

An Initiative of



Concept by



India Inc. Digital Playbook 2025



CONTENTS

03 Preface

07 Executive Summary

09 Digital Strategy & Transformation Journey

15 AI Integration & Automation

21 Cybersecurity Threat Landscape

27 Workforce Evolution & Digital Skills

32 Regulatory Compliance & Governance

37 Key Contributors

Founders:

Ashish Srivastava

Anupam Gupta

Management:

Vaibhav Kumar, Vice President, Tech Disruptor Media, BNG

Atul Kumar Pandey, Director - IT & Digital Strategy, Tech Disruptor Media, BNG

Research, Edit, and Analysis:

Nisha Sharma, Senior Tech Correspondent, Tech Disruptor Media, BNG

Praneeta, Senior Correspondent, Tech Disruptor Media, BNG

Design:

Vipin Rai, AGM - Art & Designing, Tech Disruptor Media, BNG

Prachi Gupta, Executive - Graphic Design, Tech Disruptor Media, BNG

Operations:

Taposhi Bose, Assistant Managers - Sales & Marketing, Tech Disruptor Media, BNG



PREFACE

The year 2025 marks a pivotal chapter in the digital evolution of Indian enterprises. As organizations accelerate technology-driven transformation, the intersection of AI adoption, advanced analytics, cloud integration, and heightened cybersecurity demands is redefining what it means to compete and thrive in the Indian economy. This momentum is met with increased regulatory scrutiny, the rapid emergence of new threat vectors, and an acute need for digital and workforce resilience.

India's marketplace is more interconnected and tech-driven than ever before. Boardrooms and C-suites are prioritizing not just technology investments, but also the governance, security, and skill-building initiatives required to secure their organizational futures. The convergence of business model innovation, regulatory change, and digital risk is reshaping traditional operational and leadership paradigms.

About the India Inc. Digital Playbook 2025 Report

To provide actionable insight into this changing landscape, the first edition of India Inc. Digital Playbook 2025, by Tech Disruptor Media, captures the voices and strategies of senior technology and business leaders across India. The report offers a benchmarking lens into digital and AI maturity, cybersecurity posture, operational challenges, regulatory priorities, and workforce readiness. It is designed to help enterprises, policymakers, and industry stakeholders:

- Benchmark their digital strategies and maturity against peers
- Identify prevailing threats and operational constraints
- Evaluate the impact of regulatory trends on technology adoption
- Assess the evolving skills landscape and workforce readiness

**Tech
Disruptor**
media.com

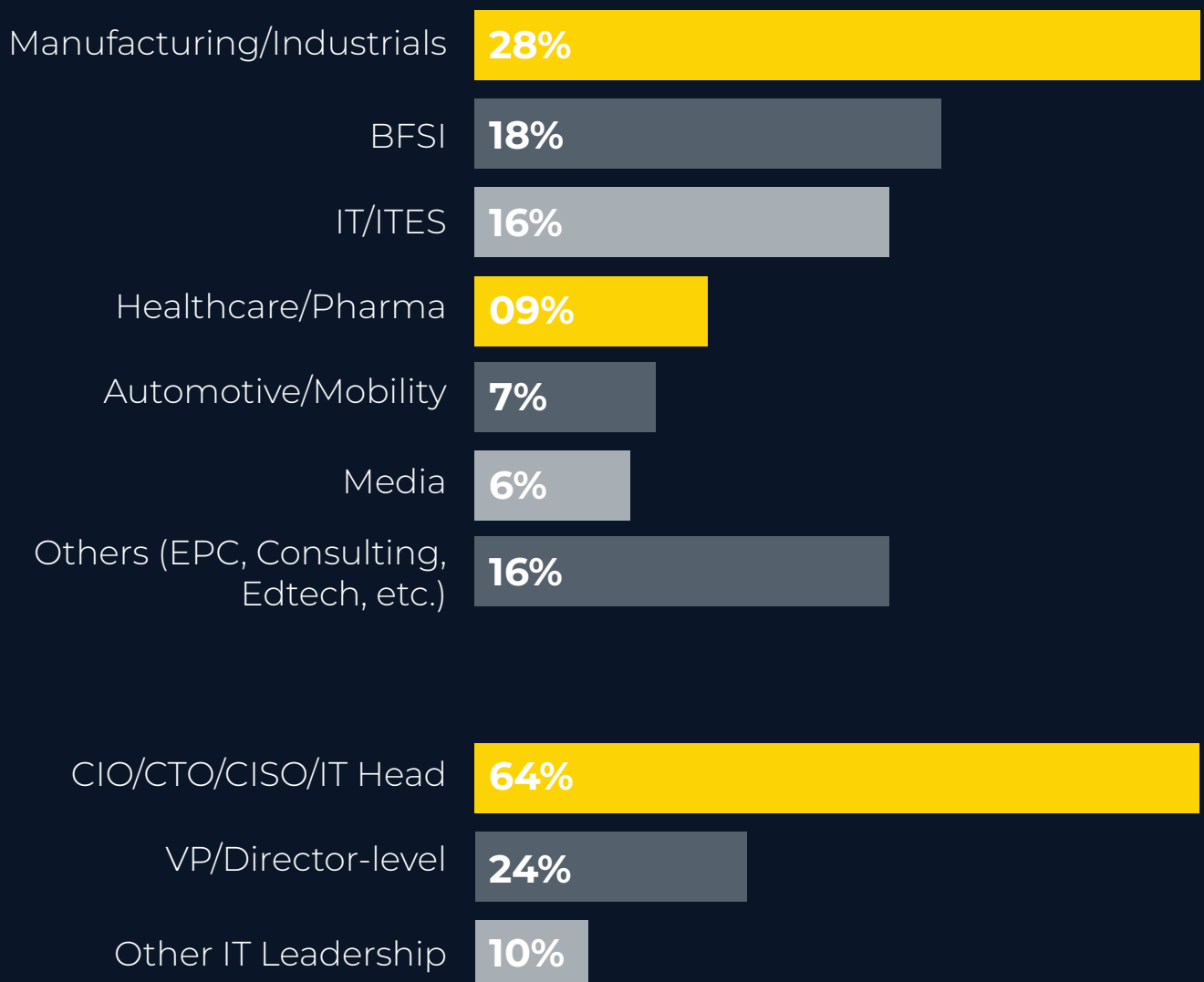
About Tech Disruptor Media

Tech Disruptor Media, a brand of Bharat Network Group, is a new-age B2B media and intelligence platform that shines a spotlight on the trailblazers transforming enterprise technology. We explore the dynamic intersection of emerging tech, business strategy, and industry disruption - curating conversations with visionary CIOs, CTOs, CISOs, and digital leaders who are driving real-world innovation, bold thinking, and measurable impact.

Survey Universe and Methodology

The report is based on an analysis of responses from senior leaders across various sectors, including BFSI, manufacturing, IT/ITES, healthcare, automotive, media, and others. Respondents include CIOs, CTOs, CISOs, IT heads, and functional leaders, ensuring a comprehensive, real-world perspective on strategic issues facing Indian enterprises in 2025.

Respondent Profile Snapshot



Scope and Structure of the Report

The report is structured to guide readers through the most critical areas shaping technology leadership and digital transformation in India today:



Digital Strategy & Transformation Journey

How organizations are progressing along the maturity curve, key catalysts, and persistent barriers.



AI Integration & Automation

The extent, impact, and obstacles of enterprise AI adoption.



Cybersecurity Threat Landscape

The shifting nature of risks, emerging threats, and defenses.



Regulatory Compliance & Governance:

The evolving complexity and organizational responses to regulatory demands.



Technology & Operations

The challenges and solutions in building operational resilience through cloud, hybrid, and integrated platforms.



Business Drivers & Policy Needs

Strategic objectives for AI and digital investment, and the policy ecosystem requirements for sustained progress.



Workforce Evolution & Skills

Assessment of skill gaps, upskilling strategies, and cultural dynamics in digital adoption.

Why This Report Matters

With Indian enterprises moving into a new era marked by digital urgency and regulatory transformation, having clear benchmarks and actionable insights has never been more valuable. The India Inc. Digital Playbook 2025 report provides technology and business leaders with a current-state assessment and forward-looking perspective — equipping them to make strategic, data-driven decisions on their digital future.

