strengthens defenses, enabling businesses to stay one step ahead of evolving cyber risks.

Conclusion

The convergence of AI, IT, and Cybersecurity represents both a challenge and an opportunity. Organizations that adopt strategic approaches, invest in intelligent solutions, and cultivate continuous learning will be best positioned to thrive in this dynamic digital era. As technology continues to evolve at an unprecedented pace, staying informed and proactive will remain the key to success.

BHARAT TRAILS

Explore the World

NOT JUST TRAVEL, A TRAIL WORTH TAKING

Advantages of Choosing Us:

- Best Tickets & Hotels
- Curated trips, zero stress.
- Easy booking, smooth travel.

NO STRESS, JUST TRAVEL.
REACH OUT NOW - WE'LL HANDLE THE REST.

bharattrails.travel@gmail.com

Wadala, Mumbai 400037/
Kalyan West Mumbai
421301

+91 836 952 3379/
+91 8097924815

bharattrails.co

THE MODERN CIO: ENABLING GROWTH, DEFENDING TRUST

By Anmol Sharma
Founder - World AI Governance (WAIG)

Just ten years ago, many Chief Information Officers (CIOs) were seen as caretakers of infrastructure-responsible for keeping servers running and applications online. Today, the transformation is profound: CIOs are now strategic leaders driving digital innovation, business agility, and resilience in a landscape shaped by rapid change and global competition.

At the core of this new mission is cybersecurity-not simply an operational necessity, but a strategic pillar for trust, compliance, and growth. Missteps can stall cloud migration, derail innovation, and erode customer confidence. So, how does a global CIO balance agility, risk, cost, and consistency across continents? For many, the answer lies in Fortinet's Enterprise License Agreement (ELA) and Enterprise Support Agreement (ESA)-two models designed to make information security a true enabler of business.

Tackling Complexity with Cost Predictability

For CIOs, budget unpredictability often hampers innovation. Traditional security vendors create uncertainty with licenses priced by data volume, user count, or number of devices-metrics that can fluctuate wildly and make planning a guessing game. Fortinet's ELA upends this approach by consolidating licenses under a single, multi-year contract, making cost predictable and easy to align with business strategy.fortinet+1

Instead of managing dozens of contracts, CIOs who move to ELA gain financial governance, simplified audits, and flexibility to reallocate licenses as priorities shift. As enterprises enter new markets or migrate workloads to the cloud, the ELA model eliminates the need for endless renegotiations.

"Predictable spend over multiple years allows IT leaders to confidently drive digital initiatives and long-term planning."

This financial certainty is not just convenience-it is a governance win. Boards and CFOs can allocate resources knowing that digital transformation projects won't trigger surprise expenses.

The Power of Global Consistency

CIOs overseeing international operations know that fragmented support is a hidden risk. Inconsistent service-level agreements (SLAs) mean one region might resolve an incident in minutes, while another struggles for hours. Fortinet's ESA offers unified, enterprise-level support-helping deliver consistent outcomes whether a branch is in Singapore, Paris, or São Paulo.fortinet+1

ESA isn't just reactive support; it includes proactive architectural reviews and best-practice guidance, transforming Fortinet from a simple vendor into a strategic partner. The result: streamlined incident resolution, continuous optimization, and assurance that every location benefits from the same high standards.

"With ESA, Fortinet becomes a partner invested in our resilience, not just a provider of break-fix responses."

Real-World Business Impact

Consider a multinational bank. By adopting ELA, it unifies licensing globally, streamlining compliance and reporting. ESA then ensures critical systems in any region get top-tier, consistent support, regardless of local differences.tei.forrester+1

Healthcare organizations use flexible licensing to expand telehealth services, confident that shifting workloads to the cloud is fully supported. Manufacturers deploying SD-WAN across plants worldwide benefit from frictionless scaling and uniform support.

Notably, the total economic impact of Fortinet's converged approach-a blend of ELA, ESA, and integrated Security Fabric-includes a 20% reduction in technology costs and a marked decrease in downtime. According to Forrester, enterprise customers have saved millions, improved operational agility, and strengthened business resilience.tei.forrester

Strategic Alignment: Enabling Tomorrow's Enterprise

The greatest advantage of Fortinet's ELA and ESA is their strategic alignment with enterprise ambitions. Today's CIO is measured not by the number of systems deployed, but by tech's impact on outcomes: resilience, customer trust, and growth.

ELA empowers CIOs to say "yes" to new business initiatives-knowing security and cost are predictable. ESA delivers the peace of mind that global support will be consistent and proactive. Together, they allow IT leadership to present a clear narrative to boards: security is not a barrier to innovation, but a foundation for safe and scalable transformation.fortinet+2

"Fortinet has enabled us to unify our approach, support growth, and maintain consistency everywhere we operate."

AI: THE DRIVING FORCE SHAPING THE FUTURE OF FINANCE

~ Naveen Bhadada

Introduction

Artificial Intelligence (AI) has moved from being a futuristic idea to a core driver of modern finance. No longer just an experiment, AI is now streamlining operations, strengthening security, and reshaping customer experiences. Finance is evolving from a back-office function into a strategic partner that influences business growth.

AI's Multifaceted Impact Across Finance

AI is transforming finance by automating processes like invoicing, reconciliations, journal entries, and expense management. What once took hours now happens in seconds, freeing professionals to focus on strategic work.

Fraud detection has become faster and more accurate, with AI spotting unusual patterns and preventing losses. In trading and investment, AI systems analyze markets and global sentiment at lightning speed, enabling smarter portfolios, sharper risk management, and an edge in high-frequency trading.

Forecasting and decision-making are also evolving. Predictive models, scenario planning, and real-time dashboards give finance leaders clearer insights into future outcomes and better strategic direction.

Customer engagement is being redefined through AI chatbots and virtual assistants that deliver 24/7 support, while human advisors focus on building deeper client relationships. At the same time, the finance workforce is shifting routine tasks are declining while skills in analytics, storytelling, and strategy are in higher demand.

Still, challenges remain. Data quality, ethical bias, and cybersecurity risks must be addressed carefully, and organizations must invest in training and governance to ensure AI empowers rather than replaces people.

