

Cybersecurity as a Precondition for the Carbon-Neutral Grid: An Investment Framework for U.S. Utility Cybersecurity Capital Allocation

Stefan Daniel Anim-Sampong

stefansampong@gmail.com

Brandeis University

Kwaku Mensah-Bonsu

Emory University

Isaac Larbi

J. Mack Robinson College of Business, Georgia State University

Systematic Review

Keywords: utility cybersecurity investment, carbon-neutral grid transition, distributed energy resources, capital budgeting, real options, FERC Order No. 893

Posted Date: September 21st, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10987772/v1>

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

The transition to a carbon-neutral electricity system depends on the widespread integration of distributed and inverter-based renewable resources. The U.S. Department of Energy and the North American Electric Reliability Corporation have identified these resources as increasing the grid's cybersecurity attack surface faster than current oversight can manage. Federal reviews have also found that guidance for assessing grid cybersecurity risk remains incomplete. In response, the Federal Energy Regulatory Commission has introduced a mandatory internal network monitoring standard and, for the first time, a voluntary financial incentive for cybersecurity investment beyond compliance requirements. However, neither these measures nor the academic literature on security economics and infrastructure capital budgeting provides a clear method for allocating cybersecurity capital as distributed and renewable generation continues to expand. This paper develops a four-component investment appraisal framework that combines the compliance floor established by NERC's Critical Infrastructure Protection standards, the loss-based investment ceiling implied by the Gordon-Loeb model, the timing flexibility provided by real options analysis, and the rate-recovery incentive created by FERC Order No. 893. The framework is applied to the cybersecurity risks associated with distributed energy resource growth in a decarbonizing electric grid. The paper's contribution is methodological rather than empirical. Its application is illustrated using the documented experience of California's CES-21 program and published industry and regulatory benchmarks rather than a hypothetical case. The paper concludes by identifying the empirical research needed before the framework can be calibrated to an actual utility capital plan.

Highlights

- Renewable and distributed energy growth is expanding the grid's cyber-attack surface
- Federal reviewers have twice found U.S. grid cybersecurity oversight incomplete
- New federal rules add a mandatory cybersecurity standard and a voluntary incentive
- No published method tells utilities how to size or time cybersecurity spending
- A four-step framework links compliance, loss economics, timing, and incentives

2 Background and Regulatory Context

2.1 Documented Gaps in Federal Cybersecurity Oversight of the Grid

GAO-19-332 examined how DOE and FERC assess and address cybersecurity risk to the electric grid. It found that DOE's risk assessments relied on an analytical approach that had not kept pace with the evolving threat environment, that FERC's mandatory CIP reliability standards addressed only some of the practices recommended in the National Institute of Standards and Technology's Cybersecurity

Framework, and that FERC's approach to evaluating compliance did not assess the risk posed by a coordinated attack against multiple, geographically distributed points in the grid at once. GAO made three recommendations, and both DOE and FERC concurred (U.S. Government Accountability Office 2019).

GAO-21-81, published approximately 18 months later, examined whether the Department of Energy's national cybersecurity strategy adequately addressed risks to electricity distribution systems. Specifically, it assessed the Multiyear Plan for Energy Sector Cybersecurity (U.S. Department of Energy 2018) and its treatment of distribution-system cybersecurity relative to generation and transmission systems. The report found that DOE's strategy primarily focused on generation and transmission risks and did not fully address risks unique to distribution systems. These included cybersecurity risks associated with the distribution-system supply chain. GAO concluded that the strategy provided limited guidance for prioritizing federal support to the portion of the grid that serves end users and hosts most interconnected DERs. At the time of GAO's most recent public update, the recommendation related to this finding remained open (U.S. Government Accountability Office 2021).

