Deloitte. | Google Cloud

CYBER FOR BOARD

A GOVERNANCE LENS ON EMERGING TECH RISKS

May 2026

Table of contents

Foreword 04

Introduction 06

The board's imperative:
Circumventing the future of cyber risk 08

Current cybersecurity challenges and board preparedness 10

Board oversight: Current state and gaps 12

Emerging technology risks and blurring boundaries 14

Regulatory changes and board accountability 16

Strategic recommendations for future-ready boards 17

Conclusion and recommendations 19

References 20

Foreword

In our dynamic world, the boardroom has become a paradoxical space. We are simultaneously at the cusp of unprecedented innovation and at the precipice of equally profound risks. For leaders in India, this tension is not an abstract concept; it is the daily reality of steering organisations through an era where the pace of digital change is extremely swift and the sophistication of cyber threats is relentless.

This report is a guide for circumventing that reality. It is born from a simple truth: the most critical decisions a board makes today are no longer confined to finance or market strategy. They now extend to the very digital fabric of the organisation, encompassing its resilience, integrity and ability to protect stakeholder trust. We see this in the surge of cyber incidents across the region, from the proliferation of ransomware to the crafty, artificial intelligence (AI)-driven social engineering attacks that exploit the human element. The same digital transformation that fuels our growth also expands our vulnerabilities, increasingly blurring the traditional lines between opportunity and threat.

The emerging technologies of AI, quantum computing and multi-cloud are more than business platforms. They are forces reshaping the risk landscape itself. They bring immense competitive advantage, while also introducing "invisible risks" that can quickly catch up with "visible benefits". This new paradigm demands a fundamental shift in governance, from reactive to proactive defence and integrated resilience. It calls for boards that are not just aware of technology, but are digitally literate, capable of asking the right questions and equipped to hold management accountable.

Ultimately, this is a human challenge. It is about leadership, foresight and a culture of vigilance that starts at the top and permeates every level of the organisation. The regulatory environment from India is mirroring this evolution, formalising what has long been a moral imperative, i.e. the duty to protect.

We hope its insights empower you to lead with confidence, transforming cybersecurity from a burden into a cornerstone of sustainable value and a catalyst for Cyber Surakshit Viksit Bharat.

Gaurav Shukla
Partner & Leader - Cyber
Deloitte South Asia

Daryl Pereira
CISO – Asia - Pacific
Google Cloud

Introduction

The corporate boardroom agenda is undergoing a profound transformation. This is because businesses are being driven by the relentless pace of digital and technological innovation, which is associated with elevating the sophistication of cyber threats. This report examines the evolving perspective of Boards over the next five years, focusing on the critical intersection of cybersecurity, emerging technologies and the increasing influence of regulatory frameworks, with a specific focus on India Boards face a dual challenge: harnessing the transformative power of new technologies for competitive advantage while simultaneously establishing robust guardrails to protect organisational integrity and stakeholder trust.

Current assessments indicate the boundaries of cybersecurity are blurring, just like the lines of digital transformation. As organisations share data and systems access with partners and other third parties, concerns about security and privacy are paramount. Ultimately, the growth of business, customer, data and digital trust is underpinned by the cybersecurity strategy, definition and enforcing of the controls and leveraging adequate solutions. Accordingly, many organisations are integrating cybersecurity across business and technology functions (The Promise of Cyber - Deloitte Global Future of Cyber Survey 4th Edition). However, significant gaps persist, particularly concerning the quality and strategic relevance of information flow from management and a rapid acceleration in AI adoption is not always matched by preparedness. Emerging technologies are blurring traditional risk boundaries, demanding a more integrated and forward-looking approach to governance. Concurrently, a wave of new regulations, such as India's Digital Personal Data Protection (DPDP) Act 2023 and RBI guidelines, such as Free-AI are intensifying board accountability, pushing cybersecurity from a technical concern to a core fiduciary duty across the region.

To pilot this complex landscape, future-ready boards must prioritise continuous education, implement integrated risk management (IRM) frameworks and cultivate a pervasive culture of proactive resilience. This strategic repositioning is essential not only for mitigating threats but also for transforming cybersecurity into a catalyst for long-term value creation and sustained organisational success.

The board's imperative: Circumventing the future of cyber risk

Introduction to the escalating cyber threat landscape and its transformation of corporate governance

The pervasive digital transformation of businesses, particularly in rapidly expanding economies such as India has fundamentally altered the risk landscape, making cybersecurity a paramount concern that permeates all aspects of corporate strategy and operations. Board members in India often ask if the cloud is more secure than on-premises infrastructure. The simple and quick answer is that, in general, it is. If one goes deeper, the answer is more nuanced and is grounded in a series of security "megatrends" that drive technological innovation and improve the overall security posture for enterprises. To ensure that they can lock in newfound agility, quality improvements and marketplace relevance, boards must prioritise safe, secure and compliant adoption of a new technological environment.

