*IOSR Journal of Business and Management (IOSR-JBM)*
*e-ISSN:2278-487X, p-ISSN: 2319-7668. Volume 28, Issue 11. Ser. 1 (November. 2026), PP 33-39*
*www.iosrjournals.org*

# Cybersecurity Technologies in Energy Systems: Business Profitability, Socioenvironmental Resilience, and Macroeconomic Implications

José Genaro González Hernández[1,2], Andrés Esteban Masilo[3]
[1] *TecNM Campus Instituto Tecnológico de Ciudad Madero, México*
[2]*Universidad Tecnológica de Altamira, México*
[3]*Instituto de Estudios Superiores en Finanzas, México*

***Abstract :***
*Digital transformation has increased the economic value and cyber exposure of electricity, oil, gas, and renewable-energy infrastructure. This study develops an integrated business and macroeconomic framework to assess the financial justification for energy-sector cybersecurity, with international comparisons and a focused application to Mexico. The research combines a structured review of 2020–2026 institutional and industry literature, a technology–business taxonomy, a discounted cash-flow model for risk reduction, and scenario analysis of potential production losses arising from electricity disruption. Official Mexican national-accounts data establish a 2025 nominal GDP benchmark of MXN 35.923 trillion; global breach-cost evidence is employed solely as cross-sector context, not as an energy-sector loss estimate. A transparent illustrative investment model shows that cybersecurity returns depend on incident frequency, conditional severity, intervention effectiveness, operating costs, and discount rates. Forward-looking low, central, and high assumptions through 2035 are specified as scenarios rather than forecasts or measured effects. The analysis recognizes operational-technology segmentation, asset visibility, incident response, governance, and supply-chain assurance as economically relevant capabilities. Results show that credible investment appraisal requires avoided expected loss, business continuity, and social and environmental externalities to be evaluated separately. The proposed framework supports utilities, industrial energy consumers, investors, and regulators, while pointing out substantial shortcomings in public data on cyber-attributable outages and firm-level cybersecurity revenues.*

***Keywords:*** *Energy cybersecurity; operational technology; return on investment; electricity resilience; gross domestic product; Mexico; sustainable development; cyber risk.*

---

Date of Submission: 27-10-2026 Date of Acceptance: 06-11-2026

---

## I. INTRODUCTION

Energy networks serve as foundational inputs for manufacturing, logistics, health care, digital services, and household welfare. Electrification, remote connectivity, distributed energy resources, and industrial automation enhance efficiency but also increase the number of assets and interfaces vulnerable to malicious activity [1]-[3]. As a result, cybersecurity constitutes not only an information-technology expenditure but also an investment in operational continuity, business resilience, and public welfare.

Quantifying the business case for cybersecurity remains challenging. Firms rarely disclose total security budgets, outages often have multiple causes, and publicly reported data breaches do not necessarily reflect control-system compromises. The 2025 IBM cross-industry average breach cost of USD 4.44 million [4] demonstrates the economic significance of cyber risk but should not be interpreted as a representative loss for electricity providers. This study explicitly distinguishes between observed evidence and hypothetical scenario inputs.

This research investigates the conditions under which energy cybersecurity investment can enhance risk-adjusted profitability and reduce the economic exposure of electricity-dependent activities. The objectives are to (i) classify relevant technologies and business functions, (ii) develop an investment appraisal method, (iii) examine international institutional arrangements and corporate disclosures, (iv) apply a transparent exposure model to Mexico, and (v) explore conditional trajectories through 2035.

## II. THEORETICAL BACKGROUND

### 2.1 Cybersecurity and operational resilience in energy systems

Energy infrastructure comprises information technology (IT), operational technology (OT), supervisory control and data acquisition (SCADA), distributed control systems, protection relays, industrial communications, and connected renewable assets. In this context, OT security emphasizes physical safety, availability, integrity, recovery, and confidentiality [1], [5]. An effective security program incorporates asset inventories, network segmentation, identity management, secure remote access, continuous monitoring, backup and recovery, and supplier risk controls [6]-[9].

