Cyber Risk Is in the Boardroom. Are Boards Ready to Govern It?

Sanchay Joshi, CISSP, CISA, FIP, LL.B.
Cybersecurity, Privacy and Technology Risk Advisor
Brisbane, Australia
LinkedIn: www.linkedin.com/in/sanchay-joshi

I. Executive Summary

Cybersecurity is now a boardroom issue, but board attention alone is not enough. As cyber risk becomes more connected to resilience, legal accountability, disclosure, AI, and enterprise value, boards need to move from receiving cyber updates to exercising effective cyber oversight. This article explains how cyber risk reached the boardroom and what organisations can do to make oversight practical, business-relevant, and accountable.

A. Cyber is now board business

Cybersecurity has evolved from an IT operational concern into a core boardroom governance issue. High-impact breaches, ransomware attacks, regulatory disclosure expectations, and governance frameworks have made cyber risk a matter of resilience, legal accountability, stakeholder trust, and enterprise value. Emerging AI-related risks are further expanding this governance challenge.

B. Attention is not oversight

Increased board attention has not automatically produced effective oversight. Many boards still receive technical updates, compliance summaries, or high-level dashboards that do not clearly translate cyber risk into business impact, risk appetite, resilience readiness, investment trade-offs, or disclosure obligations.

C. Four shifts matter

Effective board-level cybersecurity oversight requires four practical shifts. Boards need sufficient cyber-risk literacy to challenge management without becoming technical specialists. Oversight must move from prevention alone to resilience, including tested incident response and business continuity plans. Board and management responsibilities must be clearly defined, with executives translating board expectations into resources, controls, culture, and readiness. Finally, cyber reporting must connect technical risk to business decisions, investment priorities, disclosure obligations, and long-term enterprise value.

D. Govern well, compete better

The boardroom question is no longer whether cybersecurity matters, but whether boards can govern it with the same discipline applied to financial, operational, and strategic risk. Organisations that do this well will be better positioned to withstand disruption, protect stakeholder trust, preserve enterprise value, and turn secure digital capability into a source of competitive advantage.

II. Introduction: Cyber is now board business

Cybersecurity oversight has become one of the defining governance challenges for modern boards. Cyber risk now affects operations, stakeholder trust, enterprise value, legal accountability, and regulatory confidence. High-impact data breaches and ransomware attacks have shown that cyber failures can disrupt business operations, trigger regulatory scrutiny, damage reputation, and force executive accountability.

This shift has been operationalised by governance frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001, expanding regulatory obligations around data protection, incident notification, and cybersecurity disclosure, and growing legal scrutiny of board and executive accountability. Together, these developments have exposed the inadequacy of treating cyber risk as an issue for technology teams alone. Cybersecurity is now an enterprise risk and business resilience issue that boards are expected to oversee with the same seriousness applied to financial, operational, and compliance risks.

The governance challenge is becoming more complex with the rise of artificial intelligence. AI introduces a new layer of cybersecurity oversight because AI systems can be exploited through adversarial attacks, amplify the scale and sophistication of cyber threats, and create novel vulnerabilities that traditional security approaches may not fully address [1]. Boards must therefore oversee not only the protection of traditional digital assets, but also the security, integrity, and governance of AI models and AI-enabled business processes.

Despite this growing attention and expanding oversight responsibility, increased board attention has not automatically translated into effective cyber oversight. Too often, directors are presented with technical jargon, compliance checklists, or superficial dashboards that obscure the real business impact, legal liability, resilience implications, and financial trade-offs associated with cyber risk [2]. Consequently, cybersecurity sits on the board agenda without the strategic clarity required for effective governance. To bridge this gap, boards must pivot from passive listening to active inquiry across four

critical fronts: understanding the organisation's actual risk posture, strengthening operational resilience, clarifying management accountability, and aligning cyber reporting with board decision-making**.**

This article traces the evolution of cybersecurity as a boardroom priority and examines how organisations can make board-level cyber oversight more effective through stronger cyber-risk capability, resilience-focused oversight, clearer board-management accountability, and cyber reporting aligned with board decision-making**.**

III. How Cyber Became A Boardroom priortity?

Boards have long carried the fiduciary duty for corporate strategy, enterprise risk, compliance, and resilience. As the threat landscape has evolved, cybersecurity has forced its way into the boardroom precisely because it now threatens each of these foundational pillars. Consequently, what was once delegated as a specialized IT concern has integrated into the board's core governance mandate.

