Kiteworks

TECHNOLOGY SECTOR BRIEF

Data Security and Compliance Risk: 2026 Forecast Report

The Benchmark-Setter's Blind Spots: Why Technology's AI Governance Leadership Masks Critical Vulnerabilities

Five Gap-Driven Predictions and Strategic Recommendations

Executive Summary

Technology organizations enter 2026 as the definitive leaders in AI governance and data security—setting the benchmarks that other industries aspire to reach. The sector leads or matches global highs on nearly every metric measured: bias audits, incident playbooks, drift monitoring, privacy-preserving techniques, and centralized data governance. When other sectors look for best practices, they look to Technology.

But leadership creates blind spots. The data reveals that Technology's governance model has specific structural gaps—in training environment isolation, data provenance tracking, and board-level cyber risk attention—that could propagate across industries as others adopt Technology's frameworks. When the benchmark-setter has gaps, those gaps become industry-wide vulnerabilities.

This sector analysis draws from a survey of 225 security, IT, compliance, and risk leaders globally, with 32 respondents representing technology organizations. The findings reveal a sector that dominates most metrics but shows surprising weaknesses in foundational areas. Five predictions emerge from these patterns—focused not on catching up, but on closing the gaps that could undermine Technology's leadership position and cascade across the AI ecosystem.

Five Predictions for Technology in 2026

1

Training environment gaps will create supply chain contamination risks

2

Weak provenance tracking will undermine otherwise strong governance frameworks

3

Board under-attention to cyber posture will create strategic blind spots

4

Technology's governance gaps will propagate across industries

5

Regulatory frameworks will be built around Technology's model—including its weaknesses

Technology vs. Global: Capability Profile

Where Technology Leads (Benchmark-Setting Performance)

Capability	Global	Technology	Advantage
Privacy-preserving techniques	33%	56%	**+23 points**
AI incident taxonomy & playbooks	27%	50%	**+23 points**
Compliance enforcement (training data)	34%	53%	**+19 points**
Bias/fairness audits	29%	47%	**+18 points**
Content authenticity/disclosure	30%	47%	**+17points**
AI impact assessments	37%	53%	**+16 points**
Drift monitoring	22%	38%	**+16 points**
Automatic revocation/DRM	25%	41%	**+16 points**
Third-party/vendor risk (board attention)	35%	50%	**+15 points**
Model explainability documentation	26%	41%	**+15 points**
Centralized AI data gateway	43%	56%	**+13 points**

Where Technology Trails or Matches Average

Capability	Global	Technology	Gap
Overall cyber risk posture (board)	54%	47%	**-7 points**
Skills gap/workforce (board)	14%	9%	**-5 points**
Isolated training environments	26%	22%	**-4 points**
Provenance & lineage	23%	19%	**-4 points**
Prompt/output logs	25%	25%	**0 points**

Five Gap-Driven Predictions for Technology in 2026

Prediction #1: Training Environment Gaps Will Create Supply Chain Contamination Risks

By 2026, technology organizations will experience AI model contamination incidents traceable to inadequately isolated training environments—undermining models that power products across industries.

Training Environmental Control	Global	Technology	Position
Isolated training environments	26%	22%	**-4 points (Below Average)**
Privacy-preserving techniques	33%	56%	**+23 points (Leader)**
Dataset access controls	35%	47%	**+12 points**
Pre-training validation	22%	28%	**+6 points**

The isolated training environment gap is striking given Technology's otherwise dominant position. At 22%, the sector actually trails the 26% global average—and sits well behind Financial Services (40%) and Energy/Utilities (36%). For an industry that builds the AI models powering applications across every sector, this represents a foundational vulnerability.

Technology has invested heavily in privacy-preserving techniques (56%) and access controls (47%), but these controls assume clean separation between training environments and production systems. Without adequate isolation, data leakage between environments, cross-contamination of training sets, and unauthorized access to model development become harder to prevent and detect.

Key Insight

Technology builds AI for the world but under-invests in the environmental controls that prevent contamination. The 4-point gap versus global averages—and 18-point gap versus Financial Services—represents a supply chain risk that extends far beyond the sector.

Opportunity

Treat training environment isolation as critical infrastructure. Implement air-gapped or strictly segmented environments for sensitive model development. Apply the same rigor to AI development environments that Technology demands for production systems. This is a relatively low-investment gap to close with outsized risk reduction.

Prediction #2: Weak Provenance Tracking Will Undermine Otherwise Strong Governance

By 2026, technology organizations will struggle to trace AI model issues to their source data despite strong detection capabilities, extending incident response timelines and regulatory exposure.