### 2.2 Economic rationale and governance

Cybersecurity contributes value by reducing expected losses and minimizing the variance of business outcomes. Financial benefits include avoided service interruptions, fewer equipment-damage incidents, reduced remediation expenses, lower legal exposure, and enhanced contractual assurance. However, security investments are not inherently profitable; the marginal risk reduction must surpass the total lifecycle cost. Governance frameworks such as NIST CSF 2.0 facilitate alignment of technology decisions with organizational objectives [6].

### 2.3 Social and environmental externalities

Energy interruptions can impact hospitals, water treatment facilities, communication systems, and vulnerable households. Physical compromise of industrial controls introduces safety and environmental risks, with the severity determined by plant-specific protections and operational conditions [1]. In contrast, cybersecurity operations require computing resources and electricity. Therefore, comprehensive assessments should consider benefits, direct resource costs, and potential externalities, rather than assuming all cybersecurity investments result in net environmental gains.

### 2.4 International institutions and Mexico

The IEA emphasizes shared responsibility across utilities, vendors, regulators, and governments [1]. European cybersecurity and energy policy increasingly address supply-chain and critical-infrastructure resilience [10]-[12]. The United States applies sector-specific guidance through federal energy and security institutions [5], [8]. Mexico provides a relevant emerging-economy case because its manufacturing and services activity depend on reliable electricity and because sector-specific cyber-loss disclosures remain limited. Mexican national accounts allow estimation of economic exposure but do not directly identify losses caused by cyberattacks [13].

## III. DEVELOPMENT

### 3.1 Research design and evidence hierarchy

This study employs documentary analysis and quantitative scenario modeling rather than causal econometric evaluation. The analysis prioritizes official statistical releases, intergovernmental reports, standards, and corporate annual filings from 2020 to 2026. Figures are categorized as observed (published), derived (calculated from published data), or hypothetical (scenario assumptions). In cases where cybersecurity-specific business revenue is not available, total corporate revenue should not be construed as energy cybersecurity revenue.

### 3.2 Technology-business taxonomy

Table 1 shows the relationship among the technology, its operational objective and economic channel

*Table 1. Technology / business taxonomy*

| Technology / practice | Operational objective | Economic channel |
|---|---|---|
| OT asset discovery and monitoring | Identify exposed control assets | Earlier detection; reduced incident duration |
| Network segmentation / zero trust | Limit lateral movement | Lower probability of cascading loss |
| Identity and privileged access | Protect remote/vendor access | Reduced unauthorized operation |
| Incident response and restoration | Restore critical processes | Lower downtime and recovery cost |
| Supply-chain assurance | Manage vendor and software risk | Reduced third-party exposure |
| AI-assisted detection | Prioritize alerts and anomalies | Potential labor savings; model and energy costs |

### 3.3 Expected annual loss and net present value

For mutually exclusive incident scenarios, the expected annual loss is defined in Eq. (1), where p represents the annual probability of incident i, L denotes its conditional monetary loss, and t indicates the year. In the case of overlapping events, dependencies and potential double counting must be explicitly modeled. The reduction in expected annual loss resulting from an intervention is described in Eq. (2). Net present value is calculated using Eq. (3), where $I_0$ is the initial investment, $O_t$ is the incremental annual operating cost, r is the discount rate, and T is the investment horizon. A positive NPV under defensible assumptions provides support for, but does not guarantee, investment.

$$EAL_t = \sum_{i=1}^{N} p_{i,t} L_{i,t} \quad (1)$$

$$\Delta EAL_t = EAL_{without,t} - EAL_{with,t} \quad (2)$$

$$NPV = -I_0 + \sum_{t=1}^{T} \frac{\Delta EAL_t - O_t}{(1+r)^t} \quad (3)$$

### 3.4 Economic exposure to electricity disruptions

Equation (4) presents a first-order approximation of production at risk in sector j, where $V_j$ denotes value-added exposure, $GVA_j$ represents annual gross value added, $s_j$ indicates the share of sector activity affected, h is the interruption duration in hours, and $q_j$ is the fraction of affected output not subsequently recovered. This formulation serves as an illustrative exposure accounting identity rather than a measured causal GDP impact. The denominator 8760 reflects a 365-day year with uniform production; sector-specific operating hours should be used when available. Indirect supply-chain effects are not included unless separately estimated.