Executive Summary

The India Inc. Digital Playbook 2025 captures the perspectives of approximately 56 senior technology executives from diverse Indian industries, including BFSI, manufacturing, IT/ITES, healthcare, and media. Their responses provide a comprehensive snapshot of where Indian enterprises stand in their digital transformation journey, highlighting both the opportunities gained and the challenges that persist amid rapid technological change.

A striking insight from the survey is the stage-wise progression of AI and analytics adoption within these organizations. While 41% of respondents report being in the piloting or partial implementation phase of AI integration, only 14% have successfully embedded AI

as a fully integrated aspect of their operations. Another third of organizations (32%) remain in the planning or exploratory phase, signaling significant potential for growth yet reflecting the cautious approach enterprises take toward these emerging technologies.

Legacy technology systems continue to impede digital transformation efforts, with 34% identifying outdated technology infrastructure as a primary barrier. This challenge is compounded by a persistent shortage of skilled talent, with 32% citing gaps in digital capabilities—especially in AI, cybersecurity, and cloud computing—as a major workforce issue. Resistance to organizational change also remains a significant hurdle, noted by 21% of respondents,

emphasizing the critical need for mindful leadership and change management practices.

Regarding cybersecurity concerns, leaders uniformly point to the growing sophistication of threats. Ransomware is the top concern for 23%, closely followed by AI-driven attacks, including deepfakes and social engineering tactics, which together account for nearly 40% of the cited threats. Despite these risks, the actual adoption of AI tools within cybersecurity functions remains limited: 44% of organizations engage AI in less than 10% of their security workload, indicating a gap between threat awareness and technological response capabilities.

Compliance challenges equally underscore the survey findings. Data privacy regulations top the list, posing the most significant difficulty for 29% of respondents. Organizations also

identify evolving cybersecurity guidelines and risks around KYC/AML compliance as substantial compliance management areas needing focus.

Taken together, these findings paint a picture of Indian enterprises at a critical inflection point. The combination of legacy system burdens, talent shortages, and escalating cyber and regulatory risks necessitates strategic investment not only in new technologies but also in workforce upskilling, automation, and integrated governance frameworks. For tech leaders aiming to propel their organizations to true future-readiness, the survey underscores the urgency of transitioning from exploratory digital initiatives to mature, scalable deployments that align technology adoption with operational resilience and compliance imperatives.



CHAPTER 1

DIGITAL STRATEGY & TRANSFORMATION JOURNEY

1.1. Setting the Stage: Digital Imperative for Indian Enterprise

In 2025, Indian organizations stand at a transformative crossroads, as accelerated digitization becomes both a source of advantage and a necessity to remain competitive. Digital strategy now transcends basic technology deployment, demanding integration of vision, process re-engineering, and reimaged value creation models. Driven by sectoral disruptions, regulatory shifts, and an urgent need for resilience, enterprises are setting ambitious goals for operational agility, customer engagement, and future readiness.

Survey feedback highlights that most Indian enterprises are amid multi-phase digital journeys—adopting new tools and frameworks, but often contending with legacy constraints, culture, and skills gaps. This landscape is characterized by varying digital maturity, with a small cohort reaching ecosystem leadership while many remain in automation or analytics pilot stages.

Key Insights

Most Indian enterprises are in early to mid stages of digital transformation, with 41% running analytics/AI pilots and only 14% achieving full

enterprise orchestration, indicating a significant gap between experimentation and full-scale integration.

1. Leadership commitment (64%) and industry collaboration (44%) are the strongest catalysts accelerating digital progress, showing that strategic sponsorship and collective knowledge sharing are key enablers.
2. Legacy system integration (34%) and skills gaps (32%) remain top barriers, highlighting operational constraints and talent shortages that hold back transformation momentum.
3. Enterprises are pursuing resilience, agility, and compliance by design as strategic pillars, embedding regulatory requirements and flexible infrastructure into their digital roadmaps to handle disruption and evolving market needs.

1.2. Strategic Priorities Shaping the Transformation Journey

Surveyed leaders identify three priority pillars driving digital transformation:

- **Resilience and Agility:** Building infrastructure that can withstand disruption,

enable rapid innovation, and scale to shifting market or regulatory needs.

■ **Data-Driven Decision Making:**

Leveraging analytics and AI to inform both strategy and real-time operations for a measurable impact on outcomes.

■ **Compliance by Design:**

Embedding evolving regulatory and privacy requirements into transformation roadmaps from inception.

Organizational Feedback Sample:

- “Our digital roadmap is designed to support business agility and regulatory compliance in equal measure.”
- “AI pilots are being embedded in business-critical processes, but scaling them requires both upskilling and process integration.”

1.3. Key Stages in Digital Transformation Observed

The journey of digital transformation reflected in the survey unfolds across several core stages:

1. Digitization of Core Operations

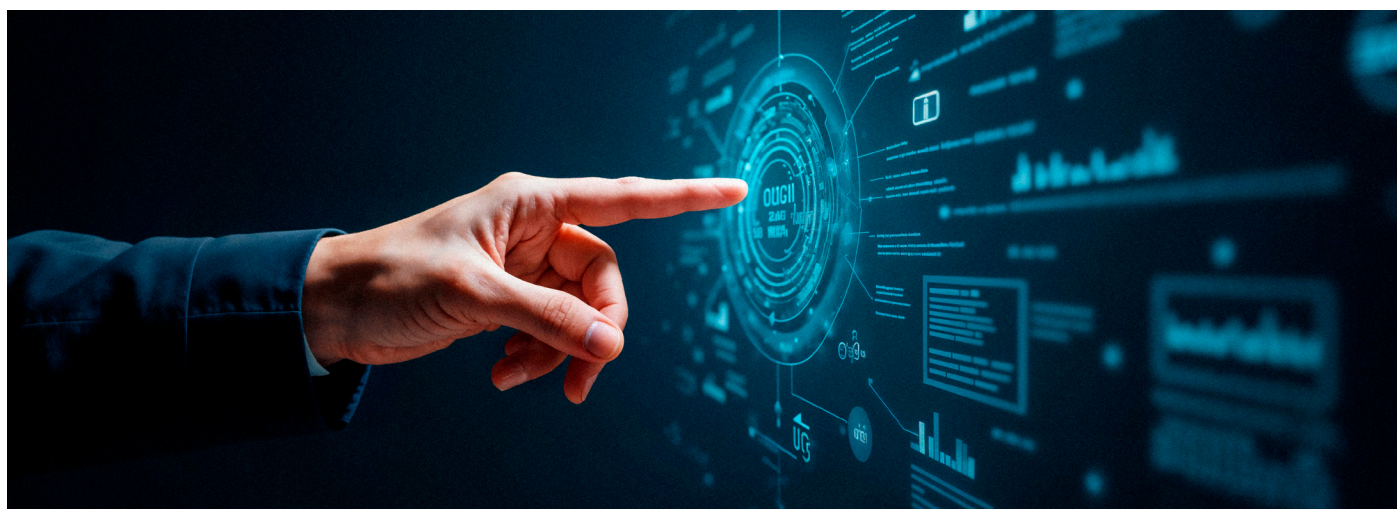
- Migration from paper/manual processes to digital workflows and documentation.
- Initial investments in ERP, CRM, and sector-specific IT systems.

2. Integration & Process Automation

- Connecting business functions via enterprise platforms, APIs, and cloud adoption.
- Introduction of automation tools—RPA and workflow engines—to reduce human error and cycle times.

3. Analytics & AI Enrichment

- Data from integrated platforms is leveraged for



dashboarding, performance monitoring, and predictive analytics.

- Early AI pilots target customer insights, fraud detection, or supply chain optimization.

4. Cross-Enterprise Orchestration

- End-to-end process automation, business intelligence integration, and proactive risk surveillance become the norm in leading organizations.
- AI moves from pilot to operationalized roles in decision support and process execution.

5. Digital Ecosystem Partnerships

- External collaboration

intensifies with fintechs, regtechs, cloud providers, and even competitors for shared platforms or standards.

Open APIs and data exchanges facilitate new product and service models. Indian enterprises progress along a staged digital maturity curve, typically advancing from basic digitization to orchestrated, AI-enabled operations:

Interpretation

A majority (41%) are currently experimenting with analytics and AI pilots, another 28% are automating and integrating processes, and only 14% have achieved full orchestration across the enterprise. Digital leadership and true ecosystem participation remain aspirational for most organizations.