The cyber horizon of the next few years will be characterised by an accelerated pace of technological change and a corresponding evolution in threat sophistication and volume. This dynamic environment demands proactive and agile governance from corporate boards. As companies look beyond initial experiments with AI and make substantial investments to scale its use across their enterprises, the need for vigilant oversight becomes even more pronounced.

The board's evolving role: Balancing innovation acceleration with robust risk guardrails

Corporate boards are increasingly challenged to strike a delicate balance. On one hand, they need to encourage rapid adoption and significant investment in new technologies such as AI to maintain and gain competitive advantage. On the other hand, they need to simultaneously act as critical "guardrails" to safeguard stakeholder trust and manage the inherent and amplified risks associated with these innovations. This necessitates exercising critical judgment on how to generate acceleration while ensuring that strategic decisions are neither too risk-averse nor too risk-aggressive.

The very technologies driving unprecedented business growth and operational efficiency, significantly expand the organisation's attack surface. Innovation pursued without integrated security considerations and robust governance is not merely risky, but potentially self-sabotaging, leading to severe financial, reputational, regulatory and operational consequences. Boards must therefore grasp that cybersecurity is more than a cost center or a barrier, but a fundamental enabler of innovation and a cornerstone of long-term value creation.

Business service and mission assurance

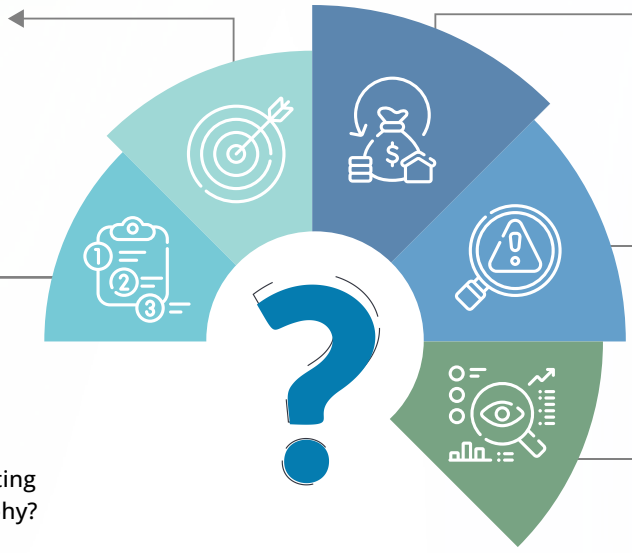
From a board perspective, the overall goal of a well-defined and orchestrated cybersecurity and risk function is to have significant ongoing assurance that business services or missions are operating securely and reliably.

Boards today increasingly focus on how cyber can optimise, preserve, protect and create value for the organisation. Being more cyber-mature does not make organisations immune to threats. It makes them more resilient when they occur, enabling critical business continuity. Boards should consider exploring how businesses have developed frameworks and governance models to integrate cyber risk, security and trust into their overall strategy. They should also ensure that cybersecurity is a proactive measure, not a reactive one. It must be recognised as an integral part of the organisation's strategic business, technology and operational framework.

They need to be more confident in challenging management on cybersecurity and technology risks should think of this as less of a dangerous threat.

They should be able to ask and get a reasonable answer to questions such as the ones listed below:

Who has deemed the residual risk acceptable? How do we independently challenge the acceptable level of residual risk to make sure we are not getting too comfortable?



What are our most critical assets and business processes?

What risks do these assets and processes face, and how are we mitigating them?

How do we monitor these mitigations to ensure they remain effective?

Are we meeting all regulatory requirements of the countries where we operate, as well as regulating ourselves in each geography?

The Board should be asking more leading questions about technology/ digital capability, not just lagging indicators of cyber performance. For example, "What percentage of our systems have been security risk-assessed and have an embedded 'secure by design' approach when they were built"? This strategic integration is crucial to avoid the inherent paradox of digital transformation.

Current cybersecurity challenges and boards' preparedness

The persistent threat landscape

The cyber threat landscape in India continues to evolve rapidly, shifting in scope, pace and sophistication. Analysis from various sources consistently identifies phishing attacks and social engineering as leading cyber threats, closely followed by ransomware, inherent weaknesses in cybersecurity systems and recent cross-border sanctions. India's rapid digital growth has significantly expanded its attack surface, leading to 369.01 million distinct malware detections across 8.44 million endpoints, with Trojans (43.38 percent) and Infectors (34.23 percent) being predominant threat vectors.[1] The growing sophistication and volume of attacks are particularly alarming.

India is witnessing sophisticated targeted attacks, including the introduction of malicious files into enterprise systems, exploitation of access keys in cloud environments and navigation across production and non-production environments, dramatically widening the blast radius. The overall volume and severity of these threats continue to grow, frequently targeting vulnerabilities that emerge from poor software coding practices and inadequate security measures employed by well-intentioned AI system developers, eager to rush products to market.

