SECURING THE ENERGY AND UTILITIES SECTOR

A CALL TO ACTION IN CYBERSECURITY

NOVEMBER 2025

BY DR. KAVEH AFLAKI & DR. MASSOUD AMIN

InsightGlobal

The energy and utilities sector is at a turning point. Digital transformation is accelerating through the use of AI, IoT, and cloud-enabled systems, but adversaries are also exploiting these same technologies to probe, disrupt, and damage critical infrastructure.

High-profile attacks on pipelines and water systems in the U.S. [1][2][3], combined with lessons from Ukraine's grid outages and ransomware on European wind operators [10][11], illustrate that cyber threats are no longer theoretical—they are operational, persistent, and globally coordinated.

Investment in digital transformation is rising sharply, with cybersecurity spending projected to exceed $377 billion by 2028 [5], AI infrastructure surpassing $200 billion [6], and U.S. utilities committing more than $780 billion to modernization [7].

Yet investors, insurers, and regulators now demand proof that these expenditures deliver measurable resilience. Boards are increasingly judged by cyber resilience metrics:

- Mean time to detect, respond, and restore
- Blackstart readiness
- Compliance alignment

Insurers are tightening coverage [12][13], and ratings agencies are factoring cyber posture into credit risk [12].

Frameworks such as **NIST CSF 2.0, NERC CIP revisions,** and the **NIST AI Risk Management Framework** provide the tools to align governance with technical defenses [8][9]. International mandates, such as the EU NIS2 Directive and the EU AI Act, further reinforce the need for globally harmonized practices [11].

What is the path forward for utilities? They must do three things:

- Pair robust investment with demonstrable resilience
- Embed AI governance into operations
- Prepare for a regulatory and financial environment that increasingly treats cybersecurity as central to business viability.

Partners like Insight Global's professional services division, Evergreen, are positioned to translate standards into practice, close talent gaps, and ensure innovation is implemented securely.

Why Energy and Utilities Must Act Now

The energy and utilities sector, spanning electric power, oil and gas, and water services, is undergoing a profound digital transformation. Sensors, smart meters, and advanced analytics are modernizing infrastructure. Artificial intelligence (AI), cloud computing, and the Internet of Things (IoT) are driving operational efficiency and enhancing productivity.

These advances, however, come with escalating cyber risks. Disruption of a grid, pipeline, or water system can endanger national security, public health, and economic stability. Cybersecurity has become a strategic imperative requiring a holistic, evidence-based approach.

UNDERSTANDING THE THREAT LANDSCAPE

Critical infrastructure is increasingly vulnerable. In May 2021, a ransomware attack on Colonial Pipeline disrupted fuel deliveries across the U.S. East Coast, demonstrating nationwide consequences from a single incident [1].

Water systems remain under pressure:

- Iranian hackers compromised multiple U.S. water utilities in 2023
- In April 2024, Russian actors breached facilities in Texas and caused tanks to overflow
- America's largest water provider disclosed a 2024 cyberattack
- The FBI warns of Chinese probing of U.S. plants [2].

A November 2024 EPA Inspector General report found that 9% of more than 1,000 public drinking water systems had critical or high-risk cyber vulnerabilities, while over 70% failed to comply with federal risk assessment and response requirements [3].

In Ukraine, coordinated cyberattacks against the grid in 2015 and 2016 resulted in widespread outages, marking the first publicly confirmed cyber-induced power disruptions at a national scale [10]. In 2021–2022, European wind operators faced ransomware attacks that disrupted remote monitoring of thousands of turbines, highlighting how renewables and distributed assets are increasingly targeted [11].

These incidents show how adversaries exploit the convergence of IT, operational technology (OT), and IoT. They also expose systemic delays: interconnection studies for new clean energy projects still average roughly 40 months, leaving vital upgrades stranded [4].

