Kiteworks

ENERGY & UTILITIES SECTOR BRIEF

Data Security and Compliance Risk: 2026 Forecast Report

Distributed Controls, Centralized Blind Spots: Why Energy's Point-Solution Approach Leaves Critical Infrastructure AI Exposed to Sophisticated Threats

Five Gap-Driven Predictions and Strategic Recommendations

Executive Summary

Energy and utilities organizations enter 2026 with a governance paradox that creates critical infrastructure risk. The sector has built strong point controls—leading on dataset access controls, isolated training environments, and privacy impact assessments—but trails dramatically on the centralized monitoring, adversarial testing, and incident response capabilities needed to defend AI systems against nation-state actors and sophisticated threat groups.

The gap isn't in control investment—it's in control architecture. Energy has approached AI governance the way it approaches traditional infrastructure: distributed controls at individual assets and systems. But AI threats don't respect asset boundaries. Adversaries targeting critical infrastructure AI will exploit the gaps between point controls—gaps that only centralized monitoring and proactive adversarial testing can identify.

This sector analysis draws from a survey of 225 security, IT, compliance, and risk leaders globally, with 22 respondents representing energy and utilities organizations. The findings reveal a sector that has invested in compliance-oriented controls while under-investing in the detection, testing, and response capabilities that critical infrastructure demands. Five predictions emerge from these patterns—each representing vulnerabilities that nation-state actors and sophisticated threat groups will target.

Five Predictions for Energy/Utilities in 2026

1. Nation-state actors will exploit red-teaming gaps to compromise critical infrastructure AI
2. Weak centralized monitoring will leave AI attacks undetected until physical impact occurs
3. Incident response gaps will extend AI compromise dwell time and damage
4. Board under-attention to AI governance will delay critical security investments
5. Encryption gaps will expose AI training data containing grid operations intelligence

Energy/Utilities vs. Global: Capability Profile

Where Energy/Utilities Leads (Point Controls)

Capability	Global	Energy/Utilities	Advantage
PIAs/DPIAs	25%	41%	**+16 points**
Dataset access controls	35%	50%	**+15 points**
Skills gap/workforce (board)	14%	27%	**+13 points**
Isolated training environments	26%	36%	**+10 points**
Regulatory compliance (board)	40%	50%	**+10 points**
Third-party AI policy & attestations	33%	41%	**+8 points**
Security metrics & KPIs (board)	24%	32%	**+8 points**
OT/IoT security (board)	15%	23%	**+8 points**
Compliance enforcement (training data)	34%	41%	**+7 points**

Where Energy/Utilities Trails (Centralized Capabilities & Adversarial Readiness)

Capability	Global	Energy/Utilities	Gap
AI data gateway	35%	18%	**-17 points**
AI red-teaming	24%	9%	**-15 points**
AI governance (board attention)	46%	32%	**-14 points**
AI data gateway monitoring	37%	23%	**-14 points**
AI incident taxonomy & playbooks	27%	14%	**-13 points**
Encryption (training data)	39%	27%	**-12 points**
Bias testing	26%	14%	**-12 points**
Data privacy (board attention)	43%	32%	**-11 points**
Model explainability documentation	26%	18%	**-8 points**
Pre-training validation	22%	14%	**-8 points**

Five Gap-Driven Predictions for Energy/Utilities in 2026

Prediction #1: Nation-State Actors Will Exploit Red-Teaming Gaps to Compromise Critical Infrastructure AI

By 2026, energy and utilities organizations will experience AI system compromises by sophisticated adversaries exploiting vulnerabilities that proactive testing would have identified—with potential impacts on grid stability, pipeline operations, and public safety.

Adversarial Testing Capability	Global	Energy/Utilities	Gap
AI red-teaming	24%	9%	**-15 points**
Bias testing	26%	14%	**-12 points**
Pre-training validation	22%	14%	**-8 points**
Red-teaming cadence	18%	9%	**-9 points**

The red-teaming gap is Energy's most dangerous vulnerability. At just 9%, the sector trails the global average by 15 points and sits far behind Defense & Security (55%), Technology (34%), and Financial Services (30%). For critical infrastructure increasingly dependent on AI for grid optimization, predictive maintenance, demand forecasting, and pipeline monitoring, this represents an invitation to sophisticated adversaries.