Table 1: Digital Maturity Stage of Indian Enterprises





Main Barriers Identified

- Legacy system integration: Cited as the most stubborn operational roadblock.
- Skills gap (AI/cloud/cybersecurity): Seen as both a technical and organizational barrier.
- Change resistance: Persistent, especially in large or heritage-heavy enterprises.

1.4. Transformation Catalysts and Barriers

Top Catalysts Driving Progress:

- Leadership Commitment: C-suite sponsorship and board-level engagement accelerate investment and prioritize digital initiatives.
- Industry Collaboration & Regulatory Push: Respondents note that active knowledge sharing and regulation often function as accelerants

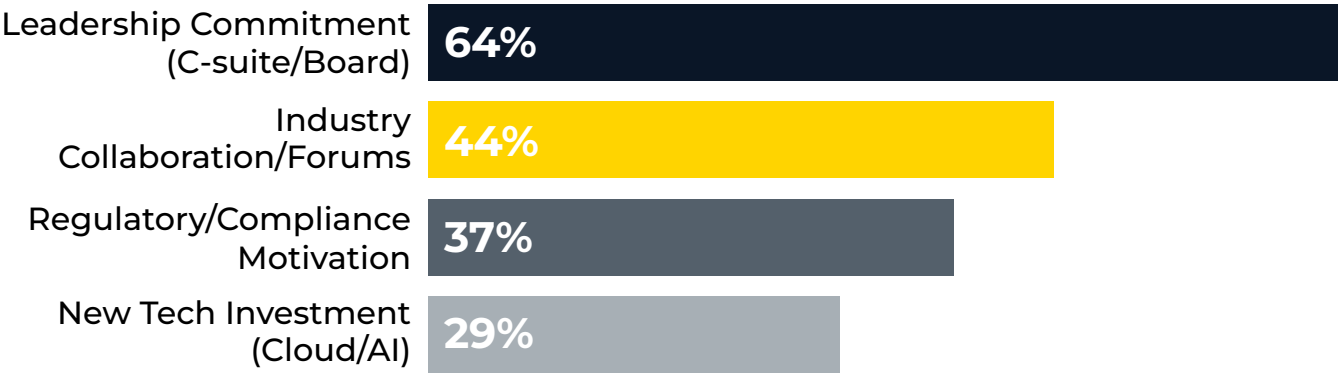
Comparative Insights

Across sectors, the difficulty of moving from pilot to full-scale digital integration parallels international OT security and integrated finance journeys, where maturity is achieved through feedback-driven models and strong executive sponsorship.

Best Practices

- Establish Clear Leadership Governance: Ensure C-suite and board sponsors actively

Table 2: Top Catalysts Reported





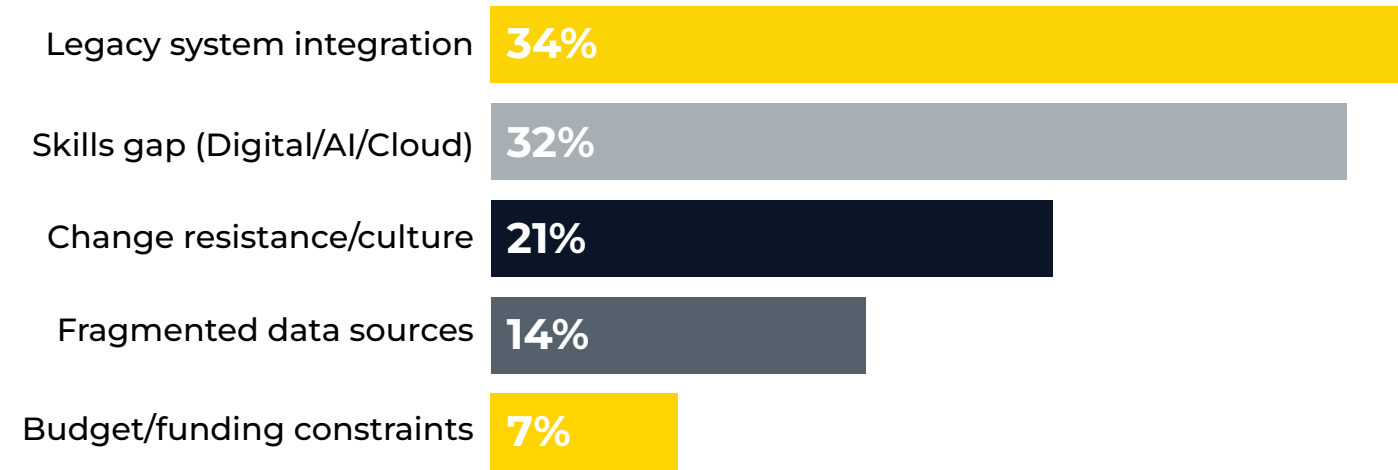
drive digital initiatives with accountability and aligned KPIs.


- Adopt a Phased, Outcome-Focused Approach: Move beyond pilots by setting measurable goals for each transformation stage, gradually scaling successful digital projects.
- Modernize Legacy Systems

Systematically: Prioritize integration and modernization of legacy platforms to reduce operational bottlenecks and boost agility.

- Foster Cross-Industry Collaboration: Leverage partnerships and industry forums to share best practices and co-develop solutions addressing common challenges.

Table 3: Key Barriers to Digital Transformation





CHAPTER 2

AI INTEGRATION & AUTOMATION

2.1. The Pulse of AI Integration in Indian Enterprises

As digital transformation accelerates, Indian enterprises face mounting pressure to integrate artificial intelligence (AI) and intelligent automation into everyday operations. This chapter delves into the readiness, scale, and real-world application of AI across sectors—drawing directly from the India Inc. Digital Playbook 2025 survey data. It examines where organizations are on the AI journey, the barriers and accelerators they encounter, and what these findings mean for enterprise competitiveness and future-readiness.

Key Insights

1. 64% of Indian enterprises are in planning or piloting stages of AI adoption, with only 10% reporting full end-to-end AI integration, underscoring a large implementation gap despite widespread interest.

2. The primary AI use cases are currently experimental or localized pilots rather than broad, scaled deployments, limiting the realization of AI’s full productivity and customer experience benefits.

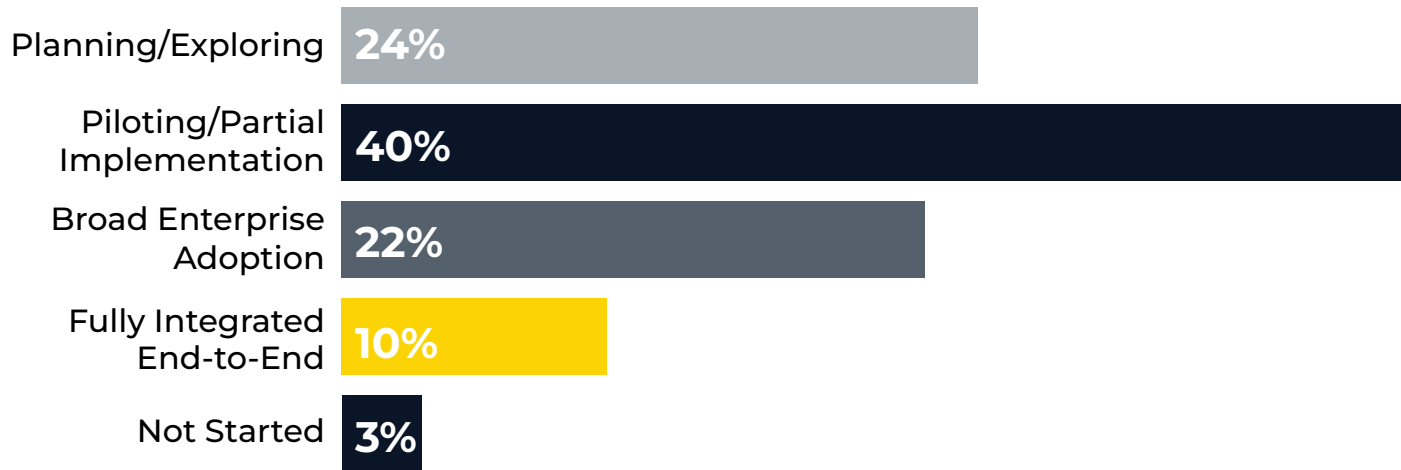
3. Organizations that fail to move beyond pilot stages risk losing competitive advantage, as AI-driven automation increasingly becomes foundational to digital maturity and operational efficiency.

4. Integration challenges include not only technical barriers but also the need for cultural adaptation and upskilling, making workforce readiness critical for AI success.