Despite significant advancements in technological defences, the human element remains a primary and increasingly sophisticated attack vector. The increasing sophistication of AI directly enables more convincing and scalable social engineering attacks. These AI-powered attacks then exploit the inherent human element more effectively, which is often considered the weakest link in the security chain. This direct exploitation means that solely relying on technical controls is insufficient, and traditional, generic employee awareness training becomes less effective against highly targeted and personalised AI-generated deception. Boards must recognise that cybersecurity is not solely a technology problem; it is fundamentally a human and cultural challenge. They need to ensure that cybersecurity strategies extend beyond technical controls to encompass robust, continuously updated and highly adaptive human-centric defences. This includes investing in advanced training programmes that simulate AI-powered threats, fostering a culture of critical thinking and scepticism and establishing clear protocols for verifying information and reporting suspicious activities across all levels of the organisation.

[1]India Cyber Threat Report 2025 | Data Security Council of India

Key questions for the board to consider

What adjustments are being made to the organisational structures and operating models responsible for implementing and overseeing risk appetite? For instance, how are the Chief Information Officer (CIO) and security operating model adapting to enable more agile Information Technology (IT) delivery within defined risk appetites, and to provide assurance over key controls in a dynamic technology environment?

How are regulators and other authorities being engaged, to keep them informed and aware of the organisation's strategy and of the plans for the migration of specific business processes and data sets? What feedback is the organisation receiving from regulators, and how is that informing our approach?

How are risk and control frameworks being adjusted, how is the organisation's risk profile changing, and how is the organisation staying within risk appetite?

How are we horizon scanning on the emerging trends and proximate threats?

Board oversight: Current state and gaps

Board engagement in cybersecurity oversight has seen positive developments. Despite the increased engagement and presence of expertise, a significant gap remains in the quality of information provided. Only 32 percent of corporate directors globally report being “completely satisfied with the information they currently receive from management on cybersecurity". A substantial 58 percent of directors explicitly state they would benefit from enhanced reporting from the management.[2] These numbers suggest a disconnect between the quantity of information and its actionable strategic value.

The increased frequency of reporting, without a corresponding improvement in the format, strategic relevance, or clarity of the information provided, leads to continued board dissatisfaction. The mere presence of a single “cyber expert” on the board may not be enough to bridge this communication gap if the management’s reports are not tailored for broader board understanding and strategic decision-making. Boards need to understand the implications of risks, not merely the technical details. They must actively collaborate with management to define the format and content of risk reports. This includes ensuring that reports analyse patterns across time and locations to provide a continuous perspective. It also means demanding metrics that measure the progress of innovation bets and highlight early warning signals, instead of merely focusing on the maximum acceptable risk. The ultimate objective should be to transform data into actionable intelligence for strategic governance.

[2]Risk Governance of Digital Transformation in the Cloud, Office of the CISO, Google Cloud

Building too much technical debt by underestimating the business consequences of inaction

Based on the success demonstrated by successful boards globally, Google Cloud's Office of the Chief Information Security Officer (CISO) has identified a shift in how cybersecurity is perceived. Leading boards are framing it as a strategic business enabler that directly supports their growth and vision. This proactive approach allows them to build a robust cyber function that is fully integrated into the corporate culture.

Boards in India focus on proactive oversight, strategic integration and fostering a risk-aware culture, rather than delegating cybersecurity solely to the IT function. Successful boards do not perceive cybersecurity exclusively through the lens of cost; successful boards recognise it as a critical investment in business resilience. This perspective allows them to prioritise resources and attention on the most relevant areas, ultimately transforming cybersecurity from a cost centre into a strategic asset that protects revenue, brand reputation and customer trust.

Google Cloud's Office of the CISO has identified a shift in how boards should view technical debt. They are not only seeing it as a technical issue; they recognise it as a significant source of avoidable cyber risk and a potential competitive disadvantage. This is particularly evident in mergers and acquisitions due diligence, where boards are proactively using two key processes to uncover and manage this risk. Boards in high-performing organisations are treating outdated and underfunded technology, including cybersecurity defences, as a potentially impaired asset. They understand that technology that does not perform its expected function can be a liability, much like non-functioning physical equipment. Similarly, they are using contingent liabilities estimation to better understand the future costs and risks associated with unaddressed cybersecurity vulnerabilities or an over-reliance on third-party vendors. This proactive approach enables them to estimate potential remediation costs and legal liabilities before they become a significant issue. By applying these strategic approaches, boards are effectively addressing technical debt, reducing their cyber risk exposure and ensuring their organisation maintains a competitive edge.