$$V_j = \frac{GVA_j s_j h q_j}{8760} \quad (4)$$

For 2027–2035, the conditional economic-scale scenarios use Eq. (5), where $V_t$ is the projected value-added exposure in year t, $V_{2025}$ is the 2025 baseline, and g is the assumed annual real growth rate (1%, 2%, or 3%). Exposure and outage parameters are held constant for illustration. These assumptions are not official forecasts. All projections are expressed in constant 2025 units unless otherwise specified.

$$V_t = V_{2025}(1+g)^{t-2025} \quad (5)$$

### 3.5 Mexico baseline and forward scenarios

INEGI reports a 2025 GDP at current market prices of MXN 35,923,239 million (MXN 35.923 trillion) in its October 2026 goods-and-services accounts [13]. This nominal aggregate serves solely to illustrate the order of magnitude; for meaningful cross-year comparisons, real GDP or sectoral gross value added should be used. Sensitivity testing considers hypothetical national exposure shares of 5%, 10%, or 20%, combined with unrecovered production shares of 25%, 50%, or 75%. These percentages do not represent estimates of Mexico's actual cyber exposure.

For 2027-2035, scenarios assume annual real value-added growth rates (g) of 1%, 2%, or 3%, and evaluate Eq. (5), using constant illustrative exposure and outage parameters. These growth assumptions are intended solely for illustrative purposes and should not be attributed to INEGI, the IMF, or the World Bank. All projections are presented in constant 2025 units unless otherwise specified.

## IV. RESULTS

### 4.1 Observed economic and cybersecurity context

A corporate financial illustration is provided in Figure 1: Fortinet reported consolidated revenues of USD 5,304.8 million (2023), USD 5,955.8 million (2024), and USD 6,799.6 million (2025). These figures are not energy-cybersecurity-specific.

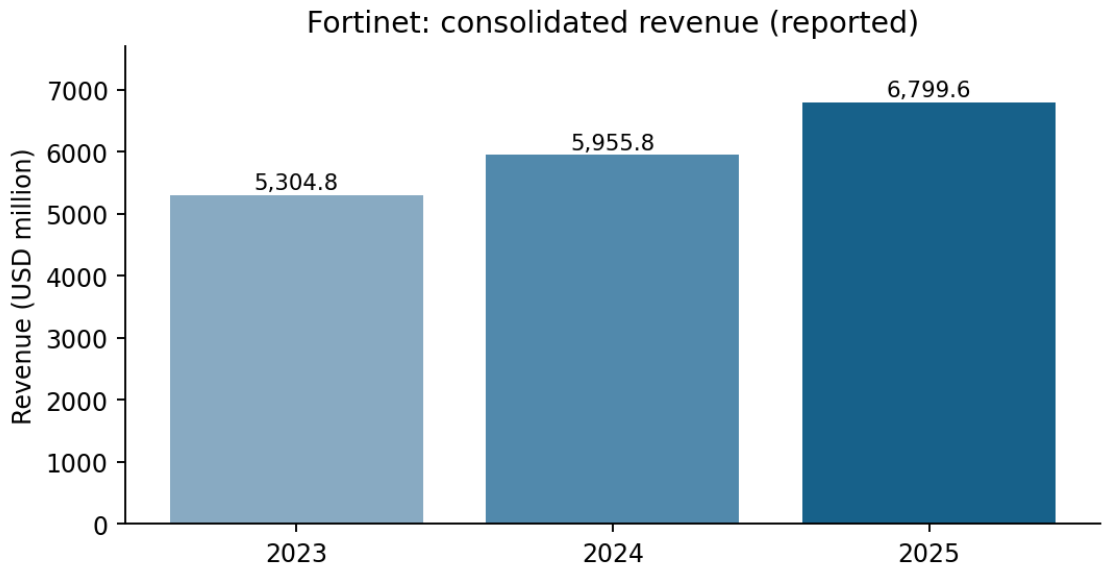



*Figure 1. Fortinet consolidated revenue, 2023–2025 (USD million)*

**4.2 Illustrative investment case**

Consider a hypothetical utility with baseline EAL of USD 2.0 million/year. Assume a 40% reduction in EAL after cybersecurity controls, upfront investment of USD 1.5 million, incremental annual operating expenditure of USD 0.2 million, a five-year horizon and an 8% discount rate. Annual net benefit equals USD 0.6 million; the five-year annuity factor is 3.9927; therefore NPV ≈ USD 0.896 million and undiscounted five-year net benefit after investment ≈ USD 1.5 million. These are calculations from declared assumptions, not measured company performance.