INVESTMENT TRENDS AND MARKET SIGNALS

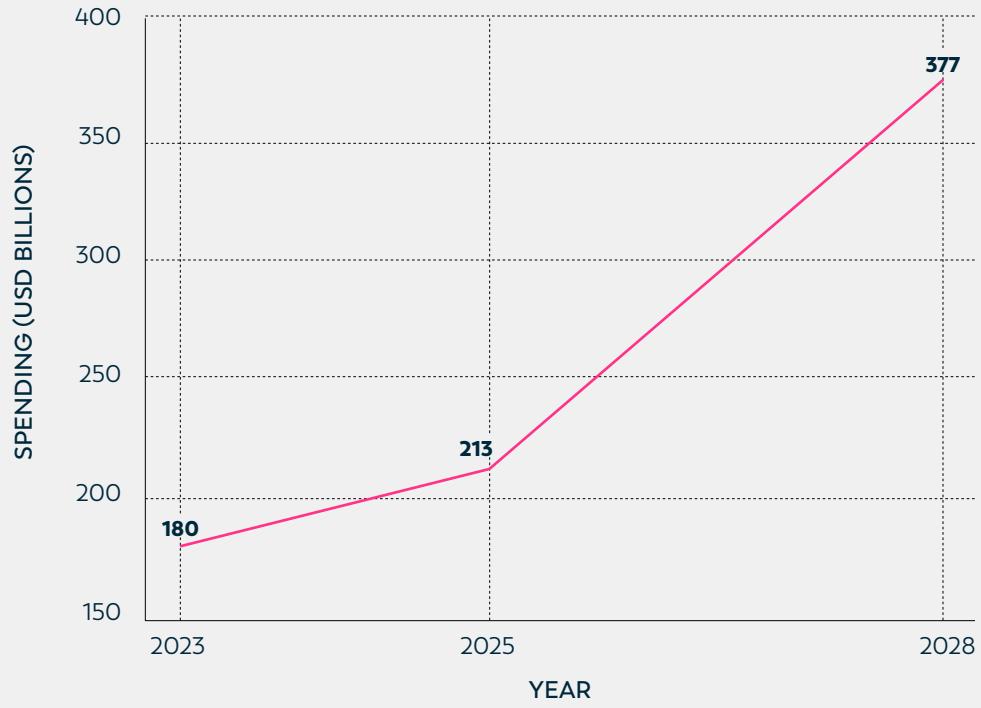
The threat environment has spurred massive investment. Global cybersecurity spending is projected to grow 12.2% year-over-year in 2025 and reach about $377 billion by 2028. Security software is the fastest-growing segment, and the United States and Western Europe will account for more than 70% of spending [5].

AI infrastructure spending rose 97% year-over-year in the first half of 2024 to $47.4 billion and is on track to exceed $200 billion by 2028. Accelerated servers already account for about 70% of AI server spending and are projected to surpass 75% by 2028 [6].

U.S. utility investment is also rising sharply: EUCI/S&P Global projects more than $780 billion in spending between 2025 and 2028—$202 B in 2025, $206 B in 2026, $211 B in 2027. Water-specific projects are expected to total $172 billion by 2028, focusing on transmission lines, distribution upgrades, battery storage, smart meters, and renewable integration [7].