Read together, these two reports describe the same structural problem from two angles. Federal guidance tells a utility a great deal about what categories of cybersecurity risk exist and, increasingly, what minimum controls it must adopt. It does not tell a utility, or the state and federal regulators who review its capital plans, how to weigh a marginal dollar of cybersecurity spending against a marginal dollar spent on any other reliability investment, or how to sequence cybersecurity spending over time as both the threat environment and the applicable standards continue to change. That is the gap this paper's framework is built to address.

2.2 The Mandatory Compliance Floor: NERC's CIP Standards

NERC's CIP-013-2 standard, *Cyber Security Supply Chain Risk Management*, requires responsible entities to develop and implement plans that identify, assess, and mitigate cybersecurity risks arising from vendor products and services used in bulk electric system cyber systems. The standard was approved by the NERC Board of Trustees on November 5, 2020, and approved by FERC on March 18, 2021 (North American Electric Reliability Corporation 2020).

In February 2023, FERC issued Order No. 887, directing NERC to develop a reliability standard requiring internal network security monitoring within trusted CIP-networked environments. The directive applied to all high-impact BES cyber systems, regardless of external routable connectivity, and to medium-impact BES cyber systems with external routable connectivity. FERC specified three objectives for the new standard. First, entities must establish baselines of expected network activity. Second, they must monitor and detect unauthorized activity within the monitored environment. Third, they must maintain logging, data retention, and evidence-preservation capabilities sufficient to support high-confidence identification of anomalous activity (Federal Energy Regulatory Commission 2023a). The resulting standard, CIP-015-1, received FERC approval in 2025 (Federal Energy Regulatory Commission 2025).

Both standards define a floor: a set of controls a responsible entity must implement, and by when, regardless of its own internal assessment of expected loss. Neither standard, nor NERC's broader CIP framework, offers a method for prioritizing discretionary investment above that floor, or for deciding how quickly to move toward it when, as with CIP-015-1, technical requirements are still being finalized while affected entities are simultaneously planning capital budgets years.

2.3 A new Financial Lever

FERC Order No. 893, Incentives for Advanced Cybersecurity Investment, issued under authority granted by the Infrastructure Investment and Jobs Act of 2021, took a different approach. Rather than mandating additional controls, it created a voluntary incentive rate mechanism through which a utility can seek either a return-on-equity adder or deferred cost recovery, with the unamortized portion of qualifying expenses included in the rate base, for cybersecurity investments that exceed mandatory CIP requirements. Eligible investments include those on a Commission-established pre-qualified list, which included participation in the Cybersecurity Risk Information Sharing Program and internal network security monitoring investments, as well as investments evaluated case by case against statutory eligibility criteria. Approved incentives generally remain available for up to five years from the date the qualifying expense is incurred (Federal Energy Regulatory Commission 2023b).

Order No. 893 is significant because it alters the economics of voluntary cybersecurity investment. For the first time, utilities can receive favorable financial treatment for cybersecurity investments that exceed mandatory CIP requirements. Investments that qualify under the order's eligibility criteria may benefit from a lower effective cost of capital than comparable nonqualifying projects. However, the order does not address key capital-planning questions. It does not indicate how much a utility should invest, when investments should be made, or how discretionary spending should be coordinated with mandatory CIP-013-2 and CIP-015-1 compliance requirements. These decisions remain the responsibility of utility capital planners, and no peer-reviewed framework currently exists to guide them.

2.4 Cybersecurity as a Precondition for Reliable Renewable and Distributed Energy Integration

The implications of this gap extend beyond regulatory compliance and directly affect the transition to a carbon-neutral electric grid. The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response and Office of Energy Efficiency and Renewable Energy projected that installed DER capacity, largely consisting of rooftop solar and battery storage, would roughly quadruple by 2025. Although the compromise of a single DER is unlikely to threaten grid reliability, the compromise of a large, aggregated fleet could create significant reliability risks if controlled by a capable attacker (U.S. Department of Energy 2022).

