



On the cyber agenda 2026

Board Leadership Center (India)

April 2026

kpmg.com/in

KPMG. Make the Difference.



Introduction

India’s growing digital and data footprint has elevated cyber risk to a material board-level concern. Cyber incidents are rising in frequency and impact, increasingly affecting service continuity, data integrity, regulatory compliance, and stakeholder confidence. For many organisations, cyber events now surface not as isolated technical failures, but as business disruptions with reputational and financial consequences.

At the same time, regulatory expectations are sharpening. The Digital Personal Data Protection Act, sectoral supervisory guidance, and heightened scrutiny of third-party and cloud dependencies along with AI adoption is redefining how organisations are expected to govern data, technology, and cyber resilience. Cyber oversight is no longer limited to controls and response plans; it extends to accountability, decision-making discipline, enhancing Trust and institutional readiness.

In this environment, boards are required to exercise informed judgement on cyber resilience, AI-enabled systems, data protection obligations, and the organisation’s ability to operate through sustained digital stress. **Cyber risk now sits at the intersection of strategy, operations, compliance, and trust.**

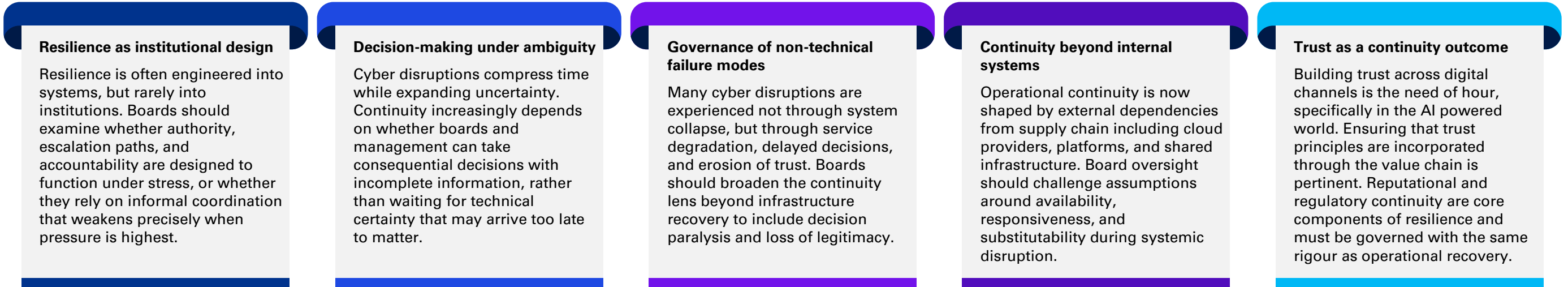
Based on our discussion with marquee directors and gathered intelligence we have prepare the ‘Cyber Agenda 2026’ which outlines key themes to support board level discussion on cyber security, technology risk, AI deployment, and digital trust for directors.



Enterprise resilience and continuity under digital stress

Cyber incidents are reshaping how continuity is experienced and judged. In digitally integrated enterprises, continuity is no longer defined by recovery timelines alone, but by the organisation’s ability to sustain operational, regulatory, and reputational legitimacy under prolonged digital stress. Increasingly, cyber events expose not the absence of plans, but the presence of ungoverned assumptions embedded in enterprise design.

For boards, this represents a material shift. Continuity is no longer a downstream operational matter; it is a governance attribute shaped by architecture, decision rights, escalation pathways, and institutional design. When disruption occurs, the central question is whether continuity has been explicitly governed or merely assumed to exist.



Considerations for the board

- Has resilience been assumed rather than explicitly governed?
- What role would the board need to take in a major cyber event?
- How would governance function in the event of lack of reliable information for an extended period?
- Are there inherent assumptions to have continuity that are beyond organisation’s control?
- Is resilience defined appropriately when trust – not systems – is at risk?

Institutional capacity and digital dependence

As digital systems become foundational to revenue, compliance, and customer access, boards are confronting a growing asymmetry: **digital dependence is scaling faster than institutional capacity**. Governance models designed for slower, linear organisations are increasingly misaligned with the speed and interdependence of digital operations.

