Google Cloud

Perspectives on security from the board

From 2025 global poll

Executive summary

The board-level cybersecurity conversation is shifting. Insights from our recent director roundtables show that the debate has moved beyond the adequacy of controls to the necessity of operational resilience.

While boards clearly recognize the strategic importance of this role, our latest polling data serves as a snapshot in time that highlights a gap between intent and execution. Respondents acknowledge critical areas for improvement, specifically in resourcing, education, business continuity planning, and understanding the impact of AI/ML.

We recognize that governance requirements vary significantly across public, private, and specialized sectors. However, our discussions with boards point to an emerging set of universal principles that define modern leadership. The following themes—reinforced by these findings—highlight the current trajectory of effective oversight and the specific areas where boards are focusing their attention.

Alicja Cade
Senior Director, Office of the CISO

David Homovich
Advocacy Lead, Office of the CISO

The shift to financial & operational assurance

There is a clear move toward **Cyber Risk Quantification (CRQ)**, with boards demanding that technical risk be translated into business terms like **Value at Risk (VaR)** and **ROI**.

In practice: Requesting joint CISO-CFO reporting that utilizes **financial impact analysis** to ensure capital allocation is tied to measurable risk reduction.

Active participation as the new standard

Passive review of static reports is being replaced by **validated assurance**, characterized by direct board-level participation in incident simulations and tabletop exercises.

In practice: Integrating an annual **board-level tabletop simulation** focused on executive decision-making, such as materiality determinations and regulatory disclosure timelines.

Balancing defense with “future-proofing”

High-performing boards are looking beyond the immediate horizon to address paradigm shifts such as **Post-Quantum Cryptography (PQC)** and AI-driven threat landscapes.

In practice: Commissioning a **long-range readiness assessment** to secure multi-year roadmaps for quantum-resistant encryption and generative AI governance.

Bottom line: While implementation adapts to specific sectors, success is now measured by the **quantified resilience** of the business.

Table of contents

Executive summary of poll results 02

Poll demographics 04

Findings and trends 05

Methodology 12

Resources 13

Contributors 14

Demographics

North America	84%
Europe	17%
Middle East & Africa	9%
Asia-Pacific & Japan	8%
South America	8%

[N=105]

Respondent role

41%

Primarily Non-Executive Directors (NEDs) (41%), Chairpersons (38%), & Advisors (36%). [N=90]

Tenure & experience

81%

A highly experienced cohort, with 81% reporting 4+ years of service and 40% holding 10+ years of board tenure. [N=89]

Board memberships

50%

Respondents currently serve on 2-4 boards. 9% of respondents serve on 5+ boards. [N=109]

Committee oversight

60%

High concentration of subject matter experts, with 60% sitting on Technology/ Cybersecurity committees. [N=88]

Organization type

71%

Dominance of Private Companies (71%). [N=89]

Key sectors

53%

Top represented industries are Technology with 53%, Professional Services (26%), and Financial Services (24%). [N=88]

Revenue split

47%

Heavy representation of Growth-Stage organizations where 47% report under $50 million in revenue compared to 21% for Global Enterprises over $1 billion. [N=89]

Note on Multi-Select Data: For demographic questions regarding roles, industries, committees, and regions, respondents were permitted to select all that apply to reflect their diverse portfolios. Therefore, total percentages for these sections exceed 100%. Percentages are calculated based on the total number of unique respondents for each question [N varies by question]. **Note on Methodology:** Poll methodology details can be found on page 12.

The board's role in cyber risk is crucial for providing effective oversight and ensuring appropriate resource allocation.

Recent mandates, including SEC cybersecurity disclosure rules, emphasize the board's role in overseeing cyber risk management and governance reporting. This regulatory environment requires boards to demonstrate active oversight of the organization's security posture.

The poll results indicate a high level of agreement regarding strategic intent, alongside lower self-reported scores for technical and policy-specific expertise. 56% of respondents agree the board approves a cyber strategy aligned with the business's objectives and risk appetite. 44% of respondents agree the board possesses the necessary cybersecurity expertise for effective program oversight. 46% of respondents indicate the board has a clear understanding of the organization's cyber insurance policy.

While a majority of respondents report alignment between cyber strategy and business goals, fewer than half of the respondents report having the specific expertise or policy knowledge required to validate the execution of that strategy.