Not embracing bad news as a business improvement opportunity

It is human nature to downplay or, at times, hide bad news. Even information about a cyber "near miss" can cause a seasoned executive to hesitate before bringing it to the board. Boards need to provide the CISO/CIO a safe space to discuss challenges, concerns and missed opportunities. Boards should allow the CISO a chance to speak without the presence of other Chief Experience Officers (CXOs) in board meetings, so that conversations can occur more privately with increased candour.

The debatable question, therefore, is: How should Indian boards approach managing cyber risk alongside all their other risks?

Fundamentally, boards must realise that they are managing a portfolio of risks. This is an optimisation problem of balancing cost and opportunity cost vs. the risk and reward of business or mission activities.

Emerging technology risks and blurring boundaries

The rapid advancement of technology is increasing the demands on board oversight, necessitating enhanced digital literacy across the boardroom. At large digital transformation is defined as the use of modern digital technologies, including all types of public, private and hybrid cloud platforms, to create or modify business processes, culture and customer experiences to meet changing business and market dynamics. Digital transformation is propelled by a range of innovative technologies that are reshaping industries and redefining business possibilities. These technologies enable organisations to streamline operations, gain valuable insights from data and deliver innovative products and services.

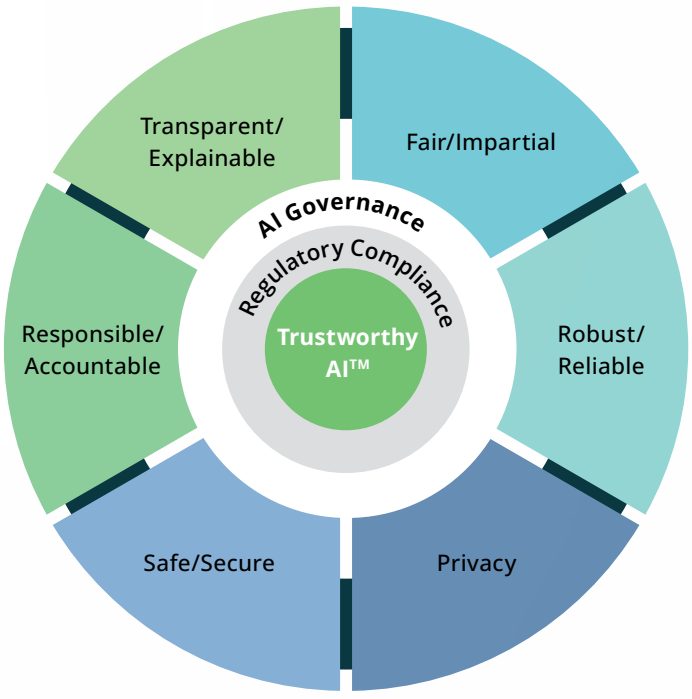
A significant part of this aspect is to tap into forces such as megatrends[3] that naturally help organisations. Boards should pay close attention to these megatrends because they are not just transient issues to be ignored once the year rolls around. Still, they influence the development of security and technology and will continue to do so for the foreseeable future. Boards should also consider that adopting a strategy that completely goes against one of these megatrends might be a signal that they need to revisit their game plan.

Boards are now compelled to evaluate not only the risks posed by cyber threats and malicious actors but also their organisation's capacity to adapt to relevant cyber risks in a technology-driven landscape strategically.

Opportunity and amplified risk of AI

AI represents a transformative force, capable of driving unprecedented efficiencies and competitive advantages across industries. However, its rapid integration, particularly in India, also presents significant and complex cybersecurity risks. The dual-edged nature of AI means it can accelerate innovation while simultaneously intensifying risk. AI drives efficiency and competitive advantage, but it also introduces new vulnerabilities and ethical dilemmas. Boards must strike a balance between adoption velocity and comprehensive risk management, ensuring the ethical development and deployment of AI. This is about managing the inherent tension between innovation and control, ensuring that the pursuit of technological advantage does not inadvertently create catastrophic vulnerabilities.

