Kiteworks

MANUFACTURING SECTOR BRIEF

Data Security and Compliance Risk: 2026 Forecast Report

Production-Floor Strength, Adversarial Weakness: Why Manufacturing's Operational AI Governance Leaves Critical Security Gaps

Five Gap-Driven Predictions and Strategic Recommendations

Executive Summary

Manufacturing organizations enter 2026 with a distinctive AI governance profile—leading the world on human oversight while trailing dramatically on adversarial testing. The sector's operational DNA shows clearly in the data: exceptional performance on production-critical controls like human oversight (63%, highest globally) and gateway monitoring (56%), but significant gaps in the proactive security testing and compliance documentation that protect against sophisticated threats.

The gap isn't in commitment—it's in threat model. Manufacturing has built AI governance around operational reliability and safety, reflecting decades of experience with production systems where human oversight and real-time monitoring prevent failures. But AI systems face adversarial threats that traditional manufacturing controls weren't designed to address. Red-teaming at 7% (less than half the global average) signals a sector that hasn't yet adapted its governance model to the AI threat landscape.

This sector analysis draws from a survey of 225 security, IT, compliance, and risk leaders globally, with 27 respondents representing manufacturing organizations. The findings reveal a sector with genuine strengths—and specific vulnerabilities that adversaries will target. Five predictions emerge from these patterns—focused on closing the gaps between Manufacturing's operational excellence and the security capabilities the AI era demands.

Five Predictions for Manufacturing in 2026

1. Adversarial AI attacks will exploit the sector's red-teaming gap
2. Compliance documentation gaps will create regulatory exposure as AI oversight expands
3. Strong monitoring will detect incidents that weak audit trails can't investigate
4. OT/AI convergence will outpace governance frameworks designed for IT systems
5. Supply chain AI risks will be under-governed despite strong operational controls

Manufacturing vs. Global: Capability Profile

Where Manufacturing Leads

Capability	Global	Manufacturing	Advantage
Human oversight for high-stakes	46%	63%	**+17 points (Highest Globally)**
AI data gateway monitoring	37%	56%	**+19 points (Tied for Highest)**
AI impact assessments	37%	52%	**+15 points**
Encryption (training data)	39%	48%	**+9 points**
AI incident taxonomy & playbooks	27%	37%	**+10 points**
Automatic revocation/DRM	25%	33%	**+8 points**
Provenance & lineage	23%	33%	**+10 points**

Where Manufacturing Trails

Capability	Global	Manufacturing	Gap
Red-teaming cadence	18%	7%	**-11 points**
PIAs/DPIAs	25%	15%	**-10 points**
Content authenticity/disclosure	30%	22%	**-8 points**
Compliance enforcement (training data)	34%	26%	**-8 points**
Immutable audit trails	25%	19%	**-6 points**
Third-party/vendor risk (board)	35%	30%	**-5 points**
Data sovereignty (board)	13%	7%	**-6 points**

Five Gap-Driven Predictions for Manufacturing in 2026

Prediction #1: Adversarial AI Attacks Will Exploit the Sector's Red-Teaming Gap

By 2026, manufacturing organizations will experience AI system compromises that proactive adversarial testing would have prevented—attacks targeting the blind spots that 93% of the sector has never tested.

Adversarial Testing Capability	Global	Manufacturing	Gap
Red-teaming cadence	18%	7%	**-11 points**
Bias testing	26%	22%	**-4 points**
AI incident taxonomy & playbooks	27%	37%	**+10 points**
Drift monitoring	22%	22%	**0 points**

The red-teaming gap is Manufacturing's most significant vulnerability. At just 7%, the sector trails the global average by 11 points and sits far behind Defense & Security (55%), Technology (34%), and Financial Services (30%). For an industry increasingly deploying AI in safety-critical production environments, quality control, and supply chain optimization, this represents a fundamental security gap.

Manufacturing has built strong reactive capabilities—incident playbooks at 37% exceed global averages. But reactive capabilities only help after attacks succeed. Red-teaming identifies vulnerabilities before adversaries exploit them: prompt injection attacks, model poisoning, adversarial inputs that cause misclassification, and data extraction techniques. With 93% of manufacturing organizations never conducting AI red-team exercises, these attack vectors remain untested.

Key Insight

Manufacturing's operational excellence doesn't translate to adversarial readiness. The sector knows how to monitor and respond to failures—but hasn't invested in proactively identifying the attack paths adversaries will use.

Opportunity

Establish AI red-teaming programs that test for adversarial inputs, prompt injection, model poisoning, and data extraction. Leverage existing safety and quality testing cultures to build adversarial testing capabilities. Manufacturing understands the value of stress-testing production systems—apply the same discipline to AI systems.

Prediction #2: Compliance Documentation Gaps Will Create Regulatory Exposure

By 2026, manufacturing organizations will face regulatory findings and audit failures due to inadequate privacy impact assessments and compliance documentation—despite strong operational controls.