2.2. Maturity of AI Adoption

Surveyed technology leaders reported their organization’s stage in adopting AI-driven operations—an essential marker

Table 2.1: AI Adoption Stages



of digital and competitive maturity.

Interpretation

- 64% of organizations are either planning or piloting AI; this means most firms are not yet scaling AI across the enterprise.
- Just 10% have achieved full, end-to-end integration, highlighting the gap between ambition and reality even at the mid-2020s technology inflection point.
- Implication for Enterprises: Widespread value from AI remains unrealized for most. Early-stage experimentation is vital, but the real differentiation will come as organizations succeed in moving beyond pilots to consistent, pervasive AI-driven operations. Enterprises lagging in integration risk falling behind on productivity, speed, and customer experience.

2.3. AI in Cybersecurity Workloads

AI’s potential to automate threat detection, rapid response, and compliance is frequently cited. But is it truly impacting daily cybersecurity workloads?

Interpretation

- Nearly half (44%) of

Table 2.2: Percentage of Cybersecurity Workload Managed by AI

% of Cybersecurity Workload Using AI	% of Organizations
0–10%	44
11–24%	20
26–40%	18
41–74%	7
>74%	2
Outsourced	2
Not Applicable/ No Response	6

organizations report that AI is used in less than 10% of their current cybersecurity workload.

- Only 9% say they use AI in more than half of their security operations.
- Implication for Enterprises: Despite industry rhetoric, AI’s actual role in cyber defense is mostly at the margin rather than the core. For enterprises, this reveals a substantial capability gap: unless AI is more widely embedded in security operations, organizations may remain reactive and exposed to advanced threats that traditional controls cannot counter.

2.4. Barriers to Scaling AI & Automation

Respondents identified the main factors impeding wider enterprise AI and automation adoption.

Interpretation

- Legacy integration (38%) dominates as the top barrier, reaffirming that many organizations struggle to connect new AI tools with older, mission-critical systems.
- Talent shortages (31%) in AI and data science are nearly as concerning, as digital strategies falter without the right skills on staff.
- Change resistance (19%)—from both culture and process inertia—remains a non-technical but serious constraint.

Implication for Enterprises

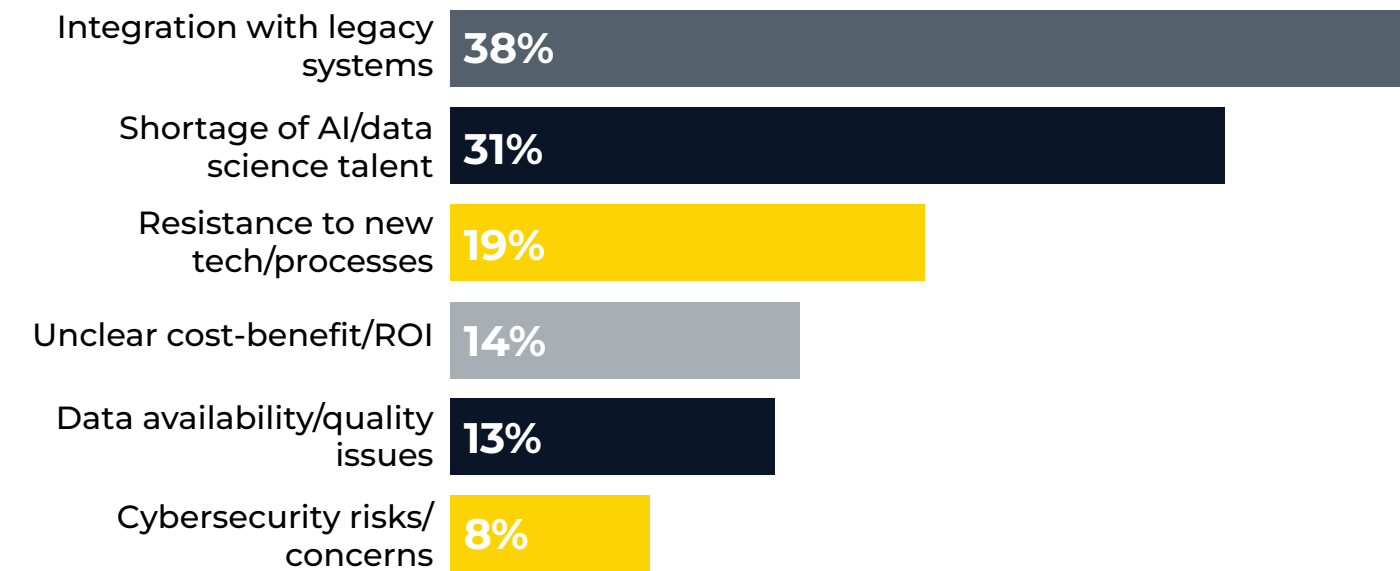
Without overcoming these hurdles, organizations will be unable to capture the productivity, risk mitigation, and innovation benefits of true AI-powered operations. This requires concerted investment in both upskilling and re-platforming—along with clear communication of AI benefits to the broader workforce.

2.4. High-impact AI Application Areas

Survey feedback and qualitative responses reveal four areas where AI and automation are already making, or poised to make, substantial impact:

- **Operational Automation:** Streamlining routine tasks in finance, HR, supply chain,

Table 2.3: Top Barriers to AI & Automation



and customer service, freeing up talent for higher-value activities.

■ **Security Operations:**

Accelerating threat intelligence, detection, and incident response, especially for emerging risks (such as AI-generated attacks and fraud).

■ **Data Analytics:** Enhancing business intelligence through predictive insights and near real-time data-driven decision making.

■ **Customer Experience:**

Personalization through AI-driven recommendations, chatbots, and proactive service delivery.

transaction fraud monitoring using AI.

Manufacturing: Predictive maintenance powered by machine learning on industrial sensor data.

IT/ITES: Conversational bots resolving service desk tickets efficiently.

2.6. Sectoral Patterns & Readiness Gaps

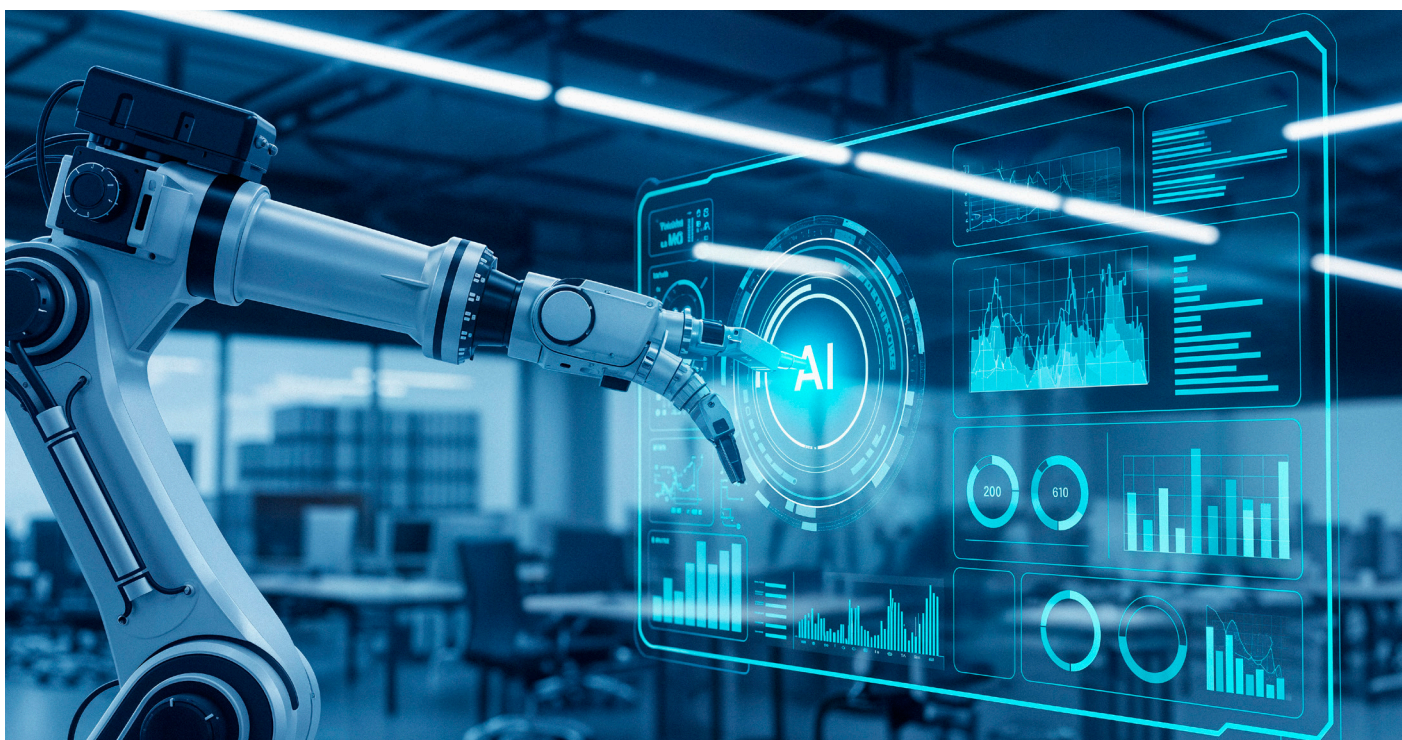
Sectoral analysis highlights several patterns:

■ Industrials and manufacturing are more likely to have AI pilots in predictive maintenance and digital twins, but legacy integration barriers are especially acute here.