Challenges and Opportunities Ahead

The opportunities presented by AI are immense, but they come with responsibilities. Organizations must balance innovation with accountability, ensuring that privacy is protected, systems are fair, and employees are adequately prepared. Strong governance frameworks and transparent practices will be critical to building trust. Those that manage this balance will not only gain efficiency but also redefine what financial excellence looks like in the digital age, setting themselves apart as leaders in a technology-driven future.

Conclusion

AI is no longer an accessory to finance—it is becoming the foundation. By automating processes, enhancing compliance, strengthening security, and enabling smarter forecasting, AI equips finance teams to be faster, more strategic, and more influential than ever before. Companies that embrace AI early will set the benchmark for the future of financial leadership. Beyond efficiency, AI offers a pathway to innovation, resilience, and sustainable growth. Those who lead this transformation today will define the standards of success for tomorrow's financial world.

AI + CYBERSECURITY: FRIEND, FOE, OR THE ULTIMATE ARMS RACE?

Sachin Godse

Pause. Think fast
Would you trust an AI to defend your company from hackers? Or do you worry AI could hack you faster than any human ever could?
Let's dive deep: what's powering the next generation of security—and what keeps CISOs up at night?

1.The AI Arsenal: How It's Changing Cyber Défense
Q: What's the biggest challenge in cybersecurity today?
A: Volume. Variety. Velocity. And creativity of modern threats. Imagine sifting through a billion logs per second!

Here's where AI flexes its muscles:
Anomaly Detection:
Machine learning algorithms (neural networks, Random Forest, SVMs) scan for outlier behaviour even if it's a zero-day exploit.
Threat Intelligence Mining:
Natural Language Processing parses security blogs, CVE archives, dark web chatter—feeding fresh clues into your SIEM.
Automated Response:
AI-driven SOAR platforms trigger instant quarantines, roll out patches, or even deceive attackers with honeytokens and sandbox environments.

Fast Fact:
Some top-tier EDR (Endpoint Detection & Response) tools now use deep learning to detect malware by file structure—not just signatures.

2.Hacker's Playground: When AI Turns Evil
Let's not pretend machines only work for the good guys.

Deepfakes for Phishing:
AI can generate synthetic voices or swap faces in video calls—making social engineering attacks frighteningly convincing.
Adversarial Attacks:
Want to confuse a neural net? Feed it manipulated packets or inputs.
Imagine image classifiers thinking a STOP sign is a speed limit sign—now apply that to IDS/IPS.

Automated PenTesting:
Generative AI can script new exploits on the fly, mutate payloads, and even write zero-click attack chains.

Quick Quiz:
Would your current SOC detect an AI-crafted spear phishing email that mimics your CEO's speech patterns? If you hesitated, the threat is already real.

3.Building Bulletproof AI Defences: It's Not Magic
Ready to deploy AI? Remember—your models are a fresh attack surface.

Adversarial Training:
Regularly retrain models with poisoned and clean data, hardening against manipulation.

Explainability:
Use LIME, SHAP, or XAI frameworks: if your AI blocks access, can it explain why (and can you prove it's not biased)?

Model Security:
Encrypt models at rest (homomorphic encryption or trusted execution environments),and enforce access controls for inference APIs.
Federated Learning:
Instead of shipping sensitive data, train models at the edge and only share weights/gradients—enhancing privacy.

Pro Tip:
Simulate red team attacks against your own AI. If your detection pipeline can't handle noisy or purposely altered data, patch those gaps quickly.

4.What's Next? Human + Machine = Unbeatable?
AI won't replace security teams, but it will make them smarter, faster, and less tired.
Expect convergence: AI-powered SOARs, self-healing networks, and unseen-predicting-past-unknowns.
Daily operations? More code, less checkbox compliance, and more focus on model governance and supply chain trust.
Ready For The AI Security Arms Race?
What's one AI-powered security tool you couldn't live without?
Or share: What nightmare scenario keeps you staring at your dashboard at 3AM?
The future of cybersecurity depends on all of us—humans and machines alike.

Cybersecurity is no longer just an IT checklist, it's about building resilience into the very fabric of the organization

By **Ravi Kajaria**
Founder of **Granuler**

In most boardrooms today, conversations revolve around growth, digital transformation, and risk. Yet for many mid-sized enterprises — the ₹100 Cr to ₹3000 Cr firms that power India's economy — IT still sits on the sidelines, seen more as a cost center than a growth driver.

When it comes to **cybersecurity**, the gap is even more dangerous. Too often, promoters assume it's "an IT department problem." In reality, cyber risk today is a **business continuity issue** — and, for some companies, an existential one.

After 25 years of leading IT in global enterprises and now working closely with promoter-led businesses at **Granuler**, I've seen how the absence of strategic IT leadership exposes organizations to inefficiency, wasted investment, and rising cyber threats.

It's time to rethink IT and cybersecurity — not as technical concerns, but as boardroom priorities.

The Hidden IT Gaps

Unlike multinationals with dedicated CIOs and CISOs, many mid-sized enterprises depend on piecemeal IT support. Vendors, consultants, and internal teams operate in silos, without alignment to business goals.
This creates three recurring problems:

1. **Strategic Blind Spot –** IT investments are reactive, not tied to business growth.
2. **Cybersecurity Neglect –** Firewalls and antivirus are mistaken for full protection. Attackers exploit governance gaps, not just technology flaws.
3. **ROI Black Hole –** ERPs, cloud systems, and analytics rarely deliver value because execution lacks ownership and governance.

The result: promoters feel IT is expensive and unreliable, employees feel frustrated, and businesses remain exposed to both inefficiency and cyber risks.

The New Mandate for IT

Enterprises that want to grow securely must reframe IT as a strategic enabler. That means:

- **Aligning IT with strategy** – Every technology investment should directly support business objectives, whether expansion, efficiency, or customer experience.
- **Embedding cybersecurity by design** – Security can't be bolted on later; it must be part of every process, platform, and governance structure.
- **Driving ROI from IT** – Every rupee invested must show measurable outcomes in scalability, productivity, or risk reduction.

This requires not just technology, but leadership.

Cybersecurity: A Business Risk, Not an IT Issue

Today, cybersecurity is about more than protecting servers — it's about protecting trust: customer trust, supply chain trust, and regulator trust.
For mid-sized enterprises, risks are amplified by:

- **Human factor:** Employees without formal training can unknowingly create vulnerabilities.
- **Shadow IT:** Business teams adopt new tools without IT oversight, creating invisible risks.
- **Limited governance:** Without senior IT leadership, cyber hygiene is inconsistent.