Aligned strategy

56% of boards have an approved, business-aligned cyber strategy [N=108]

Sufficient expertise

44% of boards have enough expertise to oversee cybersecurity [N=108]

46% of boards clearly understand their cyber insurance scope and exclusions [N=107]

Google Cloud insights

There are opportunities to advance governance through financial empowerment. Boards are championing models that empower the CISO to quantify cyber risk in financial terms (ROI, Value at Risk). This approach facilitates dedicated oversight of cyber insurance exclusions and financial exposure, ensuring the approved strategy drives resilience and business value.

Budgets are foundational to a security program's success

The board's oversight ensures financial investment translates directly into operational capability. The clarity of management's expectations for adequate staffing and budget is a direct result of strong board oversight.

The poll data indicates a narrow difference in perception regarding resource adequacy and readiness. 49% of respondents agreed the budget is adequate to address identified risks. Agreement slightly decreases to 48% when respondents were asked if the program possesses the necessary operational resources (staff, tools, training). The agreement level regarding both financial adequacy and operational resource readiness is below 50% for both metrics.

49% believe their cyber budget is sufficient for known risks [N=92]

48% of boards believe the cybersecurity team has resources needed to protect their assets [N=91]

Google Cloud insights: The board can champion a reporting model where the CISO, CIO, and CFO unify their vision, ensuring that investments translate directly into robust operational capability. This promotes strategic alignment and ensures that financial commitment maximizes resilience and value creation across the organization.

Communication is paramount to modern cyber governance

Security reporting at the board level increasingly prioritizes financial and operational business impact. This structure is intended to align cybersecurity dialogue with the organization's overarching business strategy.

The poll results provide the following aggregate levels of agreement regarding communication channels. 73% of respondents agree that effective communication channels exist between the board and the leadership team. 57% of respondents agree that open communication exists between the board and the cybersecurity team. 61% of respondents agree that the cybersecurity team communicates effectively with the board.

The poll identifies varying levels of agreement across three distinct communication categories. Reporting indicates the highest level of agreement regarding board-to-leadership channels, while reported agreement regarding open communication between the board and cybersecurity teams is lower by comparison in the aggregate data.

Leadership communication

73%

have robust board-to-leadership communication channels

[N=91]

Cybersecurity communication

57%

have transparent board-to-cyber team communication

[N=91]

Risks & incident communication

61%

see effective board-level reporting on cyber risks and incidents

[N=92]

Google Cloud insights

Strategic governance can advance through C-Suite partnership. The board can champion reporting models that empower the CISO to partner directly with the CFO to translate cyber risk into quantified financial terms (ROI, Value at Risk). This action facilitates dedicated oversight of financial exposure, moving the security dialogue from technical detail to strategic resilience.

The board holds the ultimate responsibility for setting the "tone at the top," which is foundational to a strong cybersecurity culture and organizational defense.

This commitment is critical because a strong culture transforms every employee into a defense layer, championing security as a shared responsibility throughout the enterprise.

The poll results indicate that 84% of boards believe the organization encourages employees to report suspected security incidents. Only 62% express confidence in the overall security culture or the consistency of employee training.

✓ **84%** promote an employee-led security reporting culture [N=85]

✓ **62%** express confidence in the overall security culture awareness [N=86]

✓ **62%** confirm ongoing cybersecurity training for staff [N=85]