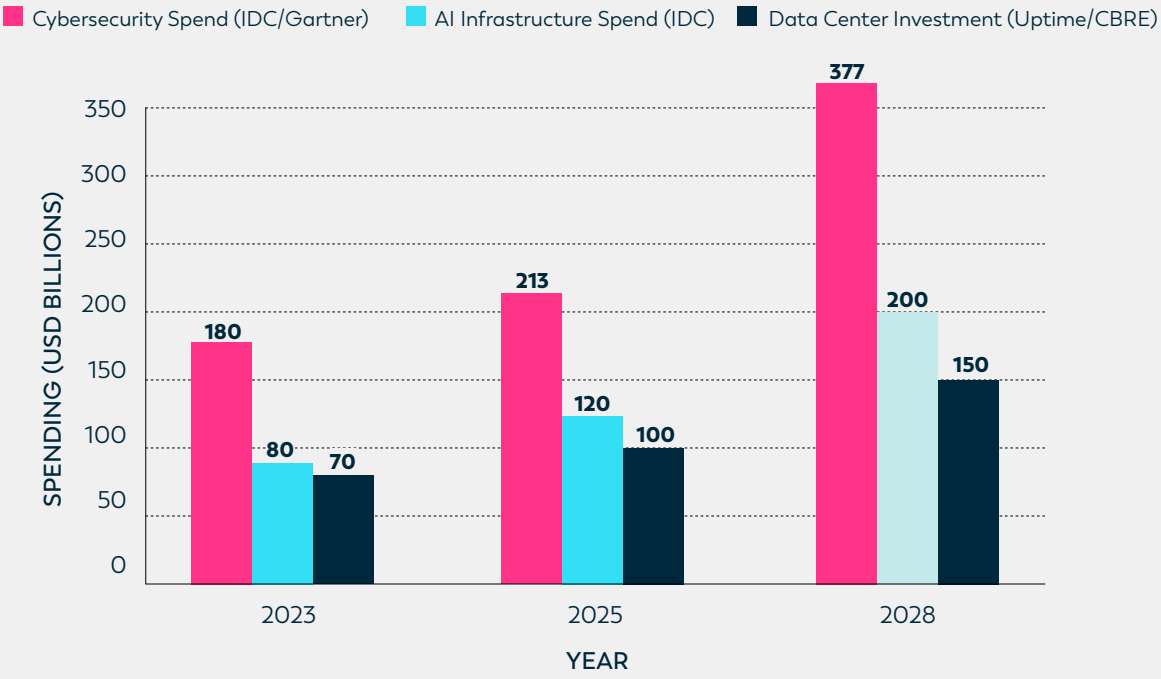
The graph (Figure 1) illustrates a strong upward trend in global security investments from 2023 to 2028.

Figure 1: *Global Security Spending (2023–2028)*



The bar graph (Figure 2) presents a compelling forecast of global technology investments from 2023 to 2028. It reveals a consistent upward trend across all three sectors, with cybersecurity spending leading the charge, rising from $180 billion in 2023 to a projected $377 billion by 2028.

Figure 2: *Technology Investments: Cybersecurity, AI, Data Centers (2023–2028)*



The graph (Figure 3) highlights a strong upward trend in technology investments across the utility sector from 2023 to 2028.

Figure 3: *U.S. Utility Sector Investment: Electricity, Oil & Gas, Water (2023–2028)*