Enterprise Use Case Examples

BFSI: Automated KYC and

■ BFSI leads in AI for fraud



detection but faces tight compliance and complex legacy systems.

- IT/ITES and media report higher skills readiness yet often use AI for customer-facing tasks rather than core operations.

What Enterprises Can Do:

- Invest in targeted workforce upskilling, especially in AI/ML and data science.
- Conduct “legacy readiness” assessments to prioritize platform modernization routes for AI integration.
- Foster a clear change management strategy to address cultural resistance and communicate the tangible benefits of AI automation.

2.7. The Road Ahead: From Pilots to Impact

The data underscores a decisive enterprise imperative: bridge the gap between curiosity/pilots and organization-wide scale. This will demand:

- **Cross-functional leadership:** Empowering not just IT but business users and risk owners to drive automation strategy.
- **Strategic digital investment:** Prioritizing initiatives with clear ROI and measurable value.

- **Continuous improvement:** Adopting feedback-driven approaches, where change is iterative and informed by real-world results.

Key Takeaway

AI-driven automation is rapidly rising on the enterprise agenda—but its transformational benefits will remain locked without scaled adoption, skill-building, and deep integration with existing systems and cultures.

Best Practices

- **Start with High-Impact, Scalable Use Cases:** Identify AI projects with clear ROI potential and scalability rather than isolated pilots.
- **Build a Robust Data Foundation:** Invest in clean, integrated data platforms to enable reliable AI model training and deployment.
- **Promote Change Management and Culture Alignment:** Engage stakeholders early, communicate AI benefits, and provide training to overcome resistance.
- **Implement Governance for AI Ethics and Risk:** Define frameworks to ensure transparency, fairness, and compliance in AI adoption.

CHAPTER 3

CYBERSECURITY THREAT LANDSCAPE



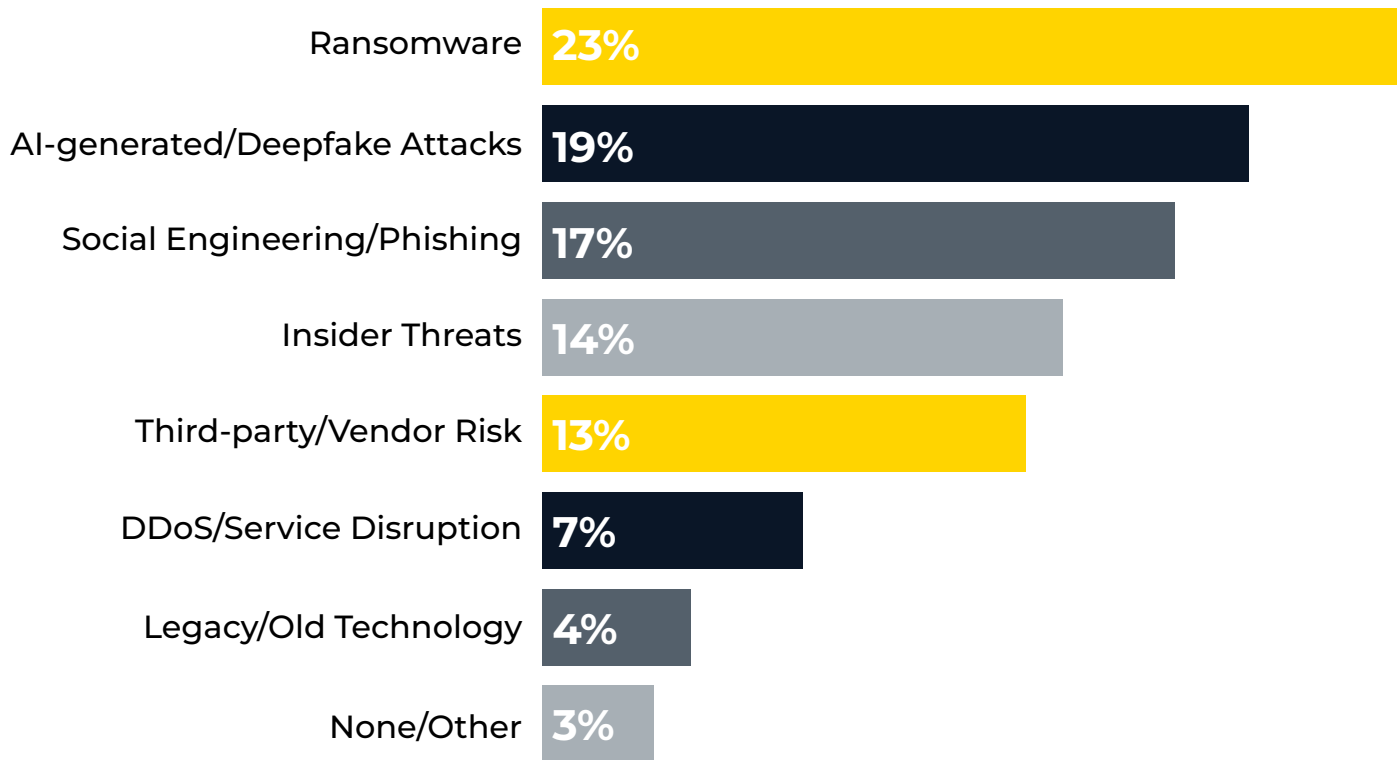
3.1. Overview: The Escalating Threat Environment

As Indian enterprises continue rapid digitization and AI adoption, the complexity and frequency of cyber threats have grown. From ransomware to deepfakes, attackers have become more sophisticated, using automated tools and targeting expanded digital surfaces. Technology leaders now place cybersecurity at the center of operational resilience, viewing cyber risk as both a business and governance priority.

Key Insights

1. 44% of organizations use AI in less than 10% of their cybersecurity
- workloads, meaning the majority of cybersecurity is still managed manually or with traditional tools despite AI's potential.
2. Only 9% use AI in more than half of their security operations, reflecting slow adoption of AI-enabled threat detection and response capabilities.
3. The evolving nature of cyber threats and regulatory pressures is elevating cybersecurity as a board-level concern, pushing enterprises to rethink defenses and governance.
4. Cybersecurity transformation requires both technology

Table 3.1: Most Prevalent Cybersecurity Threats



upgrades and organizational awareness, with increasing emphasis on integrating AI tools to enhance agility and response times.

3.2. Current Threat Types and Prevalence

The India Inc. Digital Playbook 2025 survey asked respondents to identify their top cyber threats. Multiple selections were permitted, reflecting the complex risk landscape.

What the Data Reveals:

- Ransomware and AI-generated attacks dominate concern, showing that both established and evolving threat vectors are major risks.
- Social engineering persists, highlighting that attackers are still exploiting human factors.

- Insider threats and third-party/vendor risks reveal that many incidents originate from trusted users or supply chain partners, not just external actors.

- Older technology and legacy systems still present a security gap.

3.3. Trends in Attack Tactics and Exposure

- **AI-Powered Attacks:** The fast rise in deepfakes and adaptive malware shows adversaries are already harnessing AI to bypass traditional defenses—making automation essential for detection.
- **Supply Chain & Vendor Attacks:** More firms now rely on ecosystem partners for digital services, increasing



exposure to attacks beyond direct corporate control.