Compliance Documentation	Global	Manufacturing	Gap
PIAs/DPIAs	25%	15%	**-10 points**
Compliance enforcement (training data)	34%	26%	**-8 points**
Immutable audit trails	25%	19%	**-6 points**
Transparency/disclosure	40%	44%	**+4 points**
AI impact assessments	37%	52%	**+15 points**

Manufacturing shows a paradox: strong on AI impact assessments (52%) but weak on privacy impact assessments (15%). This suggests the sector has prioritized operational and safety assessments while under-investing in privacy-specific documentation. As AI regulations expand to cover manufacturing contexts—worker monitoring, quality control systems, supply chain optimization—this documentation gap becomes a compliance liability.

The pattern extends to audit trails (19% vs. 25% global) and compliance enforcement (26% vs. 34%). Manufacturing can demonstrate what its AI systems do operationally, but may struggle to prove compliance with privacy, data protection, and emerging AI-specific regulations that require documented assessments and immutable evidence.

The Gap

Manufacturing has built AI governance for operational purposes but hasn't extended documentation practices to meet regulatory requirements. The 10-point PIA gap and 6-point audit trail gap represent compliance exposure as AI regulations expand into manufacturing contexts.

Opportunity

Extend existing AI impact assessment processes to include privacy-specific requirements. Implement immutable audit trails that satisfy both operational and regulatory needs. Treat compliance documentation as an extension of quality management systems that manufacturing already operates effectively.

Prediction #3: Strong Monitoring Will Detect Incidents That Weak Audit Trails Can't Investigate

By 2026, manufacturing organizations will identify AI anomalies quickly but struggle to investigate root causes due to incomplete audit trail and logging capabilities.

Detection vs. Investigation Capability	Global	Manufacturing	Position
AI data gateway monitoring	37%	56%	**+19 points (Leader)**
Data governance audit trails	40%	44%	**+4 points**
Immutable audit trails	25%	19%	**-6 points**
Prompt/output logs	25%	26%	**+1 point**
Provenance & lineage	23%	33%	**+10 points**

Manufacturing excels at real-time monitoring—AI data gateway monitoring at 56% matches Financial Services for the global lead. The sector will detect when AI systems behave unexpectedly. But immutable audit trails at 19% (six points below average) create an investigation gap: detecting anomalies is one thing; proving what happened, when, and why is another.

This matters for both security incidents and regulatory inquiries. When an AI system causes a production issue, quality escape, or safety incident, manufacturing organizations will know something went wrong. But incomplete audit trails make it harder to reconstruct the sequence of events, identify root causes, and demonstrate to regulators that appropriate controls were in place.

Key Insight

Manufacturing has invested in detection but under-invested in the forensic capabilities that make detection actionable. Strong monitoring combined with weak audit trails means knowing something is wrong without being able to prove what happened.

Opportunity

Implement immutable, tamper-evident audit trails for AI systems that match the rigor of production quality records. Integrate AI audit logging with existing manufacturing execution systems. Ensure audit capabilities support both operational investigation and regulatory evidence requirements.

Prediction #4: OT/AI Convergence Will Outpace Governance Frameworks

By 2026, manufacturing organizations will deploy AI in operational technology environments faster than governance frameworks can adapt—creating security gaps at the IT/OT boundary.

OT-Related Governance	Global	Manufacturing	Position
OT/IoT security (board attention)	15%	22%	**+7 points**
Human oversight for high-stakes	46%	63%	**+17 points (Leader)**
Isolated training environments	26%	33%	**+7 points**
AI data gateway	35%	41%	**+6 points**

Manufacturing shows elevated board attention to OT/IoT security (22% vs. 15% global)—appropriate given the sector's operational technology footprint. Human oversight leadership (63%) reflects Manufacturing's safety culture. But these metrics measure awareness and traditional controls, not AI-specific OT governance.

As AI systems increasingly interface with production equipment, quality inspection systems, predictive maintenance platforms, and supply chain automation, they create new attack surfaces at the IT/OT boundary. Traditional OT security focused on network segmentation and access control; AI-enabled OT requires governance frameworks that address model integrity, training data security, and adversarial robustness in environments where failures have physical consequences.

The Gap

Manufacturing has strong OT security awareness but hasn't yet developed AI-specific OT governance. The sector's AI governance frameworks were built for IT contexts and may not adequately address the unique risks of AI systems that interface with physical production environments.

Opportunity

Develop AI governance frameworks specifically for OT deployment contexts. Address model integrity, training data security, and adversarial robustness for AI systems that interface with production equipment. Extend safety-critical system governance practices to cover AI-specific failure modes.

Prediction #5: Supply Chain AI Risks Will Be Under-Governed Despite Strong Operational Controls

By 2026, manufacturing organizations will experience supply chain disruptions caused by third-party AI failures that operational controls weren't designed to prevent.