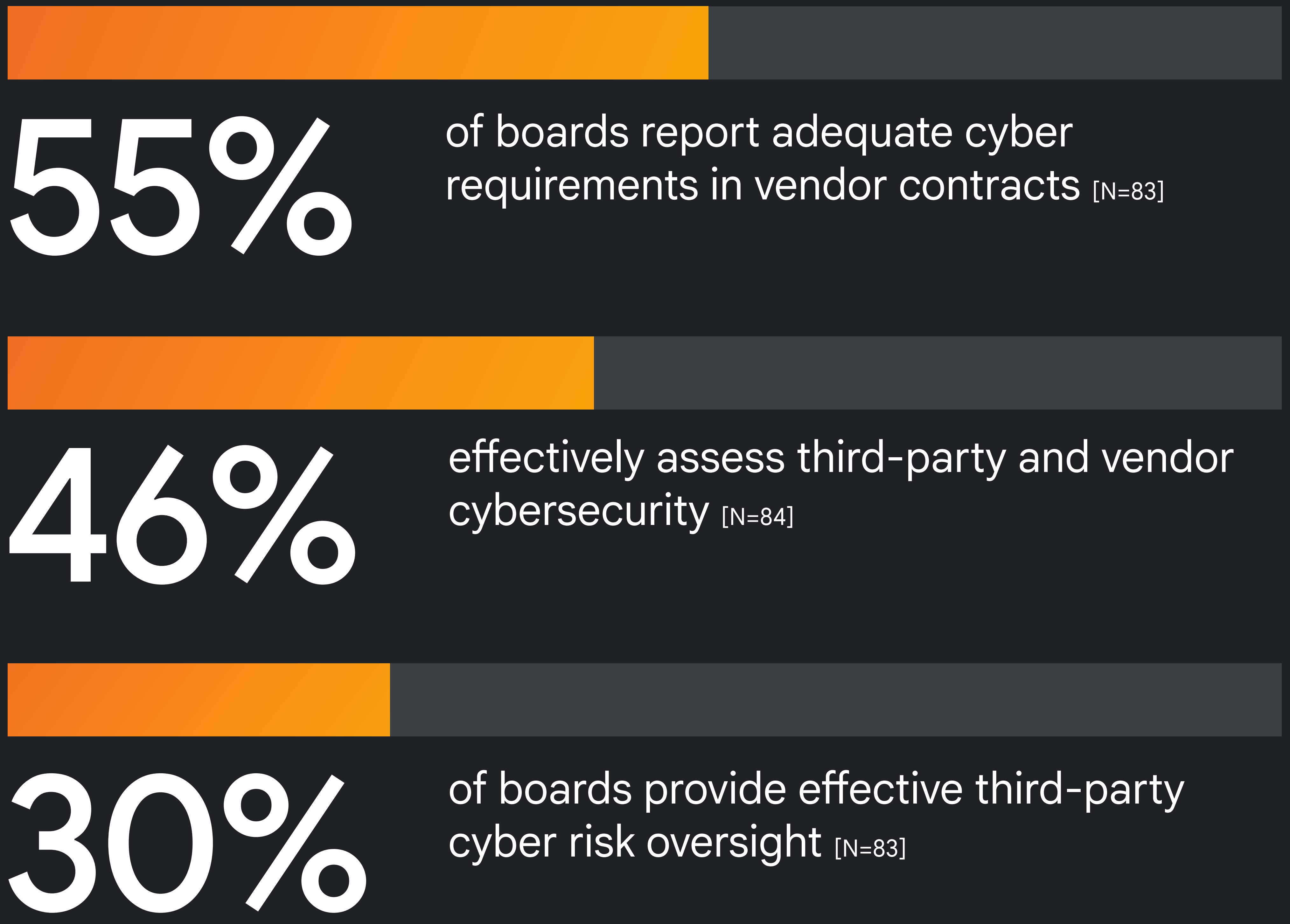
Google Cloud insights

The ultimate defense is a proactive culture, enabled when governance principles emphasize psychological safety and a no-blame culture. A strong culture transforms employees into a powerful, shared organizational defense layer, the board has the opportunity to facilitate systematic investment in security awareness.

Third-party risk management is key for resilience

Effective supply chain governance requires a strategic and continuous approach, moving beyond compliance documents like a SOC report. Risk management should focus on vendor criticality and aggregated risk, using continuous, risk-based monitoring to prioritize and assess the potential impact of vendor failure on core business operations.

Poll data indicates a gap between established third-party risk controls and board-level oversight. 55% of respondents believe appropriate contractual agreements are in place, and 46% agree that third-party assessments are effective. However, only 30% of respondents believe the board effectively oversees this risk. This data shows a 25-point difference between the reported existence of controls (contractual agreements) and confidence in the board's oversight function.



55% of boards report adequate cyber requirements in vendor contracts [N=83]

46% effectively assess third-party and vendor cybersecurity [N=84]

30% of boards provide effective third-party cyber risk oversight [N=83]

Google Cloud insights: Effective oversight requires the board to mandate a shift from static compliance checks (like SOC reports) to automated, real-time risk quantification. This necessitates using cloud-native tools to provide continuous monitoring of vendor posture, prioritize risk based on business criticality, and aggregate all third-party risk intelligence into a single view.