Nation-state actors targeting energy infrastructure invest significant resources in identifying attack paths. With 91% of energy organizations never conducting AI red-team exercises, these adversaries face untested attack surfaces. Prompt injection attacks on grid management AI, adversarial inputs to pipeline monitoring systems, model poisoning in predictive maintenance—these attack vectors remain unexplored in the vast majority of energy organizations.

Key Insight

Energy operates critical infrastructure that nation-state actors actively target—yet has the second-lowest red-teaming rate of any sector measured. The 9% adoption rate means adversaries face essentially undefended AI attack surfaces across the energy sector.

Opportunity

Establish AI red-teaming programs immediately, with particular focus on AI systems interfacing with operational technology. Engage specialized red-team services with critical infrastructure experience. Test for prompt injection, adversarial inputs, model poisoning, and data extraction across grid management, pipeline monitoring, and predictive maintenance systems. This is a national security priority, not just an organizational one.

Prediction #2: Weak Centralized Monitoring Will Leave AI Attacks Undetected Until Physical Impact Occurs

By 2026, energy organizations will discover AI system compromises only after adversaries have achieved physical impact—grid instability, equipment damage, or supply disruption—because distributed controls lack the centralized visibility to detect sophisticated attacks.

Centralized Monitoring Capability	Global	Energy/Utilities	Gap
AI data gateway	35%	18%	**-17 points**
AI data gateway monitoring	37%	23%	**-14 points**
Data governance audit trails	40%	41%	**+1 point**
Drift monitoring	22%	18%	**-4 points**

The AI data gateway gap reveals Energy's architectural vulnerability. At 18%, adoption trails the global average by 17 points—while dataset access controls lead at 50%. This pattern shows the sector has implemented controls at individual systems and datasets but hasn't built the centralized visibility layer that aggregates signals across the AI environment.

Sophisticated adversaries don't attack single systems in isolation—they move laterally, compromise multiple components, and mask their activity across distributed infrastructure. Energy's point-control approach may detect anomalies at individual assets, but without centralized gateway monitoring, organizations can't correlate signals across systems to identify coordinated attacks before they achieve physical impact.

The Gap

Energy has strong controls at individual assets but weak visibility across the AI environment. The 17-point AI data gateway gap and 14-point monitoring gap create blind spots where sophisticated adversaries can operate undetected.

Opportunity

Deploy centralized AI data gateways that aggregate signals across distributed AI systems. Implement monitoring that correlates activity across grid management, pipeline operations, and maintenance systems. Build visibility architectures that match the interconnected nature of critical infrastructure AI—point controls alone won't detect coordinated attacks.

Prediction #3: Incident Response Gaps Will Extend AI Compromise Dwell Time and Damage

By 2026, energy organizations will experience extended AI compromise dwell times—adversaries persisting in AI systems for months—due to inadequate incident taxonomies, playbooks, and response capabilities.

Incident Response Capability	Global	Energy/Utilities	Gap
AI incident taxonomy & playbooks	27%	14%	**-13 points**
Automatic revocation/DRM	25%	18%	**-7 points**
Immutable audit trails	25%	18%	**-7 points**
Prompt/output logs	25%	23%	**-2 points**

At 14% AI incident playbook adoption, Energy trails the global average by 13 points and sits well behind Technology (50%), Manufacturing (37%), and Financial Services (33%). When AI system compromises occur—and given the red-teaming gap, they will—86% of energy organizations will be building their response in real time.

The implications for critical infrastructure are severe. Extended dwell time in energy AI systems means adversaries can study grid operations, identify cascading failure points, position for coordinated attacks, and establish persistence for future exploitation. Without documented playbooks and practiced response procedures, every AI incident becomes an improvised crisis response rather than an executed plan.

Key Insight

Energy's incident response gaps compound its detection gaps. Weak monitoring means late detection; weak playbooks mean slow response. Combined, these gaps create the conditions for extended adversary dwell time in systems that control critical infrastructure.