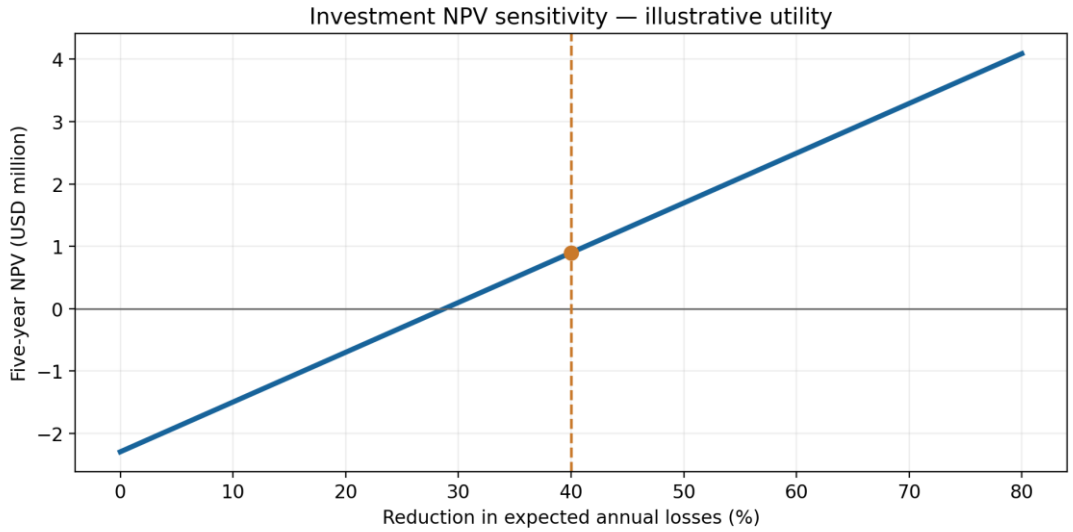



*Figure 2. Five-year NPV sensitivity to expected-loss reduction; hypothetical utility assumptions*

**4.3 Mexico: illustrative interruption exposure**

Using the 2025 nominal GDP benchmark solely as a scale reference, assume that 10% of economic activity is impacted by a 24-hour interruption and that 50% of the corresponding time-proportional output is irrecoverable. The resulting production-at-risk proxy is calculated as 35.923239 trillion × 0.10 × (24/8760) × 0.50 ≈ MXN 4.921 billion. This figure does not represent a historical loss, a forecast, or a verified cyberattack impact. The estimate excludes nonlinear spillovers, sectoral heterogeneity, replacement generation, and compensatory production.

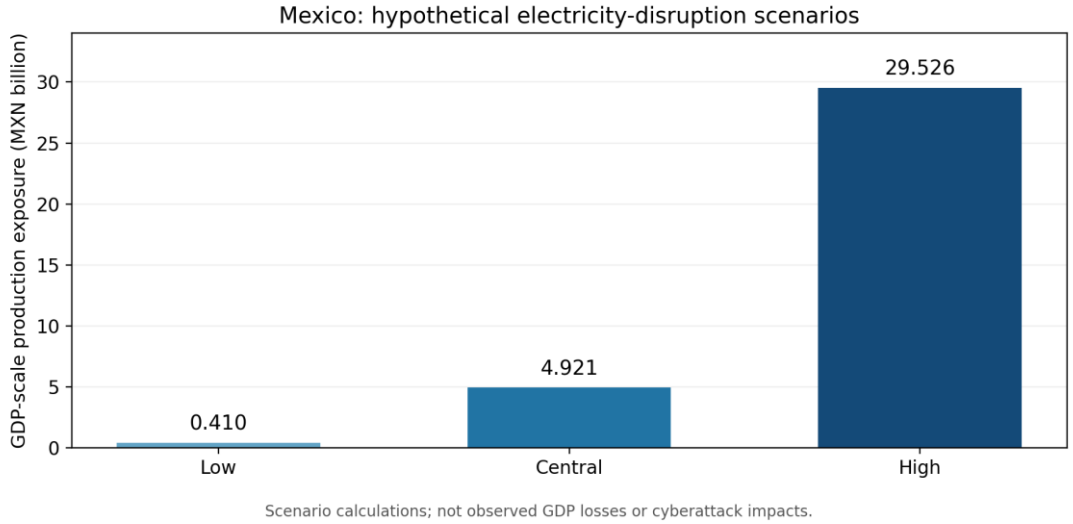



*Figure 3. Illustrative Mexico production exposure under three hypothetical outage scenarios*