Effective incident response and resilience is paramount for the board, serving as the ultimate verification of a firm's security investment and fiduciary duty.

60%

maintain current and comprehensive incident response plans [N=93]

34%

of boards participate in tabletop simulations [N=92]

53%

regularly test and update their incident response plans [N=91]

56%

report timely board updates during significant cyber incidents [N=91]

The effectiveness of incident recovery and the mitigation of financial or reputational impact are critical components of organizational stability. This poll assessed the current state of incident response (IR) planning and the reported levels of board-level engagement.

The findings represent self-reported agreement levels across five distinct categories of cybersecurity preparedness. The data indicates that a majority of respondents (ranging from 53% to 60%) report the existence of formal documentation, testing protocols, and communication channels. Separately, the participation of the board in tabletop exercises was reported affirmatively by 34% of poll respondents.

Google Cloud insights: The board's governance role is to assure the organization's recovery capability, not execute the incident response plan. Effective oversight requires mandating and monitoring quantifiable metrics to measure the resilience of critical systems, rather than relying on subjective confidence in documentation.

Strategic governance demands a dual focus: defending today's critical data assets while proactively building resilience against tomorrow's disruptive shifts

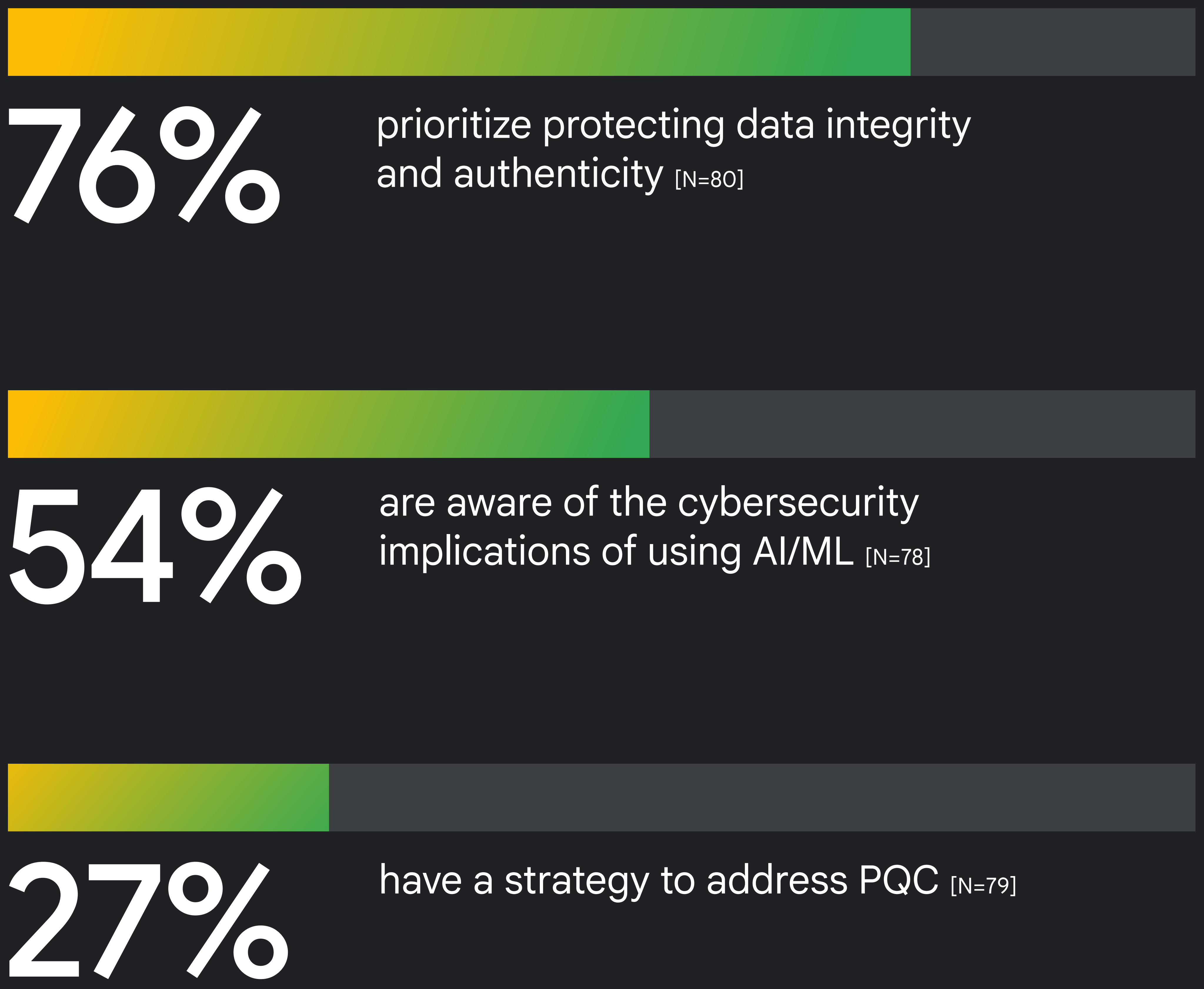
Effective board oversight increasingly involves the integration of cybersecurity as a strategic business enabler. This involves balancing current operational security requirements with the identification of emerging technological risks.