Deloitte's Trustworthy AI™ Framework



[3]Megatrends

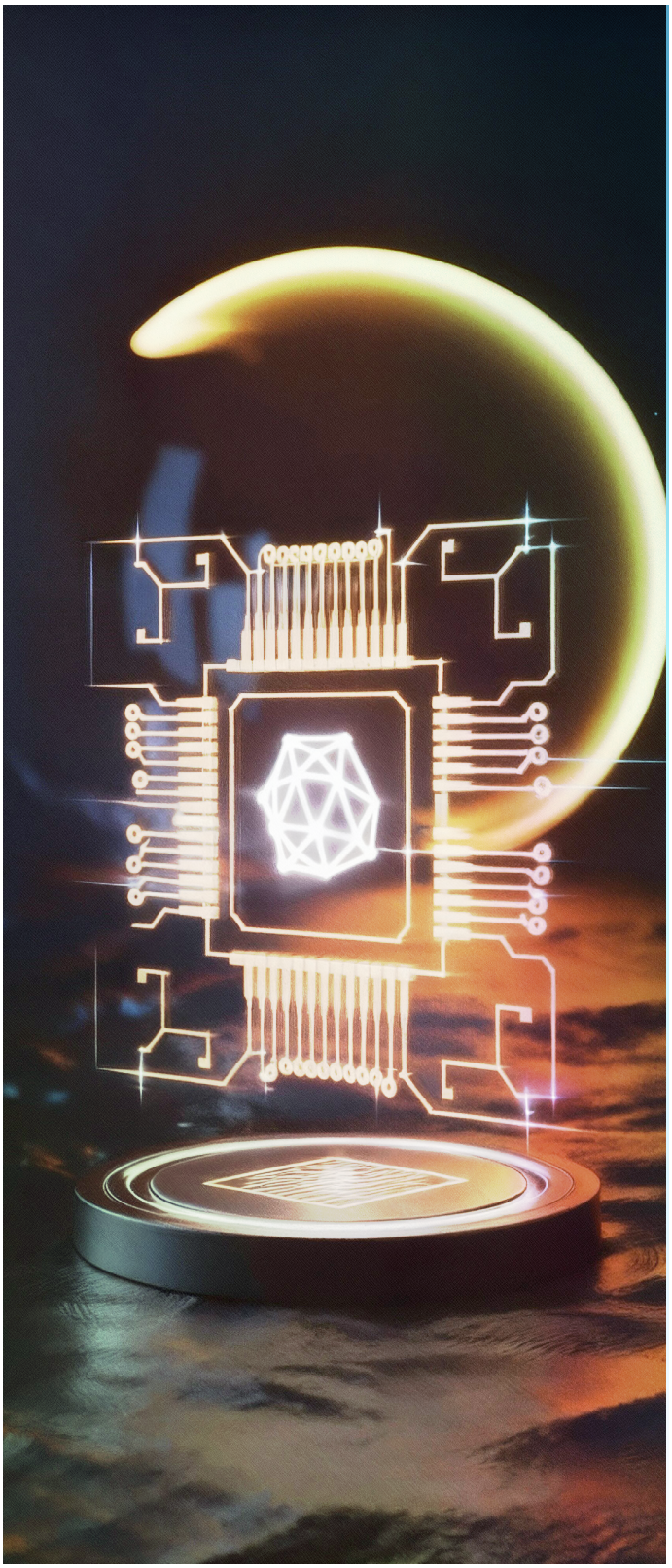
The looming cryptographic threat of quantum computing

Although still in its early stages, quantum computing poses a significant long-term threat to current cybersecurity paradigms. India's National Quantum Mission (NQM), approved in April 2023 with a budget of INR6,003.65 crore (2023–2031),[4] aims to position India as a global leader in quantum technology, including the development of quantum-resilient encryption techniques and Post-Quantum Cryptography (PQC) frameworks. The future threat of quantum computing, while not immediate, demands proactive mitigation. The time to prepare is now, given the extended transition period required for implementing PQC across complex IT infrastructures. Boards must initiate strategic planning for cryptographic agility to protect long-term data confidentiality and ensure the organisation's foundational security mechanisms remain robust against future computational advancements.

Exploitation expansion: Zero-days and supply chain risks

Zero-day exploitation, which involves exploiting previously unknown vulnerabilities, is no longer the exclusive capability of highly sophisticated actors. The proliferation of exploit technology has made this troubling threat available to a broader range of global adversaries. The Google Threat Intelligence Group (GTIG) observed a continued and critical increase in the exploitation of enterprise-specific technologies throughout 2024. The proportion of zero-day vulnerabilities targeting enterprise products jumped from 37 percent in 2023 to 44 percent in 2024,[5] showing a persistent expansion of the attack surface.

A disturbing development is the concentration of attacks on the very technologies intended to provide defence. Zero-day vulnerabilities in security and networking software and appliances accounted for over 60 percent of all zero-day exploitation of enterprise technologies in 2024. This means that perimeter security appliances, such as those with high-value tools and extensive administrative access, are now the most effective vectors for extensive system compromise. This shift necessitates a radical overhaul of trust models. The failure of perimeter-based security is evident, indicating that the architectural reliance on the security appliance's inherent trustworthiness is fundamentally flawed. Therefore, the board must treat the wholesale transition to Zero Trust Architecture (ZTA), encompassing least-privilege access and network segmentation, as a necessary capital expenditure to secure core business processes, rather than an optional IT project.



[4]National Quantum Mission: India's Quantum Leap
[5]A review of zero-day in-the-wild exploits in 2023 - Google Blog

Regulatory changes and board accountability

The landscape of corporate governance is increasingly shaped by a growing body of regulations that mandate and intensify board oversight of cybersecurity. This regulatory dominance is a primary driver for boards to elevate cybersecurity to a strategic imperative.