Supply Chain AI Governance	Global	Manufacturing	Position
Third-party/partner AI policy & attestations	33%	37%	**+4 points**
Third-party/vendor risk (board attention)	35%	30%	**-5 points**
Software supply chain security (board)	8%	11%	**+3 points**
Data sovereignty (board attention)	13%	7%	**-6 points**

Manufacturing shows mixed performance on supply chain AI governance. Third-party AI policies (37%) slightly exceed global averages, but board attention to third-party risk (30%) and data sovereignty (7%) trails. This suggests operational teams have implemented vendor controls, but executive focus hasn't elevated supply chain AI risk to strategic priority.

Manufacturing supply chains increasingly depend on AI for demand forecasting, logistics optimization, quality prediction, and supplier risk assessment—often provided by third-party vendors. When these AI systems fail, produce biased outputs, or are compromised, the impact cascades through production schedules, inventory management, and customer commitments. The 5-point board attention gap on third-party risk suggests this exposure isn't receiving appropriate strategic visibility.

Key Insight

Manufacturing's supply chain complexity creates significant AI dependency on third-party systems. Board under-attention to third-party risk (30% vs. 35% global) and data sovereignty (7% vs. 13%) suggests strategic blind spots in supply chain AI governance.

Opportunity

Elevate supply chain AI risk to board-level visibility. Extend existing supplier quality management frameworks to cover AI system governance. Require AI-specific attestations from vendors providing demand forecasting, logistics optimization, and other AI-enabled supply chain services.

Strategic Recommendations for Manufacturing Organizations

The data points to five priority investments for manufacturing organizations preparing for 2026. These aren't foundational capabilities—they're targeted interventions designed to close specific gaps in an otherwise strong operational governance posture.

1. Establish AI Red-Teaming Programs Immediately

Close the 11-point red-teaming gap by building adversarial testing capabilities for AI systems. Test for prompt injection, adversarial inputs, model poisoning, and data extraction. Leverage existing safety and quality testing cultures—Manufacturing understands stress-testing production systems; apply the same discipline to AI. Consider third-party red-team services to accelerate capability development.

2. Extend Compliance Documentation to Meet Regulatory Requirements

Address the 10-point PIA gap by incorporating privacy impact assessments into existing AI governance processes. Implement immutable audit trails that satisfy both operational investigation and regulatory evidence requirements. Treat compliance documentation as an extension of quality management systems—Manufacturing already excels at documented processes.

3. Build Forensic Capabilities That Match Detection Investments

Complement industry-leading monitoring (56%) with audit trail capabilities that support incident investigation. Implement tamper-evident logging that reconstructs the sequence of events when AI systems fail. Ensure audit capabilities support regulatory inquiries, not just operational troubleshooting. Strong detection without strong forensics limits accountability.

4. Develop AI-Specific Governance for OT Environments

Create governance frameworks that address AI deployment in operational technology contexts. Cover model integrity, training data security, and adversarial robustness for AI systems interfacing with production equipment. Extend safety-critical system governance to address AI-specific failure modes. Don't assume IT-focused AI governance translates directly to OT environments.

5. Elevate Supply Chain AI Risk to Strategic Priority

Close the 5-point board attention gap on third-party risk by integrating supply chain AI governance into executive reporting. Extend supplier quality management to cover AI system governance, training data practices, and incident notification. Manufacturing supply chains depend on third-party AI—ensure that dependency receives appropriate strategic visibility.

From Policy to Practice

Manufacturing enters 2026 with genuine strengths—world-leading human oversight, exceptional gateway monitoring, and strong AI impact assessment practices. The sector's operational DNA shows clearly: Decades of production experience have built governance reflexes around monitoring, oversight, and real-time response that translate effectively to AI systems.

But AI systems face threats that production systems don't. Adversarial attacks, model poisoning, prompt injection, and data extraction require proactive security testing that 93% of manufacturing organizations haven't implemented. Compliance documentation gaps create regulatory exposure as AI oversight expands into Manufacturing contexts. And supply chain AI dependencies introduce risks that operational controls weren't designed to address.

The task isn't building AI governance from scratch—Manufacturing has strong foundations. It's adapting those foundations to address the adversarial threat landscape, regulatory requirements, and supply chain complexities that AI systems introduce. Organizations that close these gaps will combine operational excellence with security resilience. Those that rely solely on operational controls will find their AI systems targeted by adversaries who exploit the testing gaps that 93% of the sector has left unaddressed.

Manufacturing built its reputation on quality, reliability, and safety. Extending that reputation to AI systems requires closing the gaps between operational governance and security governance. 2026 is the deadline to complete that work.

Research based on survey of 225 security, IT, and risk leaders across 10 industries and 8 regions. 27 respondents represent manufacturing organizations. 97% represent organizations with 1,000+ employees. Survey fielded Q4 2025.

For the complete report with detailed methodology, industry breakdowns, and regional analysis, download it now.

Download the Report

Kiteworks