The poll results indicate a high level of agreement regarding the protection of existing data assets. 76% of respondents agree that their organizations prioritize protecting the integrity and authenticity of their data.

The poll data identifies specific levels of reported awareness and strategic planning concerning emerging technological developments. Specifically, 54% of respondents agree that their organization is aware of the cybersecurity implications associated with the use of AI/ML technologies. Furthermore, 27% of respondents agree that a strategy is in place to address issues related to post-quantum cryptography (PQC).

Google Cloud insights

Boards have a clear opportunity to translate their strong mandate for immediate data integrity (76%) into future strategic resilience. By governing the creation of a clear, future-proof roadmap, the C-suite can proactively manage emerging risks like AI and ensure long-term readiness against paradigm shifts.



Methodology

This report is based on the results of an anonymous online poll of 100+ Board Directors and strategic advisors, conducted by Google Cloud’s Office of the CISO (OCISO) between August and November 2025.

This report provides a fresh look at the current state of board-level cybersecurity governance, assessing how leadership teams are navigating the gap between strategic oversight and operational readiness.

Unless otherwise noted, all statistics in this report are derived directly from the poll and reflect a diverse cross-section of industries and regions. Assessment questions used a 5-point Likert scale ranging from ”Strongly Disagree” (1) to ”Strongly Agree” (5).

The percentages highlighted in this report represent the aggregate of positive sentiment (”Agree” and ”Strongly Agree”). Lower agreement levels do not strictly indicate disagreement; in many cases, it reflects a portion of respondents selecting ”Neutral,” indicating a lack of visibility or certainty rather than active opposition.

The data is presented at the aggregate level to ensure statistical significance of all reported results. Note that respondents were not required to answer every question. Figures throughout this report reflect the specific number of respondents for each query [N], as participation varied by question topic.

Board Resources

- ✓ Find curated board of directors resources on cybersecurity, risk governance, and secure transformation on our Board of Directors Insights Hub.

- ✓ Read the latest edition of our Perspectives on Security for the Board report series that equips the boardroom community with committed, consistent thought leadership and critical insights essential for effective strategic cybersecurity oversight.

- ✓ Empower your strategic oversight with the Board Edition: Cloud Threat Horizons Report, which provides actionable intelligence on cloud threats to digital trust, recovery resilience, and human security.

- ✓ Subscribe to The Cyber-Savvy Boardroom, the monthly podcast from Google Cloud's OCISO, for cybersecurity insights designed to fit seamlessly into busy schedules, featuring top board advisors and thought leaders delivering high-level strategic conversations.

Contributors

Alicja Cade
Senior Director,
Office of the CISO

Nick Godfrey
Senior Director,
Head of Office of the CISO

David Homovich
Advocacy Program Lead,
Office of the CISO

Lesly Merine-Lecocq
Security Advisor,
Office of the CISO

Thiébaut Meyer
Director,
Office of the CISO

Lia Wertheimer
Advocacy Program Manager,
Office of the CISO

Jennifer Burnside
Practice Leader,
Mandiant Crisis Communications

Kerry Helby
Strategic Audience Lead,
Global CISO & Board Advocacy