NERC has identified a key regulatory challenge underlying this risk. Mandatory CIP standards apply to bulk electric system cyber systems but generally do not cover distribution-connected DERs or DER aggregators, despite their growing importance to the electric grid. This gap is significant because a

single aggregator may coordinate hundreds or thousands of renewable and storage resources. Consequently, the compromise of an aggregator could have far greater consequences than the compromise of any individual device (North American Electric Reliability Corporation 2022).

As a result, a substantial portion of the cybersecurity investment required to protect DERs and inverter-based renewable resources falls outside the mandatory CIP requirements discussed in Section 2.2. These investments are therefore discretionary capital-allocation decisions. Their importance may be greater than a device-level assessment suggests because aggregation concentrates risk. This type of investment decision is the primary focus of the framework developed in this paper.

2.5 Synthesis

Sections 2.1 through 2.4 establish four facts this paper treats as its point of departure. First, federal oversight bodies have found, in two separate reports several years apart, that the guidance available for assessing and prioritizing grid cybersecurity risk is incomplete. Second, NERC's CIP standards, most recently CIP-015-1, establish a binding compliance floor with its own timeline, independent of any individual utility's internal loss calculus. Still, that floor stops at the boundary of the bulk electric system. Third, FERC's Order No. 893 has, since 2023, created a genuine financial incentive for discretionary investment above that floor, but one whose availability depends on eligibility criteria that a utility must weigh against ordinary capital budgeting considerations. Fourth, and most directly tied to the carbon-neutral transition, the fastest-growing part of the grid's attack surface, distribution-connected DERs, is also the part current mandatory standards do not reach, which means the security of the renewable and storage assets a decarbonizing utility is adding fastest depends almost entirely on discretionary investment decisions. These four facts are individually well documented. Their interaction, and how a utility should navigate all of them at once when building a capital plan, is not; that is the undertheorized space this paper's framework occupies.

3 Theoretical Foundation

3.1 The Economics of Security Investment: The Gordon Loeb Model

Gordon and Loeb (2002) developed a foundational economic model for information security investment. The model demonstrates that organizations should limit cybersecurity spending to an amount justified by the expected loss from a security breach. Its central insight is that security investments exhibit diminishing returns. As a result, organizations can overinvest in security, not only underinvest, relative to their actual risk exposure.

For utilities, the Gordon-Loeb model provides an upper limit on discretionary cybersecurity spending based on the expected loss an investment is intended to prevent. However, the model does not address when an investment should be made or whether it should be implemented in stages. It also does not account for investments required by regulatory mandates. Developed for a general information-security

context, the model does not distinguish between voluntary cybersecurity expenditures and compliance-driven investments, a distinction that is critical to utility capital planning.

3.2 Real Options and Capital Budgeting Under Uncertainty

A separate body of research in finance and infrastructure engineering addresses a limitation of traditional capital budgeting. Methods such as net present value often fail to capture the value of managerial flexibility. This flexibility may include delaying an investment, expanding it as uncertainty declines, or abandoning it if conditions change. Meier, Christofides, and Salkin (2001) developed an approach that combines contingent-claims analysis and integer programming to evaluate investment portfolios under uncertainty. Their approach recognizes the value of staging investment decisions over time. Martins, Marques, and Cruz (2015) similarly argue that infrastructure projects are well suited to real options analysis because they involve large, partly irreversible investments made under uncertain future conditions.

Utility cybersecurity investments share many of these characteristics. This is especially true for cybersecurity investments related to DERs. The threat landscape continues to evolve, technical standards continue to develop, and both DER adoption and cybersecurity technologies are changing rapidly. A utility that invests too early may commit to technologies that do not align with future compliance requirements or the eventual scale of its DER portfolio. Conversely, delaying investment may increase exposure to cyber risk and reduce the opportunity to benefit from the limited-time incentives available under Order No. 893. Real options analysis is designed to evaluate tradeoffs of this kind. However, existing studies have not applied real options analysis specifically to utility cybersecurity investment or integrated it with the compliance requirements established by NERC's CIP standards.