A ransomware attack or breach doesn't just cause downtime — it can paralyze operations and inflict lasting reputational damage.
That's why forward-looking enterprises are taking a **two-pronged approach:**

- **Investing in employee training** so end users: often the weakest link understand the risks of phishing, social engineering, and unsafe practices. A cyber-aware workforce is as critical as firewalls or encryption.
- Exploring **cyber insurance** as an added layer of resilience. Just as businesses insure plants and machinery, it's time to insure digital assets and continuity against potential breaches.

Cybersecurity is no longer just an IT checklist. It's about building resilience into the very fabric of the organization.

A Call to Promoters and CXOs

The digital economy is unforgiving. One weak IT decision can erase years of growth. But with the right leadership and governance, technology becomes a growth engine and a security shield.
To every promoter and CXO reading this:

- Don't treat cybersecurity as a checklist.
- Don't delegate IT strategy to vendors.
- Don't underestimate governance.
- And don't forget your people — a well-trained employee is your first line of defense.

Instead, bring IT into the boardroom. Surround yourself with leaders who can connect business strategy with technology execution. That's how Indian enterprises will modernize without chaos — and thrive securely in the digital era.

AI-Based Cybersecurity Management the Future

by Unmesh Deshpande

Is AI-Based Cybersecurity Management the Future? A Field Note for CIOs

Picture your SOC at 02:17 a.m. Alarms cascade, tickets flood, dashboards glare red. In the old world, analysts scramble. In the new one, an AI sentinel triages the noise, stitches events across endpoints, cloud, SaaS, and OT, quarantines a rogue workload, and drafts a precise incident report before a human blinks. Tempting? Sure. Inevitably, the future? Not without sober structure. Let's cut through the hype and answer the question with a narrative that's practical, MECE, and CIO-first.

What "AI-Based Cybersecurity Management" Actually Means

Across the lifecycle (Identify → Protect → Detect → Respond → Recover):

- **Identify**: AI infers your real asset inventory from telemetry, flags unknown shadow IT, and maps blast radii via attack-path modeling.
- **Protect**: It tunes policies (IAM, segmentation, DLP) to risk, not guesswork.
- **Detect**: It correlates signals (UEBA, EDR/XDR, NDR, CSPM, SaaS logs) to score intent, not just indicators.
- **Respond**: It orchestrates playbooks, auto-isolates devices, rotates creds, and opens tickets with human-in-the-loop gates.
- **Recover**: It prioritizes restoration based on business criticality and validates integrity post-restore.

By autonomy levels (Assistive → Adaptive → Autonomous):

- **Assistive**: Summaries, prioritization, suggested actions.
- **Adaptive**: Learns from feedback; safely executes with approvals.
- **Autonomous**(bounded): Acts within hard guardrails where speed beats hesitation.

The Boons (Why CIOs Lean In)

1) Scale & Speed
AI doesn't tire. It processes petabytes of telemetry, collapses dwell time, and slashes alert fatigue. Mean-time-to-detect and respond improves not by percentages but by orders of magnitude.

2) Signal Fidelity
Pattern-and-context beats signature-only detection. AI links "low" anomalies across identity, device, and cloud into a "high" campaign with a start, middle, and end. Fewer false alarms, fewer blind spots.

3) Proactive Defense
From breach-and-attack simulation to purple-team insights, AI keeps testing your controls, not annually—but continuously. It spots misconfigurations as they appear and proposes fixes with impact estimates.

4) Economic Advantage
Automated toil removal (enrichment, de-duplication, routing) means analysts focus on judgment, not janitorial work. You convert headcount from ticket clearing to threat hunting and control assurance.

5) Resilience by Design
Autonomous micro-isolation and least-privilege remediation reduce blast radius. Recovery becomes business-aware: restore revenue engines first, validate with AI-assisted integrity checks, and document for audit.

The Banes (Why CIOs Lose Sleep)

1) Model Risk (Accuracy, Drift, Adversaries)
False positives erode trust; false negatives invite ruin. Data drift degrades models quietly. Adversarial ML and data poisoning raise a new threat class: the model itself becomes an attack surface.

2) Explainability & Audit
"When did it know, why did it act, and who approved?" Regulators, boards, and insurers demand answers. Black-box decisions collide with compliance (ISO 27001, sectoral regs, privacy laws, and local data rules).

3) Process & Talent Debt
Automation without process maturity is just faster chaos. Playbooks age; access boundaries blur; "automation debt" accumulates. You still need architects who can speak model metrics, not just SIEM queries.

4) Platform & Vendor Lock-In
Closed feature stores, opaque pricing, and non-portable playbooks can trap you. Exits get expensive right when you're most dependent—post-breach or during audits.

5) Governance Liability
AI will act. When it blocks a surgeon's workstation at the wrong time or retains sensitive logs beyond policy, who's accountable? Governance gaps become legal gaps.

A Pragmatic Operating Model

Governance (who decides)

- Model Risk Committee: CISO, CIO, Legal, Data, and Ops own a living AI risk register.
- RACI for Autonomy: Define which actions are assistive, which need approval, and which are pre-authorized during defined incident severities.
- Model Lifecycle: Versioning, drift monitoring, retraining cadence, deprecation rules, and third-party model attestations.

Architecture (how it fits)

- Data Plane: Unified telemetry lakehouse with lineage, PII tagging, and retention controls.
- Model Plane: Feature store, evaluation harness (precision/recall, ROC, FPR by use-case), adversarial testing bench.
- Control Plane: SOAR + policy engine to enact changes across EDR, IAM, network, cloud, and SaaS.
- Trust Plane: Policy-as-code, approvals, evidence capture, and immutable logs.

Guardrails (how it stays safe)

- Human-in-the-Loop Defaults for identity changes, data access, and production segmentation.
- Kill Switch & Canary: Rollbacks within minutes; test changes in micro-segments first.
- Red Teaming & Chaos: Continuous adversarial exercises on the model and the orchestration layer.

Metrics (how you know it works)

- Leading: Data coverage %, model precision/recall, drift score, playbook success rate.
- Lagging: MTTD/MTTR, containment time, recurrence rate, cost-to-serve per incident, audit NCs, and business hours lost.