Data Lineage Capability	Global	Technology	Position
Provenance & lineage	23%	19%	**-4 points (Below Average)**
Immutable audit trails	25%	34%	**+9 points**
Drift monitoring	22%	38%	**+16 points (Leader)**
AI incident taxonomy & playbooks	27%	50%	**+23 points (Leader)**

Technology leads on drift monitoring (38%) and incident playbooks (50%)—meaning it will detect when models behave unexpectedly and have documented response procedures. But provenance and lineage tracking sits at just 19%, below the already-modest 23% global average.

This creates a diagnosis gap. Technology organizations will know something is wrong and have playbooks to respond, but will struggle to trace issues back through the data supply chain to identify root causes. As AI models increasingly incorporate third-party datasets, open-source components, and synthetic data, the inability to track data lineage becomes a critical weakness in otherwise mature governance frameworks.

The Gap

Technology has built excellent detection and response capabilities but can’t reliably trace problems to their source. The 4-point provenance gap creates blind spots in incident investigation and makes it harder to prevent recurrence.

Opportunity

Implement comprehensive data lineage tracking across the AI development life cycle. Document data sources, transformations, and model training relationships. Integrate provenance metadata with existing audit trail capabilities. Strong lineage tracking amplifies the value of Technology’s industry-leading detection investments.

Prediction #3: Board Under-Attention to Cyber Posture Will Create Strategic Blind Spots

By 2026, technology boards will be surprised by cyber incidents because executive attention has shifted to AI governance while foundational security posture monitoring has declined.

Board Attention Area	Global	Technology	Position
Overall cyber risk posture	54%	47%	**-7 points (Below Average)**
AI governance/responsible AI	46%	53%	**+7 points**
Third-party/vendor risk	35%	50%	**+15 points (Leader)**
Security metrics & KPIs	24%	31%	**+7 points**
Skills gap/workforce	14%	9%	**-5 points**

Technology boards have embraced AI governance (53%) and third-party risk (50%) as priorities—appropriate given the sector's role in the AI ecosystem. But overall cyber risk posture attention has dropped to 47%, seven points below the 54% global average and well behind Defense & Security (82%), Professional Services (67%), and Financial Services (65%).

This represents an attention reallocation that may have gone too far. AI governance is critical, but it doesn't replace foundational cybersecurity. Technology organizations remain high-value targets for nation-state actors, ransomware operators, and supply chain attackers. Board under-attention to overall cyber posture creates risk that AI governance investments alone won't address.

Key Insight

Technology boards have pivoted to AI governance—appropriately—but may have over-rotated away from foundational cyber posture. The 7-point gap versus global averages suggests strategic blind spots are forming.

Opportunity

Rebalance board attention to ensure AI governance investments complement rather than replace cyber posture monitoring. Integrate AI-specific risks into overall cyber risk frameworks rather than treating them as separate domains. Ensure foundational security doesn't become the neglected baseline while AI governance captures executive attention.

Prediction #4: Technology's Governance Gaps Will Propagate Across Industries

By 2026, the training environment and provenance gaps in Technology's governance model will appear in other sectors as they adopt Technology-defined best practices.

Capability	Technology	Professional Services	Financial Services
Isolated training environments	22%	27%	40%
Provenance & lineage	19%	27%	30%
AI incident playbooks	50%	40%	33%
Bias/fairness audits	47%	33%	30%

Technology's governance model emphasizes detection, response, and privacy-preserving techniques—areas where the sector dramatically outperforms. Other industries adopting Technology's frameworks will inherit these strengths. But they'll also inherit the structural de-emphasis on training environment isolation and provenance tracking.

This creates a systemic risk. Technology's blind spots become industry-wide blind spots as other sectors adopt Technology-defined frameworks, vendor solutions, and best practice guidance. The gaps identified here won't stay contained to the Technology sector—they'll propagate through the AI governance ecosystem.

The Gap

Technology defines the AI governance frameworks that other industries adopt. When Technology under-invests in specific capabilities, those gaps become embedded in industry-wide standards and vendor offerings.

Opportunity

Recognize Technology's role as the governance benchmark-setter and close gaps before they propagate. Engage in standards development to ensure training environment controls and provenance tracking receive appropriate emphasis. Technology's investments in these areas will improve governance across the entire AI ecosystem.

Prediction #5: Regulatory Frameworks Will Encode Technology's Model—Including Its Weaknesses

By 2026, AI regulations will reflect Technology's governance priorities, potentially under-weighting the foundational controls where Technology trails.