The intensifying regulatory landscape

The regulatory landscape in India is rapidly intensifying, imposing robust oversight requirements on boards. In India, the DPDP Act, which came into effect in August 2023, regulates the processing of digital personal data and has extraterritorial effect for entities offering goods or services in India. The Act establishes the Data Protection Board of India as an independent body for enforcement, with powers similar to those of a civil court. Operating digitally. Significant Data Fiduciaries (SDFs) under the DPDP Act have additional obligations, including designating a Data Protection Officer in India who is responsible to the board, appointing an independent data auditor and undertaking Data Protection Impact Assessments and periodic audits. Penalties for non-compliance can range from INR50 crore to INR250 crore per violation,[6] with the highest fines for breaches of security safeguards, failure to notify breaches and mishandling children's data.

Board accountability and fiduciary duties

The failure of a board to properly understand and effectively mitigate cyber risks, resulting in a cyber incident or damage to the company (whether reputational or otherwise), may amount to a breach of director duties, potentially exposing directors to personal liability in certain jurisdictions.

For instance, in India, non-compliance with the DPDP Act can result in sanctions for violations, with the Data Protection Board having powers similar to those of a civil court. While the DPDP Act primarily targets data fiduciaries, significant data fiduciaries are required to appoint a data protection officer responsible to the board of directors.

The evolving standard of care means boards are increasingly expected to possess or acquire sufficient cyber literacy to fulfil their oversight duties, moving beyond delegating entirely to management. This elevates the standard of care to include proactive engagement with technology risks, fostering a culture of cyber resilience from the top down. Directors have a fiduciary duty to exercise reasonable care, skill and diligence, which now explicitly extends to cybersecurity oversight. This requires boards to organise themselves to ensure cybersecurity receives appropriately informed attention and oversight. While the board retains final oversight, much of the initial work can and should be done by board committees, which can provide more knowledgeable

[6]The Digital Personal Data Protection Act, 2023

Strategic recommendations for future-ready boards

To effectively navigate the complex and rapidly evolving landscape of cybersecurity and technology risks, boards must adopt a proactive, integrated and continuously adaptive approach to governance.

Enhancing board expertise and governance structures

A critical first step is to cultivate cyber literacy across the entire board. Optimising oversight allocation is equally essential. While the audit committee frequently oversees cybersecurity (81 percent of Fortune 100 companies in 2024, up from 20 percent in 2018),[7] boards should periodically reassess where cyber risk oversight sits, whether with the whole board, an audit committee, a risk committee or a dedicated cybersecurity or technology committee, to ensure its effectiveness. Clear documentation and communication of responsibilities across various committees (risk, audit, compliance) are essential, providing a multi-disciplined and collaborative approach that integrates technological innovation and related risks. For instance, a technology committee charter might include oversight of technology strategy, significant technology investments, operational resiliency planning and third-party technology strategy, with regular reports to the risk and compliance committees.

Boards should also champion the adoption of IRM frameworks. IRM encourages a holistic and dynamic approach to risk management, recognising that individual risks are interconnected and can impact areas across the institution. This involves building a comprehensive risk ecosystem with coordinated systems and processes for enhanced decision-making. A key pillar of IRM is fostering a risk-aware culture in which every employee, from management to entry-level hires, understands and actively participates in risk mitigation. This framework helps align IT plans with business goals, manage risks effectively and ensure IT processes meet stakeholder needs.

[7]The Role of Auditors in Company-Prepared Cybersecurity Information: Present and Future

Proactive risk management and resilience building

Developing robust risk appetite frameworks is paramount. Boards should consider developing and using these frameworks to guide decision-making, focusing on the maximum acceptable risk while also agreeing on early warning signals and metrics to gauge the progress of innovation bets. This ensures that risk-reduction decisions are shared across security and business stakeholders, based on a shared understanding of organisational risk appetite.

Continuous threat intelligence and assessment are vital for maintaining a strong security posture. Business continuity and crisis contingency plans should be regularly pressure-tested, accounting for a variety of scenarios, including responses to geopolitical crises and other potential threats. Regular management-crisis exercises can expose faulty information flows and interpersonal tensions that could lead to breakdowns in a real crisis. Boards should also ensure their organisation uses external frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27001, ISO 42001, ISO 42005, MITRE Corporation's Adversarial Threat Landscape for Artificial-Intelligence Systems (MITRE Atlas), Security Architecture Implementation Framework (SAIF), Cybersecurity Assessment and Risk Analysis Framework (CARAF) and/or Control Objectives for Information and Related Technologies (COBIT), to boost cyber defences and gain a clear view of organisational readiness. These frameworks provide structured methods to evaluate an organisation's cyber posture, identify gaps and align cybersecurity efforts with business goals. As India embarks on meeting the Viksit Bharat goal with the Cyber Surakshit Bharat vision, the urgency of a proactive, intelligence-driven approach to mitigating digital risks is warranted.