A CIO's Adoption Roadmap (Sequenced, Not Sprinkled)

Stage 0 — Baseline & Hygiene
Rationalize tools, fix logging gaps, inventory identities, and map controls to MITRE/NIST. If the data is messy, the model is mush.

Stage 1 — Assistive AI in the SOC
Start with enrichment, deduplication, narrative summaries, and priority scoring. Measure precision/recall; tune thresholds with analyst feedback loops.

Stage 2 — Adaptive Orchestration
Automate "safe" actions (block known bad hashes, turn off stale tokens) behind approvals—Codify exception handling. Introduce AI-guided hunt queries and posture recommendations.

Stage 3 — Bounded Autonomy
Pre-authorize micro-isolation on high-confidence detections, SaaS misconfig remediation within guardrails, and credential rotation for non-human identities.

Stage 4 — Enterprise Nervous System
Extend to OT/IoT, third-party SaaS, and DevSecOps. Align with business impact models so the AI defends revenue, not just servers.

What Won't Change (Anchor to First Principles)

- **Accountability:** The buck still stops with you. AI is a tool; accountability is a role.
- **Defense in Depth:** Layered controls, least privilege, backups, and drills will always matter.
- **Humans & Culture:** Phishing will still land; someone will still click. Training and tone-from-the-top remain decisive.
- **Table-Top Realism:** Practice awkward scenarios: "AI blocked the CFO's login mid-quarter close"—what now?

Vendor Questions That Separate Signal from Noise (MECE)

- Model Cards & Lineage: What data trained it? What populations underperform? How is drift reported?
- Security of the AI: How do you defend against data poisoning, prompt injection (for AI copilots), and model theft?
- Explainability: Can we see factors behind each decision and export them for audit?
- Data Boundaries: Where does data live? How is PII minimized? Can we enforce regional localization?
- Control & Exit: Can playbooks run on our SOAR? What's the migration path out?
- SLOs & Cost: Clear SLOs for precision/recall and response latency; transparent pricing tied to value—not just ingest volume.

So, is AI-based cybersecurity Management the Future?

Yes—but only the disciplined version of it. The future belongs to organizations that treat AI not as a silver bullet but as a force multiplier inside a governed operating model. The boons are real: scale, fidelity, and resilience. The banes are too: model risk, opacity, and lock-in. Your job is to engineer the asymmetry—capture the upside while capping downside with architecture, process, and metrics.

Here's the plain truth: attackers already use automation and AI. Standing still is moving backward. But sprinting without a map is just running in circles. Build the rails, then let the train run faster.

Your move, CIO: What is the single high-impact security action you're willing to let AI execute autonomously—today—and what is the one action you will never delegate to a machine?

EXCITING TRAVEL PACKAGES BY

BHARAT

ANDAMAN NICOBAR

13,000/-

HIMACHAL

17,999/-

UJJAIN

9,000/-

TRAILS

DUBAI

THAILAND

SINGAPORE

BHARAT TRAILS

Experience unforgettable journeys with our trusted tour and travel services.

+91 836 952 3379 bharattrails.travel@gmail.com bharattrails.co

INNOVATION WITHOUT INCLUSION: THE INCOMPLETE AI REVOLUTION

BY SACHIN MAHIND

Al: Balancing Innovation with Humanity

Artificial Intelligence (Al) is no longer a futuristic concept-it has become the heartbeat of Industrial Revolution 4.0. Smart factories, predictive analytics, web-based decision making. and mass customization are reshaping the way industries operate. Businesses today are witnessing an era where speed, adaptability, and intelligence drive competitiveness. Ideas and creativity, more than capital, are becoming the true currency for survival.

Yet, with every revolution comes responsibility. While Al opens doors to unprecedented growth, it also forces us to pause and reflect. How do we draw the line between technological efficiency and human sustainability? How do we ensure that innovation uplifts rather than disrupts society?

The Double-Edged Sword of Automation

Al adoption is no longer optional; it is a necessity for organizations striving for excellence. From automated production lines to Al-driven customer experiences, efficiency is being redefined. But efficiency comes with a price. Automation has the potential to displace millions of jobs, particularly for those in lower skilled or routine roles.

This displacement can create a dangerous imbalance. When livelihoods are threatened and people are left without purpose, idleness may become the "devil's workshop" Societies risk facing rising inequality, frustration, and even unrest if inclusive strategies are not in place

History has shown us that revolutions are double-edged. The first industrial revolution created jobs but aho disrupted livelihoods of artisans. The IT boom transformed economies but widened the skill gap. Similarly, if Al is not managed thoughtfully, it may deepen divides tuther than bridge them

Leadership Responsibility: Innovation with inclusion

The challenge for leaders is clear embracing Al without disturbing the social ecorystem. This requires vision, empathy, and decisive action. Al must not widen the gap between the rich and poor but instead become a bridge for opportunite

Three approaches vital here:

Reskilling and Upskilling

Workers displaced by machines must be equipped with new skills for tomorrow's roles. Reskilling programs, continuous learning platforms, and collatioration with academia are essential Corporates need to treat learning not as an event but as a continuous joumey

Inclusive Growth

Al should not be reserved only for elite organizations or privileged communities. MSMEs, rural entrepreneurs, and underrepresented groups must also find opportunities in this transformation. Public-private partnerships can play a huge role in democratizing access to Al-driven tools.

3. Human-Al Collaboration

The narrative must shift from Al replacing humans to Al augmenting humans. Machines are efficient at data crunching, but creativity, empathy, and ethical judgment qualities uniquely human-remain irreplaceable. Future-ready organizations will empower employees to work with Al rather than compete against it

Safeguarding the Future: The Ethics of Al

Beyond jobs and productivity, one of the most pressing concerns is data privacy in today's digital age, data is often described as the new oil. But just as oil can pollute, data too can be misused without ethical safeguardi

Every transaction, every decision, and every online footprint generates data. Without governance, this wealth of information can easily be weaponized-whether through surveillance, manipulation, or exploitation. Leaders must recognize that customer trust is fragile, one breach can undo years of goodwill

The solution les in transparent governance, stringent data protection frameworks, and global cooperation. Al ethics should not remain a buzzword-it must translate into boardroom priorities and actionable policies. Businesses that put ethics at the heart of their Ai strategies will stand out not just for their their intelligence, but for their integrity.