*Table 2. Hypothetical cases and parameters*

| Hypothetical case | Affected activity | Hours | Unrecovered share | GDP-scale proxy, MXN billion |
|---|---|---|---|---|
| Low | 5% | 8 | 25% | 0.410 |
| Central | 10% | 24 | 50% | 4.921 |
| High | 20% | 48 | 75% | 29.526 |

**4.4 Conditional 2035 macroeconomic scenarios**

To facilitate comparability, illustrative real growth rates applied to a normalized 2025 index of 100 result in 2035 indices of 110.46 (1% growth), 121.90 (2%), and 134.39 (3%). These indices represent hypothetical economic scale only; they do not predict cybersecurity incidents or suggest that cyber investments drive GDP growth. Future empirical research should link the sector-specific value-added base to outage frequencies, restoration times, and validated cyber-attribution probabilities.

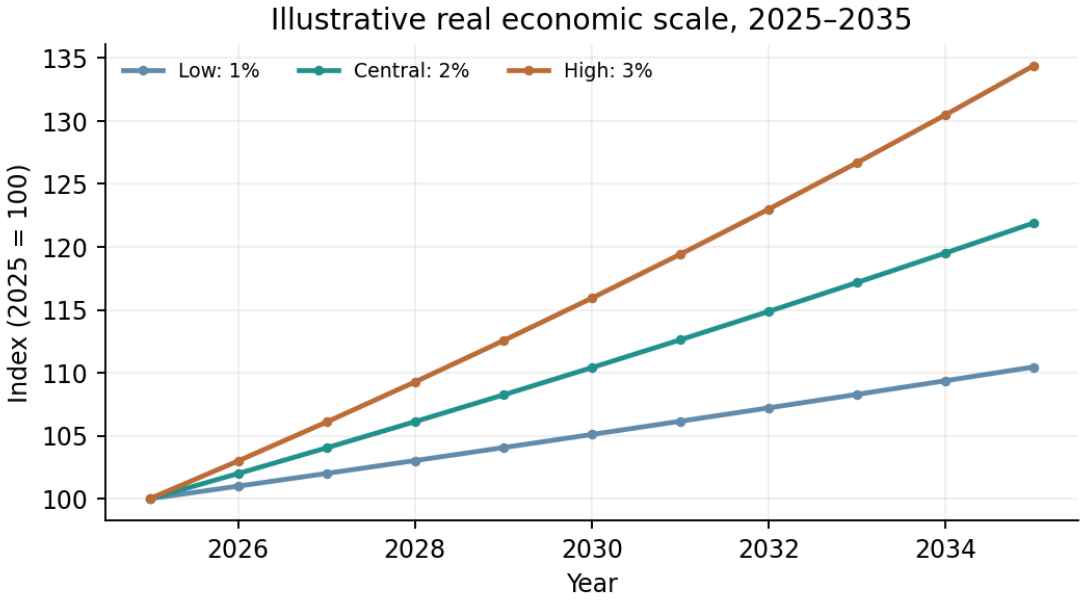



*Figure 4. Conditional economic-scale indices for 2025–2035, assuming 1%, 2%, and 3% annual real growth*

*Table 3. Different scenarios and parameters*

| Scenario | Assumed annual real growth | 2035 value-added index (2025=100) | Evidence status |
|---|---|---|---|
| Low | 1% | 110.46 | Hypothetical |
| Central | 2% | 121.90 | Hypothetical |
| High | 3% | 134.39 | Hypothetical |

### 4.5 Comparative financial performance of cybersecurity providers

In addition to the single-company example, Table 3 presents a comparison of audited consolidated 2025 results for Fortinet and Palo Alto Networks. Revenue, operating income, and GAAP operating margin serve as corporate-wide indicators; these metrics do not specifically isolate energy-sector cybersecurity sales or demonstrate that energy-specific products generated these returns. The fiscal year-ends differ: Fortinet's ends in December, and Palo Alto Networks' in July.