A. Cyber began as an IT concern

For decades, cybersecurity was largely invisible to corporate boards. The prevailing view was that cyber threats were technical problems meant to be managed by the CIO, IT manager, or technology teams, similar to maintaining servers, networks, and email systems [3]. Board agendas were more commonly dominated by financial performance, strategic transactions, legal compliance, and the requirements introduced by the Sarbanes-Oxley Act of 2002 for publicly listed companies in the United States [4].

Although Sarbanes-Oxley did not explicitly address cybersecurity, it created a governance infrastructure around internal controls, executive certification, disclosure, and accountability that later became relevant to cyber oversight [5]. By requiring CEOs and CFOs to personally certify the accuracy of periodic reports and the effectiveness of disclosure controls and procedures, the Act introduced principles that would eventually extend to cybersecurity disclosures as cyber risks and incidents became material business risks requiring disclosure assessment [6].

This period therefore marked an important starting point: cyber risk was not yet treated as a board-level enterprise risk, but the governance foundations for future board accountability were beginning to emerge.

B. From News Headlines to the Boardroom: How Data Breaches Redefined Leadership Priorities

This began to shift following major cyber incidents that exposed the inadequacy of treating cybersecurity as a purely technical issue. The 2013 Target data breach, which involved the compromise of point-of-sale systems through third-party vendor credentials, affected more than 60 million customers, triggered lawsuits, created significant costs, and contributed to the resignation of both the CIO and CEO [7]. The 2017 Equifax breach, caused by a failure to apply a known security patch, exposed sensitive data relating to 143 million individuals, resulted in major legal, financial, and reputational consequences, and was followed by the departure of the CIO, CSO, and CEO [8]. Together, these incidents demonstrated that cyber failures could damage customer trust, trigger regulatory scrutiny, impose significant financial costs, and reach the level of executive accountability.

C. Colonial Pipeline made cyber a resilience issue

The 2021 Colonial Pipeline ransomware attack broadened board-level concern further by showing that cyber incidents could disrupt critical infrastructure and threaten national security. The attack affected a major fuel pipeline supplying the eastern United States, contributed to fuel shortages and panic buying, and led to emergency government action [9]. Unlike earlier breaches that were often understood primarily as data protection failures, Colonial Pipeline made cyber risk visible as an operational resilience issue: a cyberattack could affect fuel supply, transport, business continuity, public confidence, and the security of nationally important infrastructure. For many organisations, the lesson was clear: cyber investment could no longer be justified only as IT protection, but as a necessary investment in operational continuity, resilience, and stakeholder trust.

D. Regulation made cyber a disclosure issue

Alongside these incidents, regulatory developments further elevated cybersecurity to board-level attention. These included U.S. Securities and Exchange Commission guidance and rules on cybersecurity disclosure, the EU's General Data Protection Regulation, Australia's Notifiable Data Breaches scheme under the Privacy Act 1988, the Security of Critical Infrastructure Act 2018, and the Cyber Security Act 2024 [10]–[15]. These regimes differ in scope and do not prescribe a single board structure for cybersecurity oversight. However, they create organisational obligations around cyber risk management, personal data protection, breach notification, disclosure, and accountability. For boards, the practical implication is clear: directors must ensure that management has appropriate systems to identify, manage, escalate, and disclose cyber incidents and cyber risks where required.

E. Frameworks made cyber a governance issue

In recent years, this shift has been reinforced by structured frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework [16], [17]. A significant development occurred in February 2024, when NIST released Cybersecurity Framework 2.0 and introduced a sixth core function: "Govern." The Govern function focuses on establishing and maintaining the governance structures necessary for an organisation to manage cybersecurity risks in alignment with business objectives and regulatory requirements. It includes organisational context, risk management strategy, roles and responsibilities, policy, oversight, and cybersecurity supply chain risk management [17]. Its addition represents a formal recognition that cybersecurity governance is not merely an operational activity, but a distinct area requiring executive and board-level attention.