Finally, using AI for Governance, Risk and Compliance (GRC) activities can significantly enhance board oversight. AI can automate risk identification and assessment, scanning internal and external data to flag emerging risks and prioritise them based on severity and likelihood. It can review policies for outdated language or regulatory misalignment, suggest updates and automate workflows for changes. For compliance, AI can track regulatory databases for new rules, map updates to existing controls and send real-time alerts when compliance thresholds are at risk. AI can also compile audit-ready documentation, flag missing controls and generate reports with minimal human input. Furthermore, AI can enhance incident detection and response by analysing user behaviour for policy violations, classifying incidents and suggesting response actions. This automation frees up GRC teams to serve more strategic roles, providing boards with enhanced data analysis, improved decision-making, streamlined policy creation and real-time insights.

Fostering a culture of cyber resilience

Cultivating an enterprise-wide cybersecurity culture is fundamental. Boards must emphasise that cybersecurity is an enterprise-wide business risk, not solely an IT concern. The "tone at the top" from the board and senior executives is crucial for promoting individual awareness, commitment and training across the organisation. This mindset begins at the board level, with the responsibility of overseeing the implementation, use and monitoring of all technologies.

Continuous employee training and awareness programmes are essential to counteract the human element as an amplified vulnerability. Boards should govern the organisational cyber literacy on technology use, ethics and policies.

Strategic communication and transparency are vital for effective oversight. Boards need to demand enhanced reporting from management, ensuring they receive consistent and comprehensive information to inform their decision-making. This involves reviewing the format of risk reports periodically to ensure they analyse patterns across time and locations, enabling a continuous rather than fragmented perspective. Establishing clear communication channels for risk reporting is crucial for IRM. Boards should also ensure the CISO has a seat at the table during strategic discussions and is included in the company's disclosure controls and procedures process. For India, Deloitte emphasises the need for a futuristic yet unified cybersecurity framework to protect the country's critical digital frontiers.

Conclusions and recommendations

The future of board governance, particularly over the next five years, is inextricably linked to the effective oversight of cybersecurity and technology risks. The analysis reveals a landscape where traditional risk boundaries are blurring, driven by the rapid adoption of transformative technologies, including AI, quantum computing and cloud computing. While boards are demonstrating increased engagement and a growing presence of cyber expertise, significant challenges persist in the quality of information received and the ability to maintain pace with the increasingly sophisticated threats. The intensifying regulatory environment, with its emphasis on board accountability and personal liability, further underscores the imperative for proactive and robust governance. To thrive in this complex digital future, boards are presented with clear strategic imperatives, as follows:

Elevating digital literacy and expertise

Boards must proactively invest in continuous education for all directors on emerging technologies and cyber risks. This includes structured cyber literacy programmes and, where necessary, recruiting directors with deep technology and cybersecurity experience. The goal is to ensure collective understanding, enabling informed challenge and strategic guidance, rather than relying on a single "expert".

Cloud as a means of managing risk

Adopting cloud technologies and adjusting business practices, processes and operating models to use the advantages of cloud fully, providing organisations with an opportunity to step-change their management of operational risk. Public clouds offer security and resilience levels that few organisations have achieved on-premises, thanks to their scale. Specific configurations, enhanced security features and ongoing security operations and updates incur additional, necessary costs. However, the per-unit cost remains lower than on-premises services, whose economics are moving in the opposite direction. Therefore, cloud adoption strategically raises the security baseline by reducing the cost of control.

Implement Integrated Risk Management

This involves moving beyond siloed risk assessments to adopt holistic, enterprise-wide IRM frameworks. This involves embedding cyber risk considerations into all strategic decisions, from new product development to third-party partnerships. Boards should define clear risk appetites, establish early warning signals and ensure continuous monitoring of the entire attack surface, including supply chains and multi-cloud environments. Given the surge in third-party breaches in the Asia Pacific (APAC) region, robust third-party risk management is paramount.

Demanding actionable intelligence

Boards must actively shape the reporting they receive from management. This means moving beyond technical jargon to strategically relevant, continuous and forward-looking reports that translate complex cyber risks into clear business implications. Metrics should focus on resilience, adaptive capacity and the effectiveness of controls against evolving threats, rather than static compliance.

Fostering a culture of proactive resilience

Cybersecurity must be ingrained as an enterprise-wide cultural imperative, driven by the "tone at the top". This involves continuous, adaptive employee training programmes designed to counter sophisticated social engineering attacks (especially AI-driven deepfakes prevalent in APAC),[8] regular pressure-testing of incident response and business continuity plans through realistic exercises and using advanced technologies such as AI to enhance GRC functions.