*Table 4. Selected cybersecurity providers: consolidated financial performance in FY 2025.*

| Company (FY 2025) | Revenue (USD m) | Operating income (USD m) | GAAP operating margin |
|---|---|---|---|
| Fortinet | 6,799.6 | 2,084.7 | 30.7% |
| Palo Alto Networks | 9,221.5 | 1,242.9 | 13.5% |

Sources: Fortinet 2025 Form 10-K and Palo Alto Networks 2025 Form 10-K.

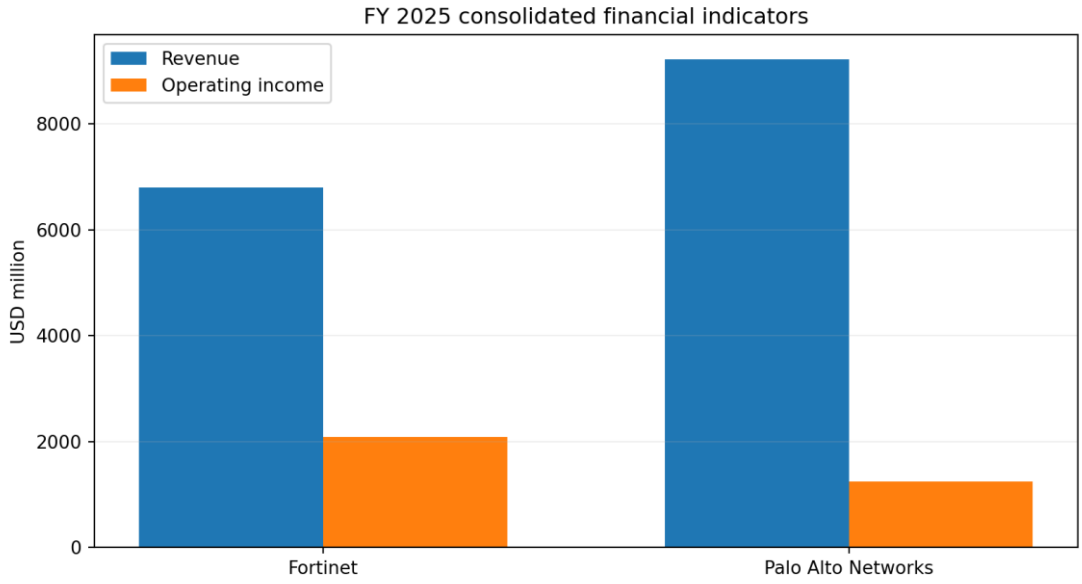



*Figure 5. Consolidated revenues and operating income of two cybersecurity providers in fiscal 2025 (USD million); not energy-specific*

The operating margin was 30.7% for Fortinet and 13.5% for Palo Alto Networks. These differences describe reported GAAP corporate performance and should not be interpreted as the return on energy-sector cybersecurity investments.

## V. FINDINGS AND COMMENTS

First, cyber resilience holds substantial economic significance because electricity serves as a general-purpose input; however, loss estimates must differentiate between data breaches and operational outages. Second, reducing expected losses can yield positive financial returns under plausible hypothetical parameters, though the investment case remains sensitive to baseline risk, control effectiveness, and maintenance costs. Third, the Mexico scenario demonstrates that even brief disruptions may expose considerable value added when numerous firms are impacted, yet national GDP is an imperfect proxy and should not be interpreted as realized damage. Fourth, business opportunities include industrial monitoring, secure remote access, incident response, compliance, and supplier assurance. While public company financial reports may indicate business scale, they typically do not isolate energy-specific cybersecurity profitability.

Environmental and social co-benefits depend on specific contexts. Preventing unsafe control actions can protect communities and ecosystems; however, empirical attribution is constrained by limited incident disclosure. Governance priorities should include safety-critical functions, restoration capabilities, independent assurance, and transparent incident reporting. Public policy may enhance investment decisions by supporting comparable sectoral incident data and standardized cyber-resilience performance metrics.