AI in customer experience enhances personalization, efficiency, and workforce management by leveraging data-driven insights to improve customer satisfaction, reduce costs, and boost agent retention. - Gaurav Pathak

AI in customer experience (CX) involves applying artificial intelligence (AI) technology to all components for customer experience & Agents Efficiency

Customer experience has become a valuable use case for AI-powered technologies as customers continue to expect more from businesses. AI technology deployed with this approach can include machine learning, natural language processing (NLP), Robotic Process Automation, predictive analytics and more.
Incorporating AI is a major component of any modern digital transformation journey.
enables businesses to tailor customer preferences and interactions, increasing customer satisfaction at the onset.
AI enhances customer interactions by analysing and sorting through vast amounts of customer data. The data analysis results in a highly personalized customer experience that addresses customer needs at all touchpoints and ramps up operational efficiency.
The capacity for data and in-depth analysis is what sets AI customer experience apart from other approaches. Its ability to detect patterns, review purchase history and monitor social media behaviour

Deliver hyper-personalised Interactions-AI can act like a personalised concierge for every customer, understanding their history and preferences, and allowing agents to better understand their needs.

Improve workforce management-Our CX Trends Report found that almost 80% of CX leaders are eager to increase their budget for better agent management tools. Many are starting to use AI in workforce management. Workforce management tools can automate tasks, provide data-driven insights and enable

AI ENGAGEMENT TO IMPROVE THE CX EXPERIENCE

decision-makers to plan their staffing needs proactively.

AI increases agent retention -We have resolved over 50K calls, we've lowered our agent attrition rate by half and over 90% of customers have given a favourable rating

By shifting to an AI solution that can fully resolve the majority of most common request types, contact centres like Love's are able to meet customer demand without increasing labour costs. Love's experienced transformational gains in savings, customer satisfaction and agent retention.

Securing the AI Frontier: Data Risks and Threats in Enterprise LLM Adoption

Damanjit Uberoi

AI adoption has quickly evolved from mere boardroom curiosity to mandate. Tools like ChatGPT, Claude, and Gemini are now embedded into daily workflows – enterprises stand on the edge of a transformational shift. Large Language Models (LLMs) power productivity, content generation, decision support, and even technical design.

These gains bring new, and often underestimated, risks. LLMs introduce a complex, evolving threat surface that most organizations are unprepared to secure. Worse still, premature or poorly guided AI adoption can expose even the most well-intentioned leadership to regulatory, reputational, and financial fallout.

This article explores the core technical threats to company data as LLMs take root in enterprise environments. It is written for security-aware leaders and technical decision-makers who must not only enable AI-driven innovation but also safeguard the data it depends on.

Each section highlights a key area of concern, outlines specific risks, and offers a framing insight to help enforce secure thinking. The goal is to equip you with the right questions, and to spark the right conversations as your organization navigates this AI frontier.

Data Leakage via Prompt Injection and Indirect Exposure
LLMs are not inherently safe. They're designed to be helpful, not secure. Malicious users can manipulate model behavior via specially crafted prompts, i.e., prompt injection, causing the model to divulge sensitive information.

Risks
Exposure of confidential documents used in training.
Accidental disclosure of internal prompt libraries or process logic Outputs that help attackers socially engineer employees.

Example Scenario: Customer-facing AI assistants revealing internal knowledge base contents through clever questioning.

Shadow AI Usage — Unmonitored LLM Access
Many employees are already using public AI tools without organizational approval in pursuit of productivity. This introduces unsanctioned dataflows outside your control.
Risks
Pasting sensitive data, i.e., source code, designs, contracts, into public tools like ChatGPT
No guarantees on data retention, reuse, or deletion
Legal or compliance violations depending on the jurisdiction or industry.

Watchpoint: Any unapproved AI tool used for real work is a potential vector for intellectual property (IP) loss.

Training Data Contamination
Organizations fine-tuning LLMs on internal datasets may inadvertently include sensitive or misleading data, leading to downstream risks.
Risks
AI systems inheriting biased behavior.
Reproduction of sensitive corporate content in generated output.
Model corruption through data poisoning attacks.
Reality: Unfiltered email archives or chat logs make poor training sources.

Hallucinations Leading to Business Risk
LLMs are confident, articulate, but not always correct. A hallucinated output can be dangerously misleading in enterprise scenarios.
Risks
Poor executive decisions based on inaccurate AI-generated summaries.
Legal or compliance missteps from hallucinated interpretations of regulations
Technical errors introduced by AI-generated code with subtle flaws.
Concern: Business leaders trusting output without proper levels of human review.

Intellectual Property Leakage via Model Interoperability
Even enterprise-grade AI platforms rely on third-party APIs. Organizations may lose control over how their data is stored, retained, or reused when internal data is shared with an LLM vendor.

Risks
Exposure of trade secrets or internal logic
Cross-border data flow violations
Legal gray zones around derivative data ownership
Crucial: Understand your model provider's data handling policy.

Data Sovereignty and Compliance Gaps
Where is your model running? What laws govern it? Who has access to inference logs?

Risks
Violations of data residency mandates, e.g., GDPR, HIPAA
Inability to provide audit trails in regulatory investigations.
Legal complications in cross-border breach scenarios.

Red flag: Many LLM platforms do not offer geographic inference isolation or compliance logging.
Security Pitfalls in Retrieval-Augmented Generation (RAG)
RAG is increasingly used in enterprises to ground LLMs in company knowledge without retraining them.
This approach reduces upfront model risks; however, it introduces a fresh set of vulnerabilities in the retrieval layer itself.

Technical Risks
Poisoned Retrieval Corpus – Attackers can insert manipulated documents into the knowledge
base, producing outputs that look authoritative but are dangerous or misleading.
Context Window Leakage – Sensitive documents accidentally indexed may be revealed
verbatim when retrieved.
Prompt Injection via Retrieved Data – Malicious instructions hidden in indexed text can subvert the model during generation.
Broken Access Controls – Many RAG implementations lack user-level filtering; once a document is indexed, it is accessible to anyone with query access.
Cross-Tenant Contamination – Poor isolation could expose one customer's sensitive data to another, especially in MSSP or multi-tenant settings.