Opportunity

Develop AI-specific incident response playbooks for critical infrastructure contexts. Document response procedures for model poisoning, adversarial manipulation, data exfiltration, and coordinated attacks on grid management systems. Conduct tabletop exercises with scenarios specific to energy AI threats. Implement automatic revocation capabilities for AI systems that show signs of compromise.

Prediction #4: Board Under-Attention to AI Governance Will Delay Critical Security Investments

By 2026, energy organizations will find that board-level AI governance attention gaps have delayed the security investments needed to protect critical infrastructure—creating exposure that executives didn't recognize until incidents occurred.

Board Attention Area	Global	Energy/Utilities	Position
AI governance/responsible AI	46%	32%	**-14 points**
Data privacy & consumer protection	43%	32%	**-11 points**
Overall cyber risk posture	54%	50%	**-4 points**
Regulatory compliance status	40%	50%	**+10 points**
OT/IoT security	15%	23%	**+8 points**
Skills gap/workforce	14%	27%	**+13 points**

Energy boards show appropriate attention to regulatory compliance (50%) and OT/IoT security (23%)—reflecting the sector's operational reality. But AI governance attention at 32% trails the global average by 14 points and sits far behind Financial Services (60%), Technology (53%), and Professional Services (80%).

This attention gap has direct consequences. Board attention drives resource allocation. With AI governance receiving 14 points less executive focus than global averages, the investments needed to close the sector's red-teaming, monitoring, and incident response gaps will face budget competition from priorities that have captured board attention. The result: Critical infrastructure AI remains under-protected while executives focus elsewhere.

The Gap

Energy boards are focused on traditional regulatory compliance and OT security but haven't elevated AI governance to commensurate attention. The 14-point AI governance gap predicts delayed investment in the capabilities this analysis identifies as urgent priorities.

Opportunity

Frame AI governance as a critical infrastructure protection priority—not a compliance exercise or technology initiative. Connect AI security investments to grid reliability, public safety, and national security outcomes that resonate with board priorities. Elevate AI governance to the same board attention tier as OT security and regulatory compliance.

Prediction #5: Encryption Gaps Will Expose AI Training Data Containing Grid Operations Intelligence

By 2026, energy organizations will experience training data breaches that expose grid operations patterns, demand forecasting models, and infrastructure vulnerability assessments—intelligence of significant value to nation-state adversaries.

Data Protection Capability	Global	Energy/Utilities	Gap
Encryption (training data)	39%	27%	**-12 points**
Data minimization & masking	41%	45%	**+4 points**
Privacy-preserving techniques	33%	27%	**-6 points**
Provenance & lineage	23%	18%	**-5 points**
Immutable audit trails	25%	18%	**-7 points**

Energy trails on encryption by 12 points—27% versus 39% globally. This gap is particularly concerning given what energy AI training datasets contain: historical grid load patterns, demand forecasting models, equipment failure signatures, and predictive maintenance data. For adversaries planning attacks on energy infrastructure, this training data represents intelligence on how the grid operates, where vulnerabilities exist, and how organizations respond to anomalies.

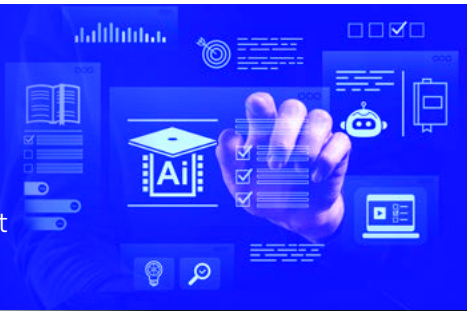
The sector shows decent performance on data minimization (45%), suggesting organizations are limiting unnecessary data collection. But unencrypted training data—even minimized—remains accessible to adversaries who breach perimeter defenses. Strong access controls (50%) help, but defense in-depth requires encryption as a backstop when access controls fail.

Key Insight

Energy AI training data contains operational intelligence about critical infrastructure—grid patterns, demand models, failure signatures. The 12-point encryption gap means this intelligence sits behind weaker protection than less sensitive data in other sectors.