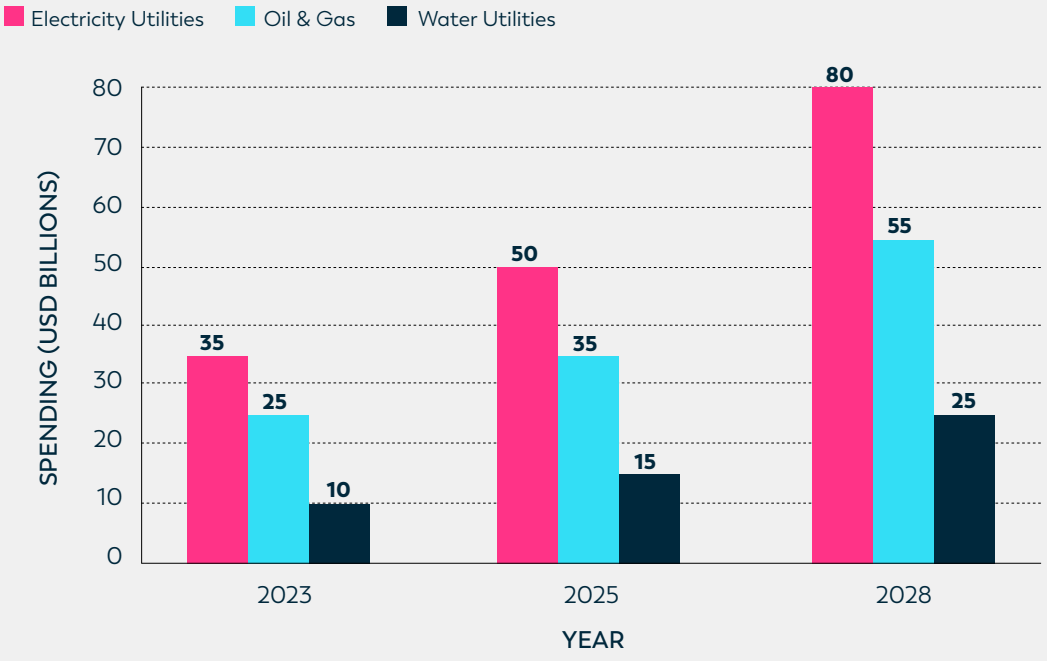


Table 1. *Key Investment Projections (USD B)*

Category	2023	2025 (est.)	2028 (proj.)	Notes
Cybersecurity (global)	~180	~213	~377	*Rapid CAGR driven by regulatory and threat pressure.*
AI infrastructure (global)	~80	>120	>200	*97% YoY growth in 1H24; accelerators dominate server spending.*
Data centers (global)	~70	–	~150	*Reflects surging AI-driven demand.*
U.S. utilities – Electricity	35	–	80	*Part of $780 B total utility investment 2025–2028.*
U.S. utilities – Oil & Gas	25	–	55	–
U.S. utilities – Water	10	–	25	*$172 B water projects by 2028.*

Note: A dash indicates that a specific intermediate figure was not provided in the source documents.

REGULATORY AND GOVERNANCE FOUNDATIONS

Regulators have adapted to the evolving threat. NIST Cybersecurity Framework 2.0 (February 2024) introduces a new "Govern" function, expands supply chain risk management, and provides quick start guides and reference catalogs to align with international standards [8].

As utilities experiment with AI for forecasting, maintenance, and interconnection planning, AI governance frameworks are also essential. NIST's AI Risk Management Framework (AI RMF 1.0) provides a lifecycle approach to mapping, measuring, and managing AI risk [8].

In addition to federal frameworks, sector-specific standards like NERC CIP are evolving to address new risks. NERC CIP 2025 revisions update four standards related to risk and security. We've explained these revisions below.

Certrec notes that lowered thresholds mean that 15–25% of distributed energy resources previously exempt now fall under medium- to high-impact compliance. The revisions mandate:

- Multi-factor authentication for remote access
- Zero-trust principles
- Centralized logging
- Modular architectures [9]

This table breaks down the key changes.

Table 2. *Key NERC CIP Revisions (Effective 2025)*

Standard	Focus	Key Change
CIP-003-9	Security management controls	Extends policy and training requirements to low-impact assets.
CIP-005-7	Electronic access control	Tightens access point monitoring and segmentation.
CIP-010-4	Configuration management	Clarifies baseline configurations and vulnerability assessments.
CIP-013-2	Supply chain risk management	Adds vendor risk oversight; reduces DER exemption thresholds.

International and AI Governance Context

The DOE's CESER office coordinates cybersecurity across the U.S. energy sector, guiding emergency preparedness and incident response. Abroad, the EU NIS2 Directive establishes a baseline for cyber requirements for essential entities, while the EU AI Act sets out a risk-based regulatory framework for AI. The UK NCSC issues sector-specific guidance. For AI, NIST's AI Risk Management Framework (AI RMF 1.0) offers a structure for mapping, measuring, and governing AI risks, complementing the CSF.

Strengthening Cyber Readiness Across Systems and Teams

As the energy and utilities sector modernizes, the challenge of cybersecurity extends far beyond technology alone. True resilience demands a coordinated approach—one that addresses not only digital systems, but also the people, processes, and partnerships that keep critical infrastructure running.

NAVIGATING AI AND AUTOMATION RISKS

Utilities employ AI/ML for demand forecasting, interconnection planning, vegetation management, and predictive maintenance. These tools can improve reliability—but they also open new attack vectors, like adversarial ML, poisoned training data, and compromised data pipelines. In addition, sensitive grid data processed in cloud environments can be exfiltrated or manipulated, posing a significant security risk.