Business Risks
False Confidence from "Grounded Hallucinations" – Leaders may trust outputs more since they're tied to real documents. If the documents were poisoned or outdated, errors are amplified to a greater scale.
Operational Blind Spots – Enterprises wrongly assume 'RAG = safe'. This complacency delays governance until leaks or poisonings are systemic.
Regulatory/IP Exposure – Auditors may question who approved sensitive documents for indexing due to inherent lack of lineage and audit controls.
High Cleanup Costs – Once a RAG index is poisoned or over-shared, remediation is far harder than fixing a one-off prompt. Continuous governance is non-negotiable.

Bottom line: RAG often reduces training complexity at the expense of opening a new attack surface.
Security teams must treat retrieval pipelines with the same rigor as they treat core model usage.
The Danger of Premature AI Adoption
Rushing into AI adoption without a security and governance framework is akin to deploying untested
software directly into production.

Minefields to Avoid
Pilots turn into production systems without oversight.
Undocumented dependencies on external AI infrastructure
Lack of internal alignment on acceptable data exposure levels.
Untrained staff relying on AI-generated output in high-stakes workflows.

Premature adoption isn't just about bugs; it's about losing control of your data ecosystem before you even realize what's at stake.

Recommendations for Leadership
1.Define an LLM Security Policy
Restrict model use by classification level of data.
Mandate enterprise LLMs with internal logging and audit trails.

2.Enable Model Usage Governance
Maintain oversight on fine-tuning datasets.
Embed guardrails and human-in-the-loop mechanisms.

3. Develop an LLM Red Teaming Program
Simulate prompt injection and model misuse.
Regularly assess output hallucination boundaries

4. Invest in Explainable AI (XAI) and Model Auditing
Choose providers that support transparent reasoning chains.
Maintain logs of prompt-output pairs for critical workflows

5. Implement Data Minimization Principles
Sanitize inputs before model access.
Enforce least privilege access to training and inference datasets.

While LLMs are powerful enablers of business transformation, their integration must be purposefully calibrated not only for performance and efficiency, but also for risk containment. These models are not just another IT investment; they represent a paradigm shift in how organizations use, share, and protect
knowledge.

Enterprises that move fast must also move smart. Overlooking the emerging data risks can undermine the very resilience and productivity that AI is meant to enhance.

Those who treat AI as a strategic asset must address its risks with the same seriousness reserved for any
new class of critical infrastructure.

In AI adoption, a 'security-first' tenet is no longer optional; it is foundational.

THE AI-DRIVEN IT REVOLUTION: RESHAPING WORKFORCE SKILLS WITH OUTCOME-BASED MODELS

PROF. DR. DIPAK TATPUJE &
MAHESH BHANDIGARE

The IT Industry is undergoing a profound transformation, driven by the emergence of Artificial Intelligence (AI) and a fundamental shift from traditional "time and materials" billing to outcome-based models. This revolution is not merely altering service delivery; it is reshaping foundational business models and, critically, necessitating a revolutionary redesign of manpower reskilling to adapt to new realities.

Outcome-based models mark a significant departure from the past, where clients paid for hours spent, regardless of impact. Currently, payments are directly tied to measurable results, such as improved system performance, delivered features, or business growth. This shift is fuelled by clients' demand for clear value, the need for stronger alignment between client and provider goals, and intense industry pressure for differentiation in an AI-driven and saturated market.

While companies like Globant pioneer outcome-based models with AI Pods, such innovations underscore a pressing challenge: the disruptive impact on the workforce and economy. This transition highlights the urgent need for reskilling, bridging the gap between legacy operations and future demands." These pods promise rapid time-to-market, cost efficiency, and scalability, demonstrating the potential of this new approach.

Outcome-based models are directly tied to measurable results rather than hours worked and are fundamentally reshaping the IT industry. Innovations such as the "AI Pods" model exemplify this shift, offering subscription-based, outcome-aligned teams that combine agentic AI with expert human oversight to deliver continuous, impactful results. This paradigm shift necessitates radical reskilling of employees. Traditional project management and technical skills are becoming obsolete as the focus shifts to AI orchestration, data engineering, cloud technologies, and cybersecurity.

Employees must develop the ability to collaborate effectively with AI, providing the "expert human oversight" crucial for AI Pods, and adapt to agile, product-centric methodologies. It is imperative to cultivate a workforce capable of leveraging AI to deliver specific, measurable business outcomes, demanding continuous learning and a proactive approach to skill development.

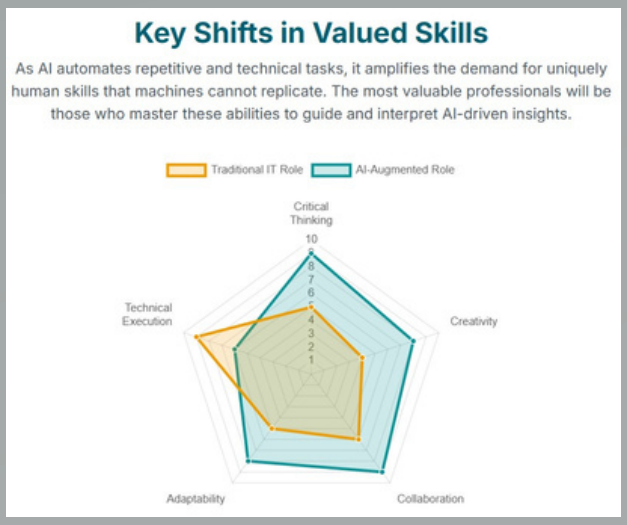
The flip side of this AI-driven evolution is its disruptive impact on the workforce and the economy. Legacy IT giants have experienced significant layoffs, such as the redundancy of employees at the middle and senior levels, even if not solely attributed to AI automation. The primary drivers of these workforce reductions are skill mismatches and the inability to redeploy workers into roles demanding new technologies and operating models.

Many employees with traditional project management or technical skills find themselves without a clear place in the new agile, product-centric, and AI-enabled work environment that is emerging. The pressure for leaner, tech-forward workforces, coupled with outcome-driven expectations and automation, is forcing established firms to reassess their talent strategy.