Cyber incidents surface this imbalance with clarity. They test whether an organisation can see itself under stress, understand dependencies, coordinate across silos, and exercise judgement as cascading failures outpace traditional reporting mechanisms.

Enterprise visibility of mission-critical digital assets
Boards often receive fragmented views of technology, cyber and AI risk. The need is to have enterprise-level visibility into systems, integrations, and data flows that are existential to outcomes and therefore demand robust governance.

Institutional readiness versus management assurance
Management confidence cannot substitute for governance. Boards should probe whether readiness has been demonstrated through tested decision authority, cross-functional coordination, and clarity of ownership—not inferred from historical stability.

Coordination risk in complex operating models
Digital architectures cut across business units, vendors, and geographies, while authority remains siloed. During cyber stress, this misalignment can slow response and diffuse accountability.

Decision latency introduced by complexity
As interdependencies grow, the time required to understand impact increases—often exceeding the time available to act. Complexity itself becomes a risk factor when it delays judgement.

Irreversibility of digital dependence
Digital systems are no longer optional or easily unwound. Dependence is therefore a governance constraint rather than a strategic choice, requiring conscious board ownership.



Considerations for the board

- Has digital dependence become mission-critical? If yes, then does the board have adequate visibility?
- Are there effective ways to distinguish institutional capacity from management confidence?
- What coordination failures would most impair response during disruption?
- Where might complexity slow decisions beyond acceptable thresholds?
- Is digital dependence understood well and are there appropriate governance measures?

Regulatory exposure in a digitally accountable environment

Cyber regulation in India is shifting from prescriptive controls towards accountability and stringent cyber incident reporting timelines. Following incidents, regulators increasingly assess whether boards exercised foresight, diligence, and judgement—not merely whether policies existed. Compliance is no longer evaluated prospectively; it is overlaid during an event.

This reframes regulatory risk for boards. Exposure now arises not only from technical failure, but from how decisions were made, escalated, and documented under pressure.

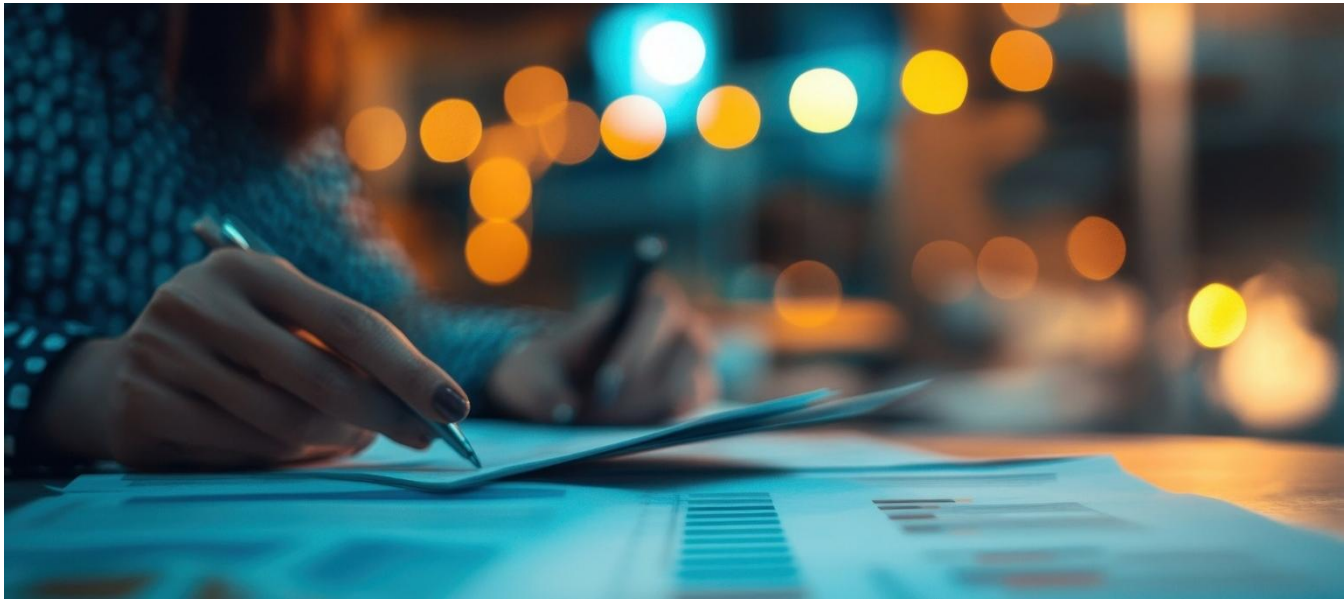
Compression of regulatory timelines
Incident reporting obligations have narrowed the window between detection and scrutiny. Boards must be prepared to exercise judgement early, often before full technical clarity emerges.