F. Organisations formalised cyber oversight

In response to this growing attention, many organisations have created board-level risk or technology committees and strengthened executive cybersecurity reporting lines [18]. However, the maturity of board engagement remains uneven in practice, particularly in the depth of full-board involvement, the quality of cyber reporting, the clarity of accountability, and directors' ability to challenge management on cyber risk [19]. The central challenge is therefore not whether boards should oversee cybersecurity, but how they can oversee it effectively.

IV. Making Board-level Cybersecurity Oversight Effective

While cybersecurity now commands a permanent place on the board agenda, formal oversight structures do not automatically produce effective governance. Effective board-level cybersecurity oversight requires boards to convert increased attention into active governance. This means understanding cyber risk as enterprise risk, clarifying who owns oversight, focusing on resilience rather than only prevention, and aligning cyber reporting with board decision-making.

A. Strengthen board cyber risk capability

A critical challenge in board-level cybersecurity oversight is the gap between technical cyber information and business decision-making. Directors do not need to become cybersecurity specialists, but they must be able to understand cyber risk as an enterprise-wide risk management issue rather than a purely IT concern. This requires sufficient cyber-risk literacy to ask informed questions, understand the legal, regulatory, and business implications of cyber incidents, assess whether risks are within the organisation's tolerance, evaluate whether cyber investments are reducing enterprise risk, and challenge management where necessary. Where boards lack sufficient internal expertise, directors should have access to appropriate cybersecurity advice to support informed oversight [2].

B. Shift oversight from security to resilience

Traditionally, organisations have focused cybersecurity oversight on preventing breaches and protecting digital assets. However, as cyber threats become more advanced, preventing every attack is unrealistic. Boards should therefore shift the conversation from asking only "Are we secure?" to asking whether the organisation can detect, respond to, recover from, and learn from cyber incidents.

Incident response is central to this shift. Effective board oversight should ensure that incident response and business continuity plans are documented, tested, and understood by management before a crisis occurs. This includes clear escalation thresholds, defined decision-making authority, communication protocols, legal and regulatory notification processes, and recovery priorities for critical business operations. Tabletop exercises and post-incident reviews can help boards and executives assess whether the organisation is genuinely prepared or merely compliant on paper [2].

C. Clarify board-management accountabiliity

Many boards assign detailed cyber-risk oversight to the audit committee, risk committee, or a dedicated technology or cybersecurity committee [18]. Regardless of the structure chosen, committee responsibilities should be explicitly documented, supported by appropriate expertise, and accompanied by substantive and recurring attention to cybersecurity [2]. Even where a committee leads detailed oversight, oversight of cybersecurity and resilience should remain a collective responsibility of the full board because cyber risk can affect strategy, operations, disclosure, reputation, and enterprise value.

Effective cybersecurity oversight requires a clear distinction between board and management responsibilities. The board's role is to oversee, challenge, set expectations, and hold management accountable. Executive management is responsible for implementing the cyber strategy, allocating resources, operating controls, preparing incident-response capability, and embedding cyber risk into business decisions. Senior leaders bridge board expectations and organisational action. By visibly prioritising cybersecurity, they signal that cyber risk is not merely a compliance or technology issue, but a business priority, helping shape cybersecurity culture, resource allocation, control implementation, and employee behaviour [20].

D. Align cyber reporting with board decision-making

Boards cannot oversee cyber risk effectively if reporting is too technical, too brief, or disconnected from business impact [2]. Too often, directors are flooded with highly technical jargon, granular compliance checklists, or superficial "red-green" dashboards [21]. Rather than clarifying the organization's risk posture, this deluge of low-level data frequently obscures real business impact, legal liability, and the complex financial trade-offs required to mitigate sophisticated threats.

This information asymmetry creates a dangerous illusion of oversight. Management teams often mistake reporting activities for risk management, presenting voluminous data on firewall blocks or patch rates that fail to answer a board's most fundamental question: *Are we resilient?* By focusing on technical metrics rather than enterprise risk, boards are left unequipped to evaluate how a major cyber disruption would impact cash flow, operational continuity, or long-term enterprise value. Consequently, security budgets are constructed without being able to quantify how those investments contribute to risk reduction.