Recognizing this revolutionary shift towards new competencies, it becomes evident that designing effective reskilling programmes is fraught with challenges, including cultural resistance and financial constraints. It is no longer sufficient to merely understand specific tools; employees need to develop competencies in AI, data engineering, cloud technologies, and cybersecurity. More importantly, they need to cultivate adaptability to agile, product-centric methodologies and the ability to collaborate effectively with AI-augmented work flows. Therefore, reskilling must be designed to foster a mindset that embraces continuous learning and innovation, preparing the workforce for roles that involve overseeing AI orchestration, interpreting predictive analytics, and managing autonomous workflows.

Designing reskilling for this new era also means acknowledging significant challenges. Beyond financial investment, there is the hurdle of change management and cultural resistance within organizations. Employees must be guided through a profound shift in their professional identities and responsibilities. The new reskilling imperative is not just about upgrading technical skills; it is about transforming talent to navigate an IT ecosystem where value creation and accountability are paramount.

The convergence of outcome-based models and AI-driven automation is irrevocably altering the IT landscape. This revolution compels organizations to fundamentally rethink their workforce strategies, making comprehensive and forward-looking reskilling urgent priorities. Future IT professionals must be proactive learners, adept at leveraging AI, and aligned with delivering measurable outcomes, effectively acting as navigators steering a highly efficient, AI-powered ship.



Points on Future Manpower:

1. Proficiency in Future-Focused Technologies: Future manpower will require extensive reskilling in areas such as AI, data engineering, cloud technologies, and cybersecurity to adapt to the evolving IT landscape.
2. Adaptability to Agile and Product-Centric Models: The workforce must move beyond legacy project management and technical skills, embracing agile, product-centric, and AI-enabled work models to remain relevant.
3. Continuous Learning and Innovation Mindset: Given the rapid technological advancements, future IT professionals will need to cultivate a mindset of continuous learning, embracing change, and investing in new skills to align with outcome-centric realities.
4. Outcome-Oriented and Value-Driven Focus: Employees will need to align their efforts directly with delivering measurable business outcomes, moving away from time-based efforts to focus on tangible results, such as improved system performance or business growth.
5. Competence in AI Orchestration and Collaboration: Manpower will increasingly work alongside and oversee AI, requiring skills in managing autonomous workflows, interpreting predictive analytics, and effectively collaborating with AI-augmented systems, as exemplified by models such as AI Pods.

(Prof. Dr. Dipak Tatpuje is a researcher in AI reskilling and Mahesh Bhandigare is a Test Automation Architect.)

Harnessing Artificial Intelligence for Next-Generation Cybersecurity

by

Pranav Paranjpe

Introduction

Artificial Intelligence, or AI, is the buzzword doing rounds prominently in the last 3 to 5 years. AI is the set of algorithms that enables computers and machines to simulate human intelligence and problem-solving capabilities. The use of AI can be very beneficial for detection, analysis and response to cyberthreats. AI uses machine learning algorithms to continuously evaluate and learn based on the system generated data. When generative AI identifies certain known cyberthreats, such as malware, it can help contextualize threat analysis and make it easier to understand by generating new text or visual attack patterns to describe what's happening. Some of the activities related to AI include speech recognition, learning, planning, problem-solving, etc. The key benefit with AI into a cybersecurity strategy is its ability to protect and defend an environment when any malicious attack begins, thus mitigating and minimising impact. AI can take immediate actions against the malicious attacks when threats impact a business.

AI in Cybersecurity Trends

Predictive Threat Analysis: AI-powered risk models and algorithms are enabling security systems to predict attacks before they happen. By analysing massive amounts of historical and real-time data, these systems can identify early warning signs and stop threats in their early stages minimising the impact.

Zero Trust with AI Verification: The Zero Trust Architecture is becoming smarter with AI integration by verifying every user and device continuously ensuring that no one is trusted by default even inside the network. AI helps make this process seamless and more accurate.

AI + Blockchain for Data Security: AI and blockchain are being used together to create tamper-proof security systems. While blockchain ensures data integrity, AI monitors for suspicious activity, making it harder for attackers to manipulate or steal sensitive information.

Next-Gen Security Operations Centres (SOC): AI is powering self-managing SOCs that can monitor, detect, and respond to threats without constant human input. This automation allows security teams to focus on critical decisions rather than routine alerts.

Problem at hand and how can AI rescue Us?

Cyber-criminal organizations have already started investing into machine learning, automation, and AI to launch large-scale, targeted cyberattacks against organizations. The number of threats and potential for ransomware impacting networks continues to grow. The organizations fear AI-powered attacks increasingly compromise sensitive data and the security teams are having sleepless nights due to the complexity of AI attacks. The same AI can be effectively used to drastically improve security team's efficiency and productivity, giving them an advantage over potential cyber criminals. From AI-generated phishing emails to deepfake frauds, security teams must fight fire with fire. AI for cybersecurity works by evaluating massive amounts of data across multiple sources to identify patterns of activity across an organization. These AI algorithms perform the evaluation by cutting through the noise of daily security alerts and false positives. The patterns monitored especially include (but not limited to) data on when and where users sign in, their traffic volumes, the devices being used to log-in and applications that users use. These mundane tasks once were handled by L1 or L2 engineers can now be handled by AI efficiently and with a shorter turnaround. AI, when properly trained, has the capability to monitor, detect, and respond to malicious behaviours faster than humans alone. Once AI understands what's typical, it can identify anomalous behaviour that may need to be investigated further

Challenges & Limitations of AI in Cyber security

While AI is transforming cyber security, it's not a magic wand. Like any technology advancements, it comes with its own set of challenges and limitations. From high implementation costs of AI enabled security tools to the risk of AI bias, organizations must carefully strategize before relying on AI as their primary defence. Understanding the limitations is crucial to building a balanced and effective security strategy.

How will AI impact cybersecurity in the future?

As opportunities and growth knock at the doors of digital fortresses, threats await to pounce at every chance they get, destabilizing progress, disrupting operations, robbing data, and tarnishing reputation.

The emergence of AI has birthed possibilities for both defenders and attackers alike. It has, however, become a double-edged sword, providing businesses with the capability to transform while offering cybercriminals a means to make their offense more devastating.

Cybercriminals are using AI to hyper-personalize their phishing campaigns more effectively by tailoring them to their target's tonality and communication style. It has made it easier for low-skilled threat actors to craft sophisticated phishing campaigns.