Limitations include reliance on cross-sector breach-cost data, lack of a validated Mexican cyber-outage dataset, simplified linear downtime-to-output assumptions, and uncertainty regarding long-term growth. Therefore, the numerical results represent scenario demonstrations rather than econometric findings. Future research should utilize confidential utility incident logs, sectoral input–output tables, probabilistic dependencies, and sensitivity analysis calibrated with operational data.

## VI. CONCLUSIONS

Cybersecurity in energy systems should be assessed as an integrated investment in operational continuity, corporate resilience, and the protection of critical public services. The proposed framework connects technology choices to expected avoided losses, discounted net benefits, and potential macroeconomic exposure. Under illustrative utility assumptions, cybersecurity yields a positive five-year net present value. In a separate scenario involving a Mexico-scale outage, the production at risk is economically significant. However, neither result demonstrates a historical causal relationship. The 2027–2035 scenarios highlight the necessity of explicit assumptions and transparent treatment of uncertainty. Managers are advised to prioritize risk-based portfolios, regulators should enhance the availability of incident data, and researchers should validate the framework using sector-level observations before making policy claims regarding GDP, employment, or environmental outcomes.

## REFERENCES

[1] International Energy Agency, “Enhancing Cyber Resilience in Electricity Systems,” 2021. https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems
[2] International Energy Agency, “Electricity Grids and Secure Energy Transitions,” 2023. https://www.iea.org/reports/electricity-grids-and-secure-energy-transitions
[3] International Energy Agency, “Electricity 2024: Analysis and Forecast to 2026,” 2024. https://www.iea.org/reports/electricity-2024
[4] IBM, “Cost of a Data Breach Report 2025,” 2025. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications%2C-97-of-which-reported-lacking-proper-ai-access-controls
[5] National Institute of Standards and Technology, “Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3,” 2023. https://doi.org/10.6028/NIST.SP.800-82r3
[6] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” 2024. https://doi.org/10.6028/NIST.CSWP.29
[7] Cybersecurity and Infrastructure Security Agency, “Cross-Sector Cybersecurity Performance Goals,” 2023. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[8] U.S. Department of Energy, “National Cyber-Informed Engineering Strategy,” 2022. https://www.energy.gov/ceser/cyber-informed-engineering
[9] European Union, “Directive (EU) 2022/2555 (NIS2 Directive),” 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[10] European Commission, “Risk Assessment Report on Cyber Resilience of the EU Telecommunications and Electricity Sectors,” 2024. https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors
[11] European Union, “Directive (EU) 2022/2557 on the Resilience of Critical Entities,” 2022: https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[12] European Union, “Regulation (EU) 2024/2847 (Cyber Resilience Act),” 2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj
[13] Instituto Nacional de Estadística y Geografía, “Cuenta de Bienes y Servicios 2025, año base 2018 (press release, Oct. 2, 2026),” 2026. https://www.inegi.org.mx/app/saladeprensa/noticia/11256
[14] World Bank, “World Development Indicators: GDP (current US$),” 2026. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD
[15] International Monetary Fund, “World Economic Outlook Database, October 2025,” 2025. https://www.imf.org/en/Publications/WEO/weo-database/2025/October
[16] International Energy Agency, “World Energy Outlook 2024,” 2024. https://www.iea.org/reports/world-energy-outlook-2024
[17] International Energy Agency, “World Energy Investment 2025,” 2025. https://www.iea.org/reports/world-energy-investment-2025
[18] ENISA, “ENISA Threat Landscape 2024,” 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[19] ENISA, “ENISA Threat Landscape 2023,” 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[20] World Economic Forum, “Global Cybersecurity Outlook 2025,” 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
[21] World Economic Forum, “Global Risks Report 2025,” 2025. https://www.weforum.org/publications/global-risks-report-2025/
[22] Verizon, “2025 Data Breach Investigations Report,” 2025. https://www.verizon.com/business/resources/reports/dbir/
[23] International Energy Agency, “Energy and AI,” 2025. https://www.iea.org/reports/energy-and-ai
[24] International Energy Agency, “Electricity 2025: Analysis and Forecast to 2027,” 2025. https://www.iea.org/reports/electricity-2025