PJM's partnership with Google demonstrates AI's potential to expedite interconnection studies; however, the average backlog remains approximately 40 months. Responsible AI deployment demands rigorous testing, data provenance, governance controls, and continuous monitoring.

SECURING OPERATIONAL TECHNOLOGY (OT)

OT systems—such as generators, pumps, compressors, and relays—often operate on decades-old protocols. Protecting them requires:

- **Network segmentation** to isolate OT and limit lateral movement.
- **Comprehensive inventories** and software bills of materials (SBOMs) to identify vulnerabilities.
- **Patch and configuration management** tailored to operational constraints.
- **Intrusion detection systems** tuned to industrial protocols.
- **Authenticated engineering workstations** and role-based access.
- **Tested backup and recovery plans** for programmable logic controllers (PLCs) and remote terminal units (RTUs).

IT/OT convergence necessitates unified security that safeguards physical processes without disrupting operations.

ADDRESSING WORKFORCE AND TALENT GAPS

Cybersecurity is a human problem as much as a technical one. The demand for OT security engineers, SOC analysts, and AI-literate data scientists far outstrips the supply. Energy firms face fierce competition, high turnover, and rising salary pressures. Addressing this gap requires:

- **Training and certification programs** to build internal capabilities.
- **Recruiting initiatives** to widen the talent pipeline.
- **Automation and orchestration** to reduce analyst workload.
- **Strategic staffing partnerships** for managed teams and build-operate-transfer models.

MANAGING SUPPLY CHAIN CYBER RISK

Complex supply chains create vulnerabilities. The SolarWinds breach demonstrated how a single compromise can impact thousands of customers. NIST CSF 2.0 and NERC CIP0132 emphasize:

- **Vendor risk assessments** and pre-award due diligence.
- **Contractual cybersecurity clauses** specifying MFA, logging, and vulnerability remediation windows.
- **Continuous monitoring** of supplier performance and software updates.
- **Secure development practices** and attestation for hardware and firmware.

Building Resilience Through Response and Metrics

INCIDENT RESPONSE READINESS

Preventive defenses are not enough; resilience hinges on rapid detection and recovery. Utilities must track the mean time to detect (MTTD), mean time to respond (MTTR), and mean time to restore (MTTR). For power systems, black start readiness under cyber-degraded conditions is critical. Robust plans include:

- Tabletop and livefire exercises incorporating cyberphysical failure modes.
- Pre-staged spares and segmentation for phased restoration.
- Conditional access procedures during emergencies.
- Validated backups and offline recovery options.
- Coordinated communication with regulators, customers, and the public.

MEASURING CYBER RESILIENCE

Utilities and regulators increasingly measure security not only by preventive controls but also by resilience outcomes. Common key performance indicators include:

Table 3. *Cyber Resilience Metrics for Utilities*

Metric	Definition	Benchmark Target
MTTD (Mean Time to Detect)	Average time to identify a cyber incident	< 24 hours
MTTR (Mean Time to Respond)	Average time to contain an active incident	< 72 hours
MTTR (Mean Time to Restore)	Average time to restore service after an outage	Sector-dependent (e.g., < 5 days for distribution utilities)
Blackstart Readiness	Ability to restore the grid without an external supply after an outage	Tested annually under cyber-degraded conditions
Compliance Readiness	% of assets aligned with NERC CIP & NIST CSF 2.0	> 95% alignment

Tracking and publishing these metrics enable boards, regulators, and investors to assess whether cyber investments are yielding improved resilience.

LINKING METRICS TO FINANCIAL DRIVERS

Cyber resilience metrics—such as mean time to detect, respond, and restore (MTTR), blackstart readiness, and incident response testing—have evolved beyond operational benchmarks. They now serve as critical financial and governance signals. Boards, regulators, and insurers increasingly require utilities to demonstrate measurable performance against these thresholds before granting favorable credit ratings, affordable insurance coverage, or access to capital [12][13].