Through weaponization, cybercriminals can create more harmful malware that can help them enhance persistence while remaining undetectable. They can also use AI-driven bots to gather open-sourced intelligence on their targets. The world's first AI-driven ransomware, PromptLock, reflects the threat that AI-powered threats could pose.

It shows how AI can be used to automate all the stages of a ransomware attack, from identifying & grouping data for exfiltration, to deciding whether to exfiltrate or encrypt data, and generating a ransom note.

It showcases how cybercriminals in the future will use AI and ML to create more dangerous payloads and adaptive ransomware that utilizes reinforced learning and multilayered systems that automatically get smarter based on their target defenses. It also proves that prompt injection will be the next big threat, especially for those organizations with unregulated AI usage.

While AI-powered threats present a whole new ballgame for defenders, it has also unlocked a range of possibilities. It can help organizations analyse large sets of data in a short span of time, predict patterns, and identify vulnerabilities at super speed, helping organizations to considerably reduce their time to detect and respond to threats with limited teams.

AI can help automate IR functions, like malware quarantining, threat detection, response, and containment. It will create more bandwidth for security teams to focus on critical aspects like improving their readiness against threats like ransomware, preparing a more robust cybersecurity strategy, and working with compliance experts to improve compliance with regulations.

While the idea of fully automated cybersecurity sounds interesting, it can miss critical alerts and be susceptible to AI-based threats.

It could make matters worse for organizations that already struggle with immediate challenges, like siloed solutions, rising cost and complexity of cybersecurity, limited visibility and control, and changing regulations.

It calls for a balanced approach that blends AI and human expertise. A way to achieve this is through the platformization of cybersecurity that unifies all the security solutions. Through a centralized platform, security teams can shift security left and automate routine security tasks that consume their time, allowing them to focus more on critical security alerts. They can extend their visibility, improve their control, and gain real-time insights to quickly respond to threats and improve their compliance.

Ultimately, organizations must not lose focus on awareness, educating employees on the data security risks associated with the use of LLMs, with some best practices to securely use them. They must create a detailed training program based on proactive assessment of awareness gaps across different levels to mitigate human error before it dominoes into a security incident.

Through shared efforts from management and workforce, cybersecurity can become part of the culture, helping organizations minimize risky behavior, mitigate human error, detect insider threats, and enhance readiness against threats.

AJAY NAWANI

CEO AT SHARKSTRIKER INC.

Aijaz Ur Rahman Quraishi Mohammed

About the Author:
"Aijaz Ur Rahman Quraishi Mohammed" is driving Qatar's Public Sector IT transformation through leadership in ERP, data operations, and cloud strategies. He is focused in digital transformation, governance, security, and disaster recovery, ensuring resilient and future-ready IT ecosystems. With expertise in audits, risk management, vendor engagement, and program delivery, he bridges strategy with execution to align technology with organizational needs.

Conscious and Ethical Technology Adoption: Navigating Digital Transformation and AI with Responsibility

Alright, lets shift the gears, let's get technical about the topic.

Digital Transformation (DT) and Artificial Intelligence (AI) are no longer just buzzwords; they're fundamentally reshaping the way organizations operate, deliver value, and plan for the future. While these technologies bring speed, comfort, and efficiency, their adoption must be conscious, ethical, and human-centered. DT is not just about adopting tools; it's about reimagining processes, culture, and customer engagement to create more agile and data-driven organizations. AI takes this further by enabling automation, smarter decisions, and new business models making transformation faster, measurable, and scalable.

However, many organizations dive into DT and AI projects without fixing the basics; they often have fragmented data, siloed systems, and unclear objectives, this must be fixed first. Without a strong foundation of clean, integrated, and secure data, even the most advanced AI initiatives are bound to fail. Cultural resistance is another barrier, people on the other hand, often view transformation as a threat rather than an opportunity. Modernization is mistaken for transformation etc. This way, organizations risk upgrading tools without truly reimagining how value is delivered.

In the end, conscious and ethical adoption of DT and AI is not optional, it's essential for long-term success. Organizations that prioritize data integrity, workforce readiness, and responsible innovation will not just adapt to the future, they will shape it.

The leaders of tomorrow will be those who recognize that transformation is not about replacing humans with machines, but about empowering people through technology to create a more resilient, inclusive, and sustainable future.
Thank You!!
--- AJ

So, what's the solution?

Success doesn't come from technology alone; it requires strong leadership commitment, cultural readiness, people empowerment, streamlined processes, and most importantly, a solid data strategy. Data must come first, a unified, accurate, and trustworthy data (consolidated, validated, and accessible across ERP, CRM, and all legacy stacks). Poor or fragmented data is one of the biggest reasons DT and AI projects fail, as feeding bad data into advanced systems undermines transformation from the start. That's why investing in data quality, governance, and ethical practices should be non-negotiable.
Additionally, strong governance frameworks should ensure fairness, accountability, and ethical AI use. At the same time, organizations should adopt an agile, modular approach: start small, demonstrate value, and scale up gradually. This not only reduces risk but also builds confidence across teams and stakeholders.
At the core, digital transformation is about people, empowering employees with new skills, preparing them for change, and building trust. When done right, DT and AI together can create sustainable progress, blending innovation with responsibility. The future belongs to organizations that don't just chase technology but use it consciously and ethically, keeping humanity at the heart of transformation.
AI, when responsibly embedded into transformation, can be the true accelerator. From automating manual processes to delivering predictive insights, AI enables smarter decisions and faster results. It makes transformation measurable, adaptive, and scalable. But success hinges on adopting AI with transparency, fairness, and inclusivity in mind. Only then can it serve as a tool for empowerment rather than exclusion.

BHARAT TRAILS

Presents

AMRITSAR TRIP

START FROM
₹15,000
4 DAY / 5 NIGHT

Inclusion:

- Hotel Stay
- Sightseeing
- Transport
- Food

About us:

Whether it's spiritual trails, vibrant festivals, or offbeat team getaways, our experiences go beyond sightseeing — they're about meaningful moments, authentic encounters, and leaving a lasting trail wherever you go.

Atul Jadhav
+91 836 952 3379

BOOK NOW

bharattrails.co

JOURNEY FULL OF Memories

Tailored Tours for Every Explorer

BALI

Benefit Services

- Airline Ticket
- Concierge Services
- Event Management
- Corporate Travel

For More Info
+91 8097924815

Visit our webiste
www.bharattrails.co