Regulatory Readiness Area	Global	Technology	Position
AI impact assessments	37%	53%	+16 points (Leader)
Transparency/disclosure	40%	44%	+4 points
Bias/fairness audits	29%	47%	+18 points (Leader)
Model explainability	26%	41%	+15 points (Leader)
Compliance enforcement	34%	53%	+19 points (Leader)

Technology's leadership on impact assessments (53%), bias audits (47%), and explainability (41%) positions the sector to influence emerging AI regulations. Regulators developing AI governance frameworks will look to Technology's practices as evidence of what's achievable and appropriate.

This influence cuts both ways. Technology's emphasis on bias audits, explainability, and impact assessments will likely appear prominently in regulatory frameworks. But the sector's relative de-emphasis on training environment controls and provenance tracking may result in regulations that under-weight these foundational capabilities—creating compliance frameworks that miss critical risk areas.

Key Insight

Technology will shape AI regulation through its demonstrated practices. The sector's governance priorities will become regulatory priorities—and its gaps may become regulatory blind spots.

Opportunity

Proactively advocate for comprehensive regulatory frameworks that include training environment controls and provenance tracking alongside bias audits and impact assessments. Technology has the credibility and expertise to shape regulations—use that influence to ensure frameworks address the full risk landscape, not just current investment priorities.

Strategic Recommendations for Technology Organizations

The data points to five priority investments for technology organizations preparing for 2026. These aren't catch-up measures—they're targeted gap-closers designed to complete an otherwise industry-leading governance posture and prevent gaps from propagating across the AI ecosystem.

1. Prioritize Training Environment Isolation as Critical Infrastructure

Close the 4-point gap on isolated training environments by implementing strict segmentation between development, training, and production systems. For sensitive AI development, consider air-gapped environments. Apply the same infrastructure rigor to AI development that Technology demands for production deployments. This is a low-cost, high-impact gap to close.

2. Implement Comprehensive Data Provenance and Lineage Tracking

Address the 4-point provenance gap by documenting data sources, transformations, and model training relationships across the AI life cycle. Integrate lineage metadata with existing audit trail capabilities. Strong provenance tracking amplifies the value of Technology's industry-leading detection and response investments by enabling faster root cause analysis.

3. Rebalance Board Attention Between AI Governance and Cyber Posture

Close the 7-point cyber posture attention gap by integrating AI risks into overall cyber risk frameworks rather than treating them as separate domains. Ensure board reporting covers foundational security posture alongside AI governance investments. AI governance is critical—but it doesn't replace the need for comprehensive cyber risk visibility.

4. Lead on Closing Gaps Before They Propagate

Recognize Technology's role as the governance benchmark-setter and prioritize gap closure to prevent weaknesses from propagating across industries. Other sectors adopt Technology's frameworks, vendor solutions, and best practices—make sure those frameworks are complete. Investments in training environment controls and provenance tracking will improve governance across the entire AI ecosystem.

5. Shape Regulatory Frameworks Proactively

Engage in AI regulatory development to ensure frameworks address the full risk landscape. Advocate for requirements covering training environment controls and data provenance alongside bias audits and impact assessments. Technology has the credibility and expertise to influence regulation—use that influence to create comprehensive frameworks, not frameworks that encode current investment patterns.

From Policy to Practice

Technology enters 2026 as the clear AI governance leader—setting benchmarks that other industries aspire to reach. The sector's investments in bias audits, incident playbooks, privacy-preserving techniques, and centralized governance represent the state of the art. When regulators, vendors, and other industries look for AI governance best practices, they look to Technology.

That leadership position creates responsibility. Technology's governance model will propagate across industries and influence regulatory frameworks. The gaps identified in this analysis—training environment isolation, provenance tracking, and board-level cyber posture attention—won't stay contained to the Technology sector. They'll become embedded in the frameworks, products, and standards that shape AI governance globally.

The task isn't catching up. It's completing the picture before Technology's model becomes everyone's model—including its blind spots. Organizations that close these gaps will solidify their leadership position and improve AI governance across the ecosystem. Those that assume current investments are sufficient will find their gaps amplified as they propagate through the industries and regulations that follow Technology's lead.

Technology built the AI governance standard. Now it's time to make sure that standard is complete.

Research based on survey of 225 security, IT, and risk leaders across 10 industries and 8 regions. 32 respondents represent technology organizations. 97% represent organizations with 1,000+ employees. Survey fielded Q4 2025.

Kiteworks
2026
Data Security and Compliance Risk Forecast Report
AI Adoption Is Accelerating. Governance Is Stalling. The Reckoning Is Coming.
REPORT
Kiteworks 2025. All Rights Reserved.

Kiteworks

www.kiteworks.com

January 2026