Embracing regulatory compliance as a strategic enabler

It is necessary to view regulatory requirements not merely as compliance burdens but as frameworks that drive best practices and enhance organisational resilience. Boards must stay updated on evolving global and regional regulations/guidelines and policies, such as India's DPDP Act and RBI Free AI, understanding their personal and corporate liabilities and ensuring robust disclosure practices that balance transparency with security.

By adopting these recommendations, boards can transform cybersecurity from a daunting challenge into a strategic differentiator, safeguarding organisational value, maintaining stakeholder trust and positioning their enterprises for sustainable growth in the digital age.

[8]Deepfake awareness training: a quick guide by guardey

References

1. Perspectives on Security for the Board March 2025 – Edition 7, Office of the CISO, Google Cloud
2. Perspectives on Security for the Board Nov 2024 – Edition 6, Office of the CISO, Google Cloud
3. Perspectives on Security for the Board Mar 2024 – Edition 4, Office of the CISO, Google Cloud
4. A review of zero-day in-the-wild exploits in 2023 - Google Blog
5. Board of Directors - Summary Guide to Cloud Risk Governance, Cloud CISO, Google Cloud
6. Risk Governance of Digital Transformation in the Cloud, Office of the CISO, Google Cloud
7. 10 questions to help boards safely maximize cloud opportunities, Cloud CISO, Google Cloud
8. 4 ways to improve cybersecurity from the boardroom, Cloud CISO, Google Cloud
9. A billion minds, one vision: Data privacy as the pillar of Viksit Bharat - Deloitte
10. Cyber Surakshit Bharat: Protecting the digital frontier for Viksit Bharat - Deloitte
11. AI at crossroads: Building trust as the path to scale - Deloitte
12. Global Future of Cyber 4th edition - Deloitte
13. India Cyber Threat Report 2025 | Data Security Council of India - DSCI
14. AI Impacts Board Readiness for Oversight of Cybersecurity and AI Risks
15. Digital Threat Report 2024 by Press Information Bureau
16. Board Oversight of AI - The Harvard Law School
17. National Quantum Mission: India's Quantum Leap
18. Enterprise Governance, Risk And Compliance Market Report, 2030 - Grand View Research
19. Data Boundary via Assured Workloads | Sovereign Cloud - Google Cloud
20. The Digital Personal Data Protection Bill, 2023
21. Governing Cybersecurity from the Boardroom - Research Gate

About Deloitte

Deloitte is one of the world's largest and most diversified professional services organisations, providing assurance and advisory, tax, management consulting, and enterprise risk management services through more than 345,374 professionals in more than 150 countries. Our organization includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touche Tohmatsu India LLP (DTTI LLP) also referred as Deloitte India is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate.

In India, Deloitte is spread across 12 cities with over 12,000 professionals, who are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments. Deloitte is well-equipped to deliver solutions to the complex challenges faced by organisations across the public and private sectors. Our edge lies in our ability to draw upon a well- equipped global network and teaming this with customised services at a local office.

We have been consistently recognized as leaders by Gartner in Cybersecurity, the Data and Analytics space, as well for Public Cloud Infrastructure Managed and Professional Services and Oracle Cloud Application Services.

https://www2.deloitte.com/in/en.html

About Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

https://cloud.google.com | https://cloud.google.com/security

Connect with us

Deloitte India

Shefali Goradia
Chairperson
Deloitte South Asia
shefalig@deloitte.com

Gaurav Shukla
Partner & Leader - Cyber
Deloitte South Asia
shuklagaurav@deloitte.com

Deepa Seshadri
Partner
Deloitte India
deseshadri@deloitte.com

Munjal Kamdar
Partner
Deloitte India
mkamdar@deloitte.com

Sathish Gopalaiah
President - Technology & Transformation
Deloitte South Asia
sathishtg@deloitte.com

Abhrajit Ray
Partner
Deloitte India
abhrajitray@deloitte.com

Tarun Kaura
Partner
Deloitte India
tkaura@deloitte.com

Ashish Sharma
Partner
Deloitte India
sashish@deloitte.com

Google Cloud

Daryl Pereira
CISO – Asia - Pacific
Google Cloud
darylpereira@google.com

Ganesh Supekar
Lead – Regional Partnerships
Google Cloud India
supekar@google.com

Vineet Parameswaran
Head – Strategic Partnerships
Google Cloud India
pvineet@google.com

Jyoti Prakash
Head – Security Business
Google Cloud India
jprakaship@google.com

Contributors

Deloitte India

Hiten Panchal

Google Cloud

Rohan Kanungo

David Homovich

Acknowledgements

Arti Sharma

Manasi Kajabaje

Sampreeti Sen

Sunita Kumari

This co-authored whitepaper applies to Google Cloud and Security products described in the Google Cloud Services Summary. The content contained herein is correct as of August 2024 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP) and Google Cloud India.