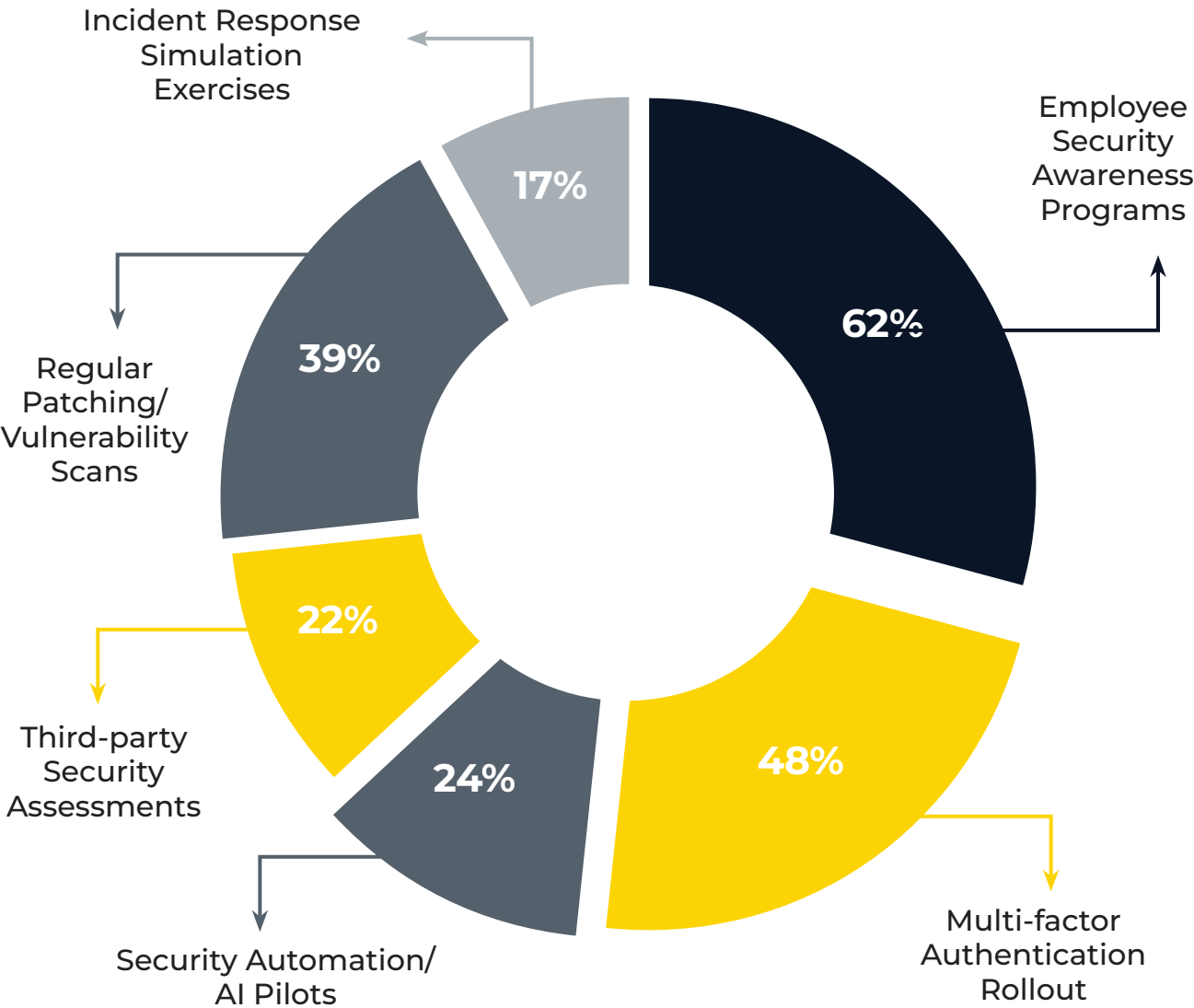
- **Insider Risks:** As employees connect via remote or hybrid work, accidental or deliberate insider incidents are climbing, especially in heavily regulated sectors.

3.4. Sectoral Differences in Threat Exposure

Different industries face unique threat mixes:

- **BFSI & IT/ITES:** Report increased targeting by ransomware and deepfake attacks, likely due to the high volume of sensitive data they control and their role as critical infrastructure.
- **Manufacturing/Industrials:** More affected by legacy tech exposures and disruptions to operational technology systems, underpinning the

Table 3.2: Defensive Measures Adopted



need for dedicated OT security protocols.

- **Healthcare & Pharma:** High concern around service disruption and the vulnerability of critical infrastructure.

3.4. Frequency and Impact of Major Incidents

Survey comments indicated:

- A significant number of respondents experienced at least one cyber incident in the past year, with ransomware and social engineering as leading causes.
- Operational downtime (especially due to ransomware) was the most damaging impact, followed by financial losses and reputational damage.
- High-maturity organizations reported both lower frequency and reduced impact of incidents, suggesting that investment in layered defenses and automation is paying off.

3.6. Defensive Posture and Response Readiness

Organizations are taking varied approaches to counter modern threats:

- **Investing in Security Automation:** A growing minority are piloting or

scaling security orchestration, automation, and response (SOAR) tools to accelerate detection and incident response.

- **Strengthening Third-party Controls:** Due diligence programs for vendor selection and continuous supply chain monitoring are on the rise.

- **Training & Awareness:** Regular employee training on phishing and insider threats has increased, though coverage and effectiveness remain uneven.

3.7. Recommendations and Lessons for Enterprises

- **Enhance Layered Defenses:** Combine traditional security controls with AI-powered detection and automation for faster, more accurate response.
- **Prioritize OT and Third-party Security:** Map and secure all operational technology endpoints and perform ongoing assessments of vendor cyber posture.
- **Focus on Human Factors:** Institute continuous training and clear, actionable insider threat policies.
- **Modernize Legacy Infrastructure:** Incrementally replace, segment, or virtually



patch outdated systems that cannot be quickly retired.

and response to improve speed and accuracy.

3.8. Outlook

The evolving threat landscape requires Indian enterprises to invest strategically—not only in technology, but also in process, culture, and governance. Leveraging data from peers, benchmarking security maturity, and collaborating across sectors and with public authorities will be crucial for defending against increasingly sophisticated actors.

Best Practices

- **Integrate AI-Enabled Security Tools Thoughtfully:** Gradually enhance manual operations with AI-based threat detection

- **Elevate Cybersecurity Accountability to Board Level:** Incorporate cyber risk metrics into board reporting and strategy discussions.
- **Adopt a Proactive, Layered Defense Strategy:** Combine technology upgrades with employee training and continuous vulnerability assessments.
- **Align Security with Business Continuity Planning:** Embed cybersecurity into overall resilience and crisis response frameworks.



CHAPTER 4

WORKFORCE EVOLUTION & DIGITAL SKILLS

4.1. The Human Factor in Digital Transformation

Workforce skills and adaptability now stand as critical differentiators for Indian enterprises navigating AI-led and cloud-based transformation. Success is no longer assured by technology investment alone; building future-ready teams with digital, analytical, and cybersecurity competencies is equally vital. The India Inc. Digital Playbook 2025 survey finds that while digital adoption surges, a prominent skills gap, change resistance, and obstacles to upskilling are limiting the pace and impact of transformation.

Key Insights

- 1. Skill gaps in AI, cloud, and cybersecurity remain a major barrier (32%) to digital transformation, emphasizing the persistent challenge of sourcing and retaining tech talent.
- 2. Workforce upskilling and adoption of a digital-first culture are prioritized by enterprises to foster resilience and sustain transformation momentum.
- 3. Digital leadership recognizes that continuous learning and change management are essential, as digital strategies fail without sufficient employee readiness and engagement.
- 4. Talent gaps affect not just

technical functions but also the broader organizational ability to operationalize AI and automation at scale.

4.2. Current Adoption of AI Tools by the Workforce

Organizations were asked about the proportion of their IT and security workforce regularly using AI-powered tools in their daily roles.

Interpretation

- The largest share of organizations (42%) reported very limited (<10%) workforce engagement with AI tools.
- Just 10% indicated that more than half their workforce is actively leveraging AI—showing that broad-based AI skills and tool adoption are still rare.

Table 4.1: AI-Powered Tools Usage (IT/Security Workforce)

% of Workforce Using AI Tools	% of Organizations
0–10%	42
11–24%	14
26–40%	23
41–74%	7
>74%	2
Outsourced	3

- Outsourcing remains marginal (2%), and most organizations are still early in the journey toward truly AI-enabled teams.