From guidance to mandate
Regulatory frameworks increasingly assign explicit responsibility for cyber resilience outcomes to boards, materially raising the stakes of board engagement.

Documentation as evidence of governance
Regulators often infer board intent from records. Absence of documented deliberation can itself be interpreted as a governance failure.

Multi-regulator exposure from a single incident
A single cyber event may trigger scrutiny from data protection authorities, sectoral regulators, law enforcement, and national authorities simultaneously amplifying consequence.

Silence as a source of risk
Delayed escalation or lack of visible board engagement can weaken regulatory confidence.



Considerations for the board

- How would decisions on cyber read when examined retrospectively?
- Are there details available on board judgement for cyber risk?
- How prepared is the organisation for early regulatory engagement?
- Does the board perceived lack of involvement be misinterpreted as indifference?
- Who holds authority for statutory disclosures under time pressure?

Digital ecosystem and third-party risk

As organisations integrate deeper into digital ecosystems, cyber exposure extends well beyond enterprise-controlled systems. Responsibility becomes shared, accountability diffused, and failure in one node can propagate rapidly across the network.

Supply chain and ecosystem risk is not merely an extension of vendor risk; it represents a distinct governance challenge that cannot be managed through contracts alone.

Operational dependence masked by contractual comfort

Legal protections offer limited mitigation during real-time disruption. Boards should focus on operational substitutability rather than contractual remedies.

Concentration risk across digital partners

Dependencies are often fragmented across business units, obscuring systemic exposure to a small number of platforms or providers.

Inherited assurance

Third-party certifications often replace deeper scrutiny of resilience, escalation capability, and recovery realism.

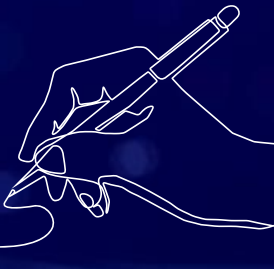
Accountability ambiguity during incidents

When failures originate externally, attribution debates can delay decisive action precisely when speed matters most.



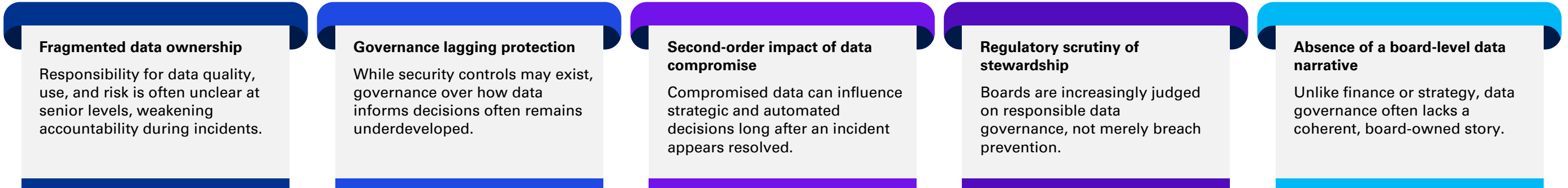
Considerations for the board

- Which all external dependencies pose existential risk to continuity?
- How much resilience is dependent on supply chain?
- Where does accountability sit when business partners aren't successful?
- How visible is ecosystem concentration risk?
- What risks are consciously accepted due to lack of substitutability?