Furthermore, this governance gap severely compromises a board's ability to manage its growing legal and regulatory exposure. Where regulators impose explicit accountability for cyber oversight, passive reliance on high-level summaries can be significantly more difficult to defend as adequate governance. If management does not translate technical updates into the business, legal, and materiality implications relevant to the board's fiduciary and oversight responsibilities, directors cannot effectively determine when an incident crosses the threshold into a disclosable material event.

To bridge this divide, cyber reporting between executive management and the board must shift away from technical operational metrics and towards a formalised framework that quantifies cyber risk in financial terms and explains its strategic impact. Effective oversight therefore depends on reporting that connects technical risk to business decisions, investment priorities, disclosure obligations, and long-term enterprise value.

V. Conclusion: Govern Well, Compete Better

The evolution of corporate board oversight of cyber risk reflects a broader maturation in how enterprises understand and govern digital threats. From its origins as an IT operational concern, cyber risk has become a strategic, legal, regulatory, and resilience imperative requiring board-level attention. The era of treating cyber risk as a technical matter beneath the board's notice is definitively over.

Today's boards face a complex and evolving mandate. They must ensure that cybersecurity is integrated into enterprise risk management, that management has the expertise and resources to protect the organisation, that incident response plans are tested and ready, and that public disclosures about cybersecurity are accurate and not

misleading. They must also determine whether the audit committee, risk committee, technology committee, or full board is best positioned to oversee cyber risk, while ensuring technical issues are translated into business consequences.

The next phase of this evolution will be shaped by how boards respond to AI, supply chain interdependence, systemic cyber threats, and increasing legal and regulatory scrutiny. Cyber risk oversight has become a central test of corporate governance. Boards that fail to evolve risk legal, operational, and reputational consequences; boards that govern cyber risk well can turn cybersecurity into a source of resilience, stakeholder trust, secure innovation, and competitive advantage.

REFERENCES

[1] World Economic Forum, *Global Cybersecurity Outlook 2026*, Insight Report, Geneva, Switzerland: World Economic Forum, Jan. 2026. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf. [Accessed: Jul. 3, 2026].

[2] L. Clinton, *Director's Handbook on Cyber-Risk Oversight*, 5th ed. Arlington, VA, USA: National Association of Corporate Directors and Internet Security Alliance, 2026. [Online]. Available: https://www.nacdonline.org/globalassets/public-pdfs/2026_directors-handbook-cyber-risk_accessible.pdf. [Accessed: Jul. 3, 2026].

[3] J. Easterly, "Corporate cyber governance: Owning cyber risk at the board level," *Cybersecurity and Infrastructure Security Agency*, Jan. 8, 2025. [Online]. Available: https://www.cisa.gov/news-events/news/corporate-cyber-governance-owning-cyber-risk-board-level. [Accessed: Jul. 3, 2026].

[4] J. G. Proudfoot, W. A. Cram, S. Madnick, and M. Coden, "The Importance of Board Member Actions for Cybersecurity Governance and Risk Management," *MIS quarterly executive,* vol. 22, no. 4, pp. 235-250, 2023, doi: 10.17705/2msqe.00084.

[5] M. A. Geiger and P. L. Taylor III, "CEO and CFO certifications of financial information," *Accounting Horizons*, vol. 17, no. 4, pp. 357–368, Dec. 2003.

[6] C. M. Krus, "Who is listening? The SEC emphasizes importance of cybersecurity disclosure," *Journal of Investment Compliance*, vol. 13, no. 1, pp. 30–32, 2012, doi: 10.1108/15285811211216673.

[7] D. F. Larcker, P. C. Reiss, and B. Tayan, "Critical update needed: Cybersecurity expertise in the boardroom," *Stanford Closer Look Series*, Corporate Governance Research Initiative, Stanford Graduate School of Business, Nov. 16, 2017. [Online]. Available: https://ssrn.com/abstract=3074594. [Accessed: Jul. 3, 2026].

[8] U.S. House of Representatives, Committee on Oversight and Government Reform, *The Equifax Data Breach: Majority Staff Report*, 115th Cong., Dec. 2018. [Online]. Available: https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf. [Accessed: Jul. 3, 2026].