Enterprise Impact

Low adoption rates signal an urgent need for investments in workforce upskilling and integration of AI literacy into everyday business processes. Firms with higher AI tool uptake are more likely to realize process efficiencies, enhanced security, and competitive agility.

4.3. Top Workforce Barriers & Organizational Pain Points

Respondents identified several persistent obstacles to building digitally capable teams:

Interpretation

- Nearly one in three organizations cite a

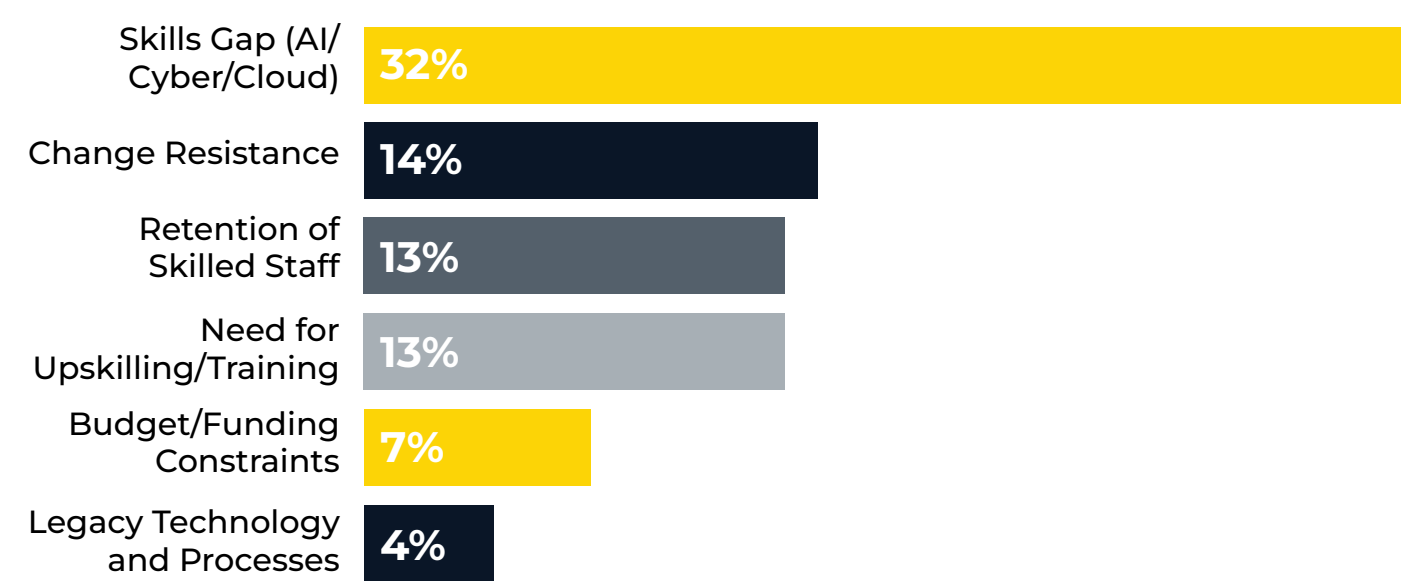
digital skills gap as their top workforce challenge, underscoring a national need for targeted talent development in AI, cybersecurity, and cloud.

- Resistance to new tools, processes, and workflows is a significant barrier, highlighting change management as an underappreciated success factor.
- Talent retention and upskilling pressures are mounting, particularly as leading professionals are increasingly in demand.

Enterprise Takeaway

Organizations that bridge these skills gaps through structured training, leadership engagement, and incentives stand to accelerate

Table 4.2: Major Workforce Challenges





their digital progress, reduce risk exposure, and foster greater innovation.

4.4. Upskilling Strategies in Practice

Qualitative survey responses and organizational narratives indicate several approaches in use:

- **Continuous Learning Programs:** Firms are rolling out in-house academies or partnering with edtechs to deliver AI, data analytics, and cybersecurity courses.
- **Peer Learning and Mentoring:** Some respondents have introduced mentorship programs to accelerate skill diffusion.
- **Certification Incentives:** Providing benefits or bonuses for employees who attain industry-recognized

certifications is becoming more common.

4.4. Sectoral Variations in Digital Skills Readiness

- IT/ITES and BFSI sectors show the highest engagement with upskilling, reflecting both advanced digital ambitions and strict compliance/regulatory mandates.
- Manufacturing and Healthcare report more acute legacy system constraints and slower change adoption, intensifying their skills challenges.

4.6. Recommendations for Enterprises

- **Prioritize Role-specific Upskilling:** Map emerging requirements in AI, cybersecurity, and cloud to tailored training programs for staff at all levels.

■ **Embed Change Management:**

Invest in leadership communication, coaching, and clear incentives to reduce resistance and foster a growth mindset.

■ **Incentivize Continuous**

Learning: Reward employees for self-motivated upskilling and for cross-functional knowledge-sharing.

■ **Retain and Attract Top Talent:**

Develop career pathways and flexible work models that retain skilled professionals and attract new expertise from the market.

Programs: Implement upskilling and reskilling initiatives focused on AI, cloud, and security competencies.

■ **Create a Digital-First Culture:**

Cultivate agile mindsets, reward innovation, and support cross-functional collaboration.

■ **Leverage Internal Talent and External Partnerships:**

Tap into in-house subject matter experts and collaborate with educational institutions or tech providers for skill development.

■ **Monitor Skill Gaps Regularly:**

Use assessments and feedback loops to dynamically adapt training and hiring strategies.

Best Practices

■ **Develop Continuous Learning**



CHAPTER 5

REGULATORY COMPLIANCE & GOVERNANCE



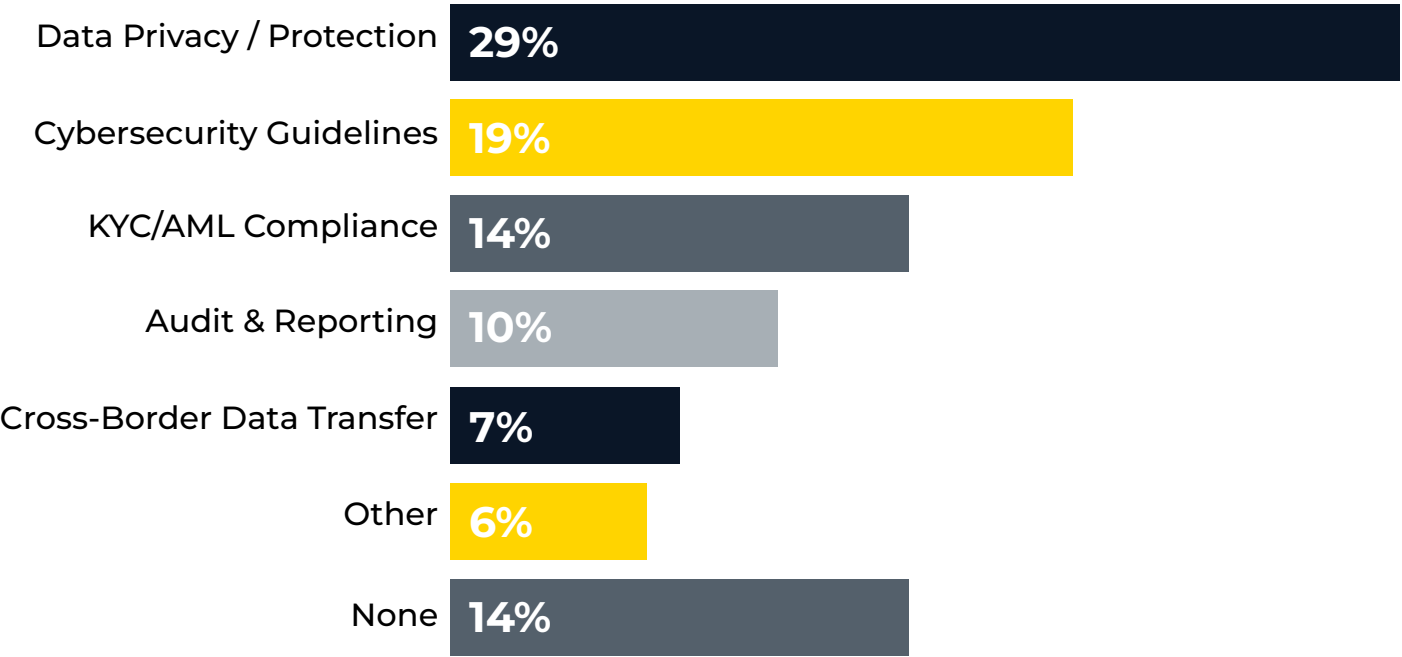
5.1. Introduction: Navigating India’s Evolving Regulatory Landscape

The India Inc. Digital Playbook 2025 survey reveals that regulatory compliance and governance are increasingly central concerns for Indian enterprises accelerating their digital and AI transformation. Compliance challenges extend beyond simple checkbox governance; they impact operational agility, technology choices, and risk management strategies. Organizations face a complex regulatory environment spanning data privacy, cybersecurity, anti-money laundering (AML), audit, and cross-border data transfer regulations.