Opportunity

Implement encryption for all AI training data at rest and in transit. Classify AI training datasets based on the operational intelligence they contain. Apply defense-in-depth principles: access controls prevent unauthorized access; encryption protects data when access controls fail. Treat AI training data as infrastructure intelligence, not just technical artifacts.



Strategic Recommendations for Energy/Utilities Organizations

The data points to five priority investments for energy and utilities organizations preparing for 2026. These aren't incremental improvements—they're critical infrastructure protection measures required to defend AI systems against sophisticated adversaries targeting the energy sector.

1. Establish AI Red-Teaming Programs as National Security Priority

Close the 15-point red-teaming gap by building adversarial testing capabilities specifically for critical infrastructure AI. Engage specialized red-team services with Energy sector experience. Test AI systems controlling grid operations, pipeline monitoring, and predictive maintenance for prompt injection, adversarial inputs, model poisoning, and coordinated attack scenarios. This is a national security imperative, not just an organizational security initiative.

2. Deploy Centralized AI Monitoring Across Distributed Infrastructure

Address the 17-point AI data gateway gap by implementing centralized visibility across distributed AI systems. Build monitoring architectures that correlate signals across grid management, pipeline operations, and maintenance AI. Point controls at individual assets aren't sufficient—sophisticated adversaries exploit gaps between distributed systems. Centralized monitoring is essential for detecting coordinated attacks.

3. Build Critical Infrastructure AI Incident Response Capabilities

Close the 13-point incident playbook gap by developing response procedures specific to energy AI threats. Document playbooks for model poisoning, adversarial manipulation, data exfiltration, and coordinated grid attacks. Conduct tabletop exercises with nation-state attack scenarios. Implement automatic revocation capabilities that can remove compromised AI systems from grid operations immediately.

4. Elevate AI Governance to Board-Level Critical Infrastructure Priority

Address the 14-point board attention gap by framing AI governance as critical infrastructure protection. Connect AI security investments to grid reliability, public safety, and national security outcomes. Position AI governance alongside OT security and regulatory compliance as a board-level priority requiring sustained executive attention and resource allocation.

5. Implement Defense-in-Depth Data Protection for AI Training Data

Close the 12-point encryption gap by encrypting all AI training data containing grid operations intelligence. Apply defense-in-depth principles: access controls prevent unauthorized access; encryption protects data when access controls fail. Classify AI training datasets based on the operational intelligence they contain about critical infrastructure patterns and vulnerabilities.

From Policy to Practice

Energy and Utilities enter 2026 having built AI governance the way it builds everything else—distributed controls at individual assets and systems, reflecting decades of operational experience with generation plants, transmission infrastructure, and distribution networks. The sector's strength in access controls, isolated environments, and privacy impact assessments demonstrates genuine investment in AI governance.

But AI threats don't respect asset boundaries. Nation-state actors targeting critical infrastructure invest in coordinated attacks that exploit gaps between point controls. The centralized monitoring, adversarial testing, and incident response capabilities that defend against sophisticated threats trail dramatically—creating vulnerabilities that adversaries will discover and exploit.

The stakes couldn't be higher. Energy AI systems increasingly control grid optimization, pipeline monitoring, demand forecasting, and predictive maintenance. Compromises don't just expose data—they threaten grid stability, pipeline safety, and public welfare. The 9% red-teaming rate means adversaries face essentially untested attack surfaces. The 14% incident playbook rate means compromises will trigger improvised responses rather than executed plans.

Energy organizations that close these gaps will demonstrate that critical infrastructure protection extends to the AI systems increasingly essential to grid operations. Those that rely on distributed point controls will discover—too late—that sophisticated adversaries operate in the gaps between assets, exploiting the architectural blind spots that only centralized monitoring and proactive testing can identify.

The sector's critical infrastructure mandate demands more than compliance. It demands the adversarial readiness that protects the systems society depends on. 2026 will determine whether Energy rises to meet that challenge or becomes a case study in what happens when critical infrastructure AI governance falls short.

Research based on survey of 225 security, IT, and risk leaders across 10 industries and 8 regions. 22 respondents represent energy and utilities 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