[9] J. Easterly and T. Fanning, "The attack on Colonial Pipeline: What we've learned & what we've done over the past two years," *Cybersecurity and Infrastructure Security Agency*, May 7, 2023. [Online]. Available: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. [Accessed: Jul. 3, 2026].

[10] U.S. Securities and Exchange Commission, "Cybersecurity risk management, strategy, governance, and incident disclosure," Final Rule, Release No. 33-11216, File No. S7-09-22, Jul. 26, 2023. [Online]. Available: https://www.sec.gov/rules-regulations/2023/07/s7-09-22. [Accessed: Jul. 3, 2026].

[11] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," *Official Journal of the European Union*, L 119, pp. 1–88, May 4, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. [Accessed: Jul. 3, 2026].

[12] Office of the Australian Information Commissioner, "Part 4: Notifiable Data Breach (NDB) Scheme," *OAIC*, updated Feb. 2025. [Online]. Available: https://www.oaic.gov.au/privacy/notifiable-data-breaches/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme. [Accessed: Jul. 3, 2026].

[13] Australian Government, *Privacy Act 1988*, No. 119, 1988, compilation no. 104, Jun. 4, 2026. [Online]. Available: https://www.legislation.gov.au/C2004A03712/latest/text. [Accessed: Jul. 5, 2026].

[14] Australian Government, *Security of Critical Infrastructure Act 2018*, No. 29, 2018, compilation no. 9, Jun. 4, 2026. [Online]. Available: https://www.legislation.gov.au/C2018A00029/latest/text. [Accessed: Jul. 5, 2026].

[15] Australian Government, *Cyber Security Act 2024*, No. 98, 2024, Nov. 29, 2024. [Online]. Available: https://www.legislation.gov.au/C2024A00098/asmade/text. [Accessed: Jul. 5, 2026].

[16] International Organization for Standardization, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. Geneva, Switzerland: ISO, 2022.

[17] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST Cybersecurity White Paper NIST CSWP 29, Feb. 26, 2024. doi: 10.6028/NIST.CSWP.29. [Online].Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. [Accessed: Jul. 3, 2026].

[18] S. Héroux and A. Fortin, "Board of directors' attributes and aspects of cybersecurity disclosure," *Journal of management and governance,* vol. 28, no. 2, pp. 359-404, 2024, doi: 10.1007/s10997-022-09660-7.

[19] M. Gale, I. Bongiovanni, and S. Slapnicar, "Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead," *Computers & Security,* vol. 121, Oct 2022, Art no. 102840, doi: 10.1016/j.cose.2022.102840.

[20] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture," *Decision Sciences*, vol. 43, no. 4, pp. 615–659, Aug. 2012, doi: 10.1111/j.1540-5915.2012.00361.x.

[21] S. Slapničar, M. Axelsen, and M. Eulerich, "Cyber risk management: An illusion of a risk-based approach," *Journal of Management Control*, Sep. 2025, doi: 10.1007/s00187-025-00401-z.

About the Author

Sanchay Joshi, CISSP, CISA, FIP, LL.B.
LinkedIn: www.linkedin.com/in/sanchay-joshi

Sanchay is a techno-legal cybersecurity and privacy risk advisor with over eight years of experience across Deloitte U.S. Offices in India, KPMG India, and PwC India. He is currently pursuing a Master of Cyber Security, specialising in Cyber Defence, at The University of Queensland, Australia.

His work sits at the intersection of cybersecurity, privacy, regulatory risk, and technology governance. He has advised Fortune 100 organisations across sectors including energy, retail, IT, telecom, pharma, and cloud services, with experience

spanning cybersecurity maturity assessments, privacy program design, ISO 27001 and SOC 2 readiness, third-party risk management, data governance, and regulatory compliance.

Sanchay is particularly interested in practical, business-aligned approaches to cyber risk governance, helping organisations communicate cybersecurity risk more effectively to senior leadership and boards.

Acknowledgement

The author gratefully acknowledges **Jihad Zein, Global Head of Governance, Risk and Assurance** at Toll Group in Australia, for his valuable practitioner insights and feedback during the development of this article.

Disclaimer

The views expressed in this article are solely those of the author and are based on his research and professional experience. They do not represent the views, positions, or policies of Deloitte, KPMG, PwC, Toll Group, The University of Queensland, or any other organisation with which the author has been associated.