Key Insights

- 1. Indian enterprises are facing increasing regulatory scrutiny, making compliance a key part of digital transformation strategies rather than an afterthought.
- 2. 37% of respondents cite regulatory and compliance motivation as a transformation catalyst, showing that evolving legal frameworks are pushing enterprises toward better governance and privacy-by-design practices.
- 3. Embedding compliance early (“compliance by design”) helps future-proof investments and avoid late-stage, costly remediation efforts.

Table 5.1: Compliance Challenge Areas



4. Organizations need integrated risk management and governance models to navigate complex regulations while advancing technology adoption and innovation.

5.2. Primary Compliance Challenges

Survey respondents were asked to identify which compliance areas present the greatest challenge for their teams.

Insights

- Data privacy leads as the most pressing challenge, reflecting the evolving Indian data protection framework and global regulations.
- Cybersecurity standards requiring operational compliance is also a significant complexity.

- Financial services and BFSI sectors emphasize KYC/AML obligations.
- A small but notable fraction report no significant compliance challenges, indicating diversity in maturity and sectoral impact.

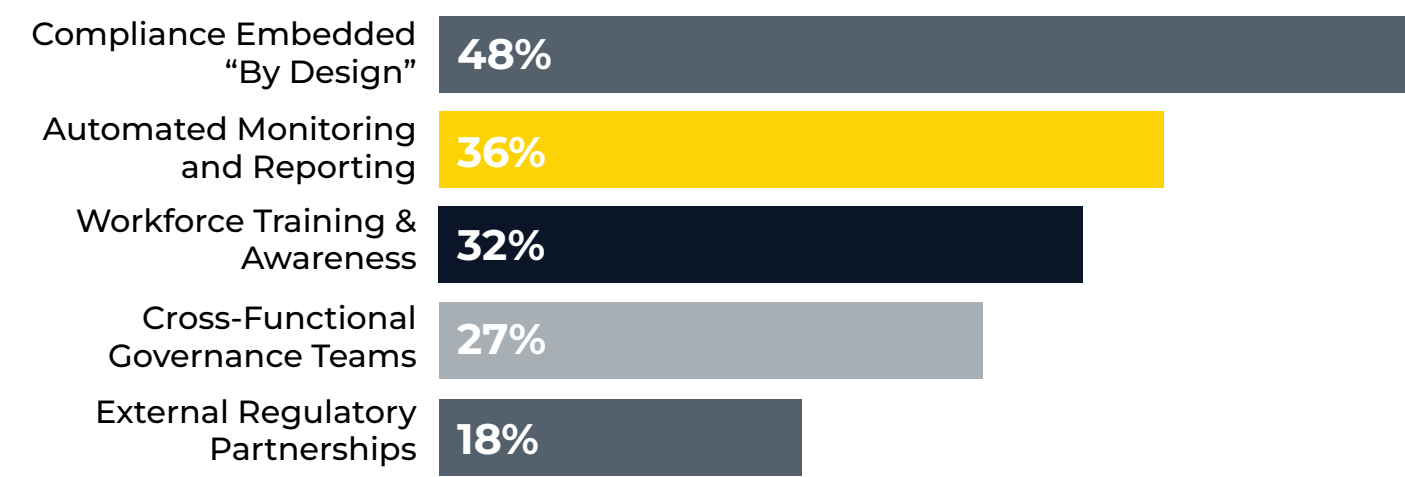
5.3. Impact of Regulatory Complexity on Operations

Respondents noted effects on business including compliance costs, delays in digital projects, and increased audit overhead. Fragmented and frequently changing regulations result in duplicated controls and increased demand for reporting accuracy.

5.4. Compliance Readiness and Governance Practices

Organizations are adopting multiple strategies to institutionalize compliance:

Table 5.2: Compliance Readiness Measures



Interpretation

- Nearly half integrate compliance considerations early in digital initiatives to avoid costly retrofits.
- Automated compliance tools are increasingly used to provide continuous assurance.
- Training and governance teams pool legal, IT, and business expertise to improve oversight and responsiveness.

5.5. Governance Structures and Accountability

Survey feedback suggests that compliance is migrating from isolated functions towards more cross-functional governance, involving senior executives and boards. This trend aligns with global best practices where regulatory risk is managed as an enterprise-wide strategic imperative.

5.6. Sectoral Perspectives

- BFSI and financial sectors report significant focus on stringent KYC/AML and audit demands.
- IT/ITES organizations highlight complexities around cross-border data transfers and privacy.
- Manufacturing and healthcare sectors observe challenges

embedded in legacy system compliance and data security.

5.7. Policy Support and Industry Collaboration Demands

Respondents expressed the need for:

- Clearer, harmonized regulatory frameworks to reduce uncertainty (24%).
- More industry forums for knowledge sharing and best practices (16%).
- Policy initiatives to promote upskilling and standardized AI governance frameworks.

5.8. Recommendations for Enterprises

- **Compliance-by-Design:** Embed compliance controls at project inception for digital and AI initiatives.
- **Leverage Technology:** Adopt RegTech solutions for automated monitoring, reporting, and risk detection.
- **Build Cross-Disciplinary Teams:** Align IT, legal, compliance, and business units to share accountability.
- **Continuous Training:** Keep workforce updated on evolving regulations and compliance tools.



- **Engage With Regulators:** Proactively participate in consultations to influence balanced, growth-oriented policy.

5.9. Conclusion

Regulatory compliance and governance are no longer back-office functions; they are strategic pillars critical for digital trust, operational resilience, and sustainable growth. Indian enterprises that effectively manage regulatory complexity and embed governance into their digital DNA will gain competitive advantage in the rapidly transforming economy.

Best Practices

- **Embed “Compliance by Design”:** Integrate legal and regulatory requirements early

in technology development and deployment processes.

- **Keep Abreast of Regulatory Changes:** Maintain dedicated teams or partnerships to monitor evolving laws and standards impacting data, privacy, and cybersecurity.
- **Implement Integrated Risk Management:** Use centralized platforms to track and mitigate risks across compliance, technology, and operational domains.
- **Foster Transparent Communication with Regulators:** Build proactive relationships to anticipate requirements and demonstrate governance maturity.

KEY CONTRIBUTORS

Nisha Sharma is a Senior Tech Correspondent at **Tech Disruptor Media**, where she reports on the intersection of innovation, digital transformation, and leadership across India Inc. With a deep understanding of enterprise IT and a flair for storytelling, Nisha has covered key developments in cybersecurity, cloud infrastructure, AI, and the future of work. She leads the editorial line on tech leadership and digital strategy, driving content that includes exclusive interviews, industry reports, and panel moderation. Nisha is known for her ability to distill complex tech themes into accessible insights that empower senior decision-makers and technology stakeholders.

Praneeta is a Senior Correspondent at **Tech Disruptor Media**, bringing a sharp editorial focus to the evolving enterprise technology landscape. With a strong print and digital journalism foundation, she covers transformative trends across AI, cloud, IoT, cybersecurity, and data analytics, offering in-depth perspectives that resonate with industry leaders. She leads the editorial line on enterprise transformation and emerging technologies, shaping high-impact narratives through interviews, roundtables, and research-driven features. Actively engaged with professional tech communities, Praneeta drives content-rich initiatives that connect innovation with strategic insight.



Nisha Sharma

Senior Tech Correspondent- Tech Disruptor Media
Bharat Network Group



Praneeta

Senior Correspondent- Tech Disruptor Media
Bharat Network Group

An Initiative of
BNG BHARAT™
NETWORK
GROUP

Concept by
**Tech
Disruptor**
media.com

Suite No. G08, C-127, Sector 63,
Noida, 201301