Data governance beyond protection

Boards are comfortable discussing data protection, but fewer have engaged with data governance as a framework of accountability. Cyber incidents increasingly expose weaknesses in data lineage, ownership, and authority often without triggering traditional security alerts. Data failures rarely remain technical; they distort decisions, erode trust, and attract regulatory scrutiny.



Considerations for the board

- How clearly is accountability for data established?
- Where might data weaknesses distort outcomes unnoticed?
- How visible is data governance to the board?
- Is there clear narrative on data governance?

AI, automation, and decision autonomy

As AI systems automate decisions at scale, judgement increasingly migrates from people to code. Cyber risk in this context extends beyond system compromise to accountability for autonomous outcomes. Boards face a governance gap where consequences remain human-owned, but decision authority is embedded in systems.

Decision authority encoded in systems

Automated systems exercise discretion without explicit governance recognition or oversight frameworks.

Explainability trailing deployment

AI adoption often outpaces resolution of trust, accountability, transparency, and auditability questions.

Attribution challenges during failure

When automated decisions go wrong, responsibility becomes difficult to trace and assign.

Cyber amplification of AI risk

Compromise of autonomous systems can propagate errors rapidly and invisibly.

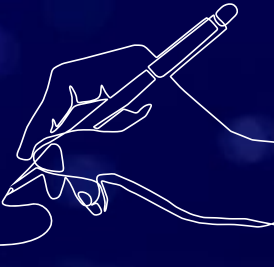
Human-centric governance assumptions

Oversight models often assume human decision-makers even where systems act independently.



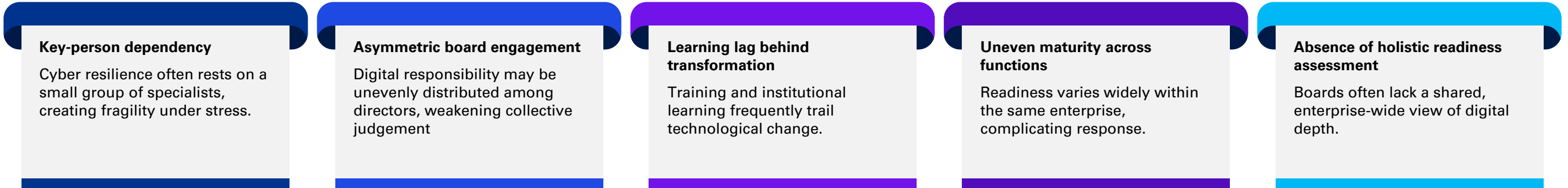
Considerations for the board

- Which decisions are effectively delegated to machines?
- How is accountability defined for autonomous outcomes?
- What constitutes meaningful oversight of AI?
- How would cyber compromise alter automated decisions?
- Are we governing intent, outcomes, or mechanisms?



Leadership depth and organisational readiness

Digital investment does not equate to readiness. Cyber incidents reveal whether capability is institutionalised or concentrated in individuals. Leadership depth, continuity, and organisational stamina increasingly shape resilience outcomes.



Considerations for the board

- How distributed is digital competence across leadership?
- Where do we rely excessively on individuals?
- How do we assess readiness beyond investment spend?
- Are we prepared for digital and leadership stress together?
- What signals would indicate erosion of readiness?

KPMG in India contacts:

Ritesh Tiwari

Partner
Board Leadership Center
E: riteshtiwari@kpmg.com

Atul Gupta

Partner and Head - Digital Trust and Cyber
KPMG in India
E: atulgupta@kpmg.com

Nitin Shah

Partner Digital Trust
Head, Cyber and Privacy
Strategy & Governance
E: nitinshah@kpmg.com

Shikha Kamboj

Partner, Digital Trust
National Leader, Data Privacy and Ethics
E: skamboj@kpmg.com

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.