Ratings agencies have begun factoring cyber preparedness into credit assessments, treating resilience as a material financial risk. At the same time, insurers are tightening coverage, introducing exclusions for nation-state attacks and requiring evidence of controls like multi-factor authentication, network segmentation, and tested response plans. Utilities that cannot show demonstrable progress face higher premiums, reduced coverage, and elevated cost of capital.

Cyber ratings now influence bond yields, investor confidence, and executive accountability. To maintain trust and financial viability, utilities must embed resilience into governance and prove that their cybersecurity investments translate into measurable outcomes.

Evergreen's Role and Approach

Insight Global's professional services division, **Evergreen**, offers end-to-end capabilities:

- **Compliance and Architecture** – Conduct gap assessments against NIST CSF 2.0 and NERC CIP, design zero-trust reference architectures for OT/IoT, and develop audit-ready documentation.
- **Operational Defense** – Build or augment SOCs for IT and OT, deploy managed detection and response tuned to industrial protocols, and integrate threat intelligence. Continuous monitoring is essential given the targeting of water utilities.
- **Secure AI Deployment** – Test AI models against adversarial inputs, validate training data and pipelines, enforce governance controls, and harden model operations. As AI infrastructure spending accelerates, ensuring trustworthiness and resilience is non-negotiable.
- **Talent and BOT** – Provide cleared professionals and build-operate-transfer teams to fill persistent skill gaps.

Looking Ahead: A Call to Action

Zero-trust architectures will become the default for access control. Quantum-safe cryptography is needed to protect long-lead time assets against future quantum attacks. Cyber-physical security will require integrated monitoring of digital and physical signals to detect anomalies. Regulatory harmonization across regions will simplify compliance. Meanwhile, investment remains robust, but regulators and investors will demand demonstrable resilience, not just spending.

Securing the energy and utilities sector is a multifaceted challenge. The industry is investing billions to modernize its infrastructure, expand AI capabilities, and defend against state-linked adversaries. Regulators are developing frameworks and lowering compliance thresholds, while urging stronger governance and supply chain oversight.

By combining robust regulation, resilient architecture, skilled personnel, and responsible innovation, utilities can safeguard essential services and foster public trust. Partners such as Evergreen translate regulations into architectures, threats into defenses, and innovation into resilience.

The energy transition cannot succeed without parallel commitment to cybersecurity.

REFERENCES

[1] CISA, The Attack on Colonial Pipeline, May 7, 2023.
[2] Industrial Cyber, FDD experts warn that EPA cyber grants are a “drop in the bucket” as attacks escalate, August 26, 2025.
[3] StateScoop, EPA: Critical cyber vulnerabilities in U.S. water utilities, Nov 18 2024.
[4] Reuters, Google Brings AI to Grid Teams, Slashing U.S. Connection Times, May 20, 2025.
[5] Moonshot News, AI threats driving cybersecurity spending, Mar 27 2025.
[6] IDC, Artificial Intelligence Infrastructure Spending to Surpass $200 B in Five Years, Feb 18 2025.
[7] EUCI/S&P Global: Utility project spend set to surge in the U.S. (2025–2028), January 21, 2025.
[8] NIST, Cybersecurity Framework 2.0, Feb 26 2024.
[9] Certrec, Navigating NERC CIP Compliance for Distributed Energy Resources, Aug 2025.
[10] SANS/ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016.
[11] ENISA, Threat Landscape for Energy Sector, 2022.
[12] Moody’s Investors Service, Cyber Risk Considerations in Credit Ratings, 2023.
[13] Marsh McLennan, Cyber Insurance Market Trends for Critical Infrastructure, 2024.

***Kaveh Aflaki**, Ph.D., M.B.A., is Industry Principal for Energy & Utilities at Insight Global and Evergreen, our professional services division. Connect with him on LinkedIn.*

***Dr. Massoud Amin** is Chairman & President at Energy Policy & Security Associates. He advises Insight Global on energy and utilities. Connect with him on LinkedIn.*