3.3 Why Neither Framework Alone Fits the Cybersecurity Capital Allocation-Problem

The Gordon-Loeb model and real options analysis address different aspects of the cybersecurity investment decision, but neither is sufficient on its own for utility capital planning. The Gordon-Loeb model establishes a loss-based upper limit on cybersecurity spending. However, it does not account for mandatory compliance requirements or the value of delaying or staging investments. Real options analysis addresses investment timing and sequencing under uncertainty, but it does not provide a basis for determining the appropriate level of cybersecurity spending. It can help identify when to invest, but not how much to invest. Neither approach considers regulatory incentives such as FERC Order No. 893, which alters the effective cost of capital for qualifying investments. Nor do they account for the regulatory boundary that excludes many DER-related assets from mandatory CIP requirements.

Consequently, utility planners are left with three separate decision inputs: a compliance floor, a loss-based ceiling, and a timing framework. The literature offers no systematic method for integrating these elements into a single investment appraisal process. It also does not address the investment incentive

created by Order No. 893. Section 4 presents a framework that brings these four considerations together.

4 A Proposed Investment Appraisal Framework

4.1 Design Principles

The framework rests on four design principles, each drawn directly from the regulatory and theoretical material reviewed in Sections 2 and 3. First, compliance is a floor, not an optimization variable. Obligations arising from CIP-013-2 and CIP-015-1 are entered into the framework as fixed, non-discretionary capital requirements with their own compliance deadlines; they are not weighed against an expected-loss calculation, because a utility does not have the option to decline a mandatory standard on economic grounds.

Second, discretionary investment above that floor, including the DER- and renewables-linked investment described in Section 2.4, is bounded by expected-loss economics. For any candidate investment that goes beyond what CIP-013-2 or CIP-015-1 require, the framework applies a Gordon-Loeb-style ceiling, capping proposed spending at a fraction of the expected loss the investment is intended to avert, asset class by asset class.

Third, discretionary investments are evaluated through a real options lens. Projects that satisfy the expected-loss criterion are not automatically funded in full. Instead, the framework examines whether phased capital deployment creates greater value as uncertainty declines. Relevant uncertainties include regulatory guidance, technology maturity, incident experience, and DER interconnection growth.

Fourth, regulatory incentive eligibility is an explicit input, not an afterthought. Whether a candidate investment qualifies for Order No. 893 treatment, and under which mechanism, is evaluated as part of the appraisal itself, because it changes the investment's effective cost of capital relative to competing, non-qualifying capital projects.

4.2 Framework Architecture

The framework proceeds as four sequential components, summarized in Table 1 and described below. Table 1 Summary of the four-component investment appraisal framework.

Component	Governing logic	Key question	Primary source
1. Compliance-floor determination	Mandatory reliability standard	What must be spent, and by when, regardless of loss calculus?	NERC CIP-013-2; CIP-015-1
2. Expected-loss screening	Gordon-Loeb loss-based ceiling	Does the discretionary investment cost less than the expected loss it avoids justifies?	Gordon and Loeb (2002)
3. Real-options staging	Option to delay / stage under uncertainty	Should capital be committed immediately or released in tranches?	Martins et al. (2015); Meier et al. (2001)
4. Incentive-adjusted portfolio ranking	Regulatory incentive eligibility	How does the investment rank against competing capital needs once cost of capital is adjusted?	FERC Order No. 893

Component 1, Compliance-Floor Determination, establishes the utility's baseline compliance obligations. It includes the CIP-013-2 supply chain risk management plan, the CIP-015-1 internal network security monitoring scope, and all relevant compliance deadlines. These requirements constitute the nondiscretionary capital plan and are excluded from further screening. Distribution-connected DERs and DER aggregators are not covered by mandatory CIP standards (Section 2.4). Therefore, investments intended to protect these resources are generally assessed under Component 2 rather than Component 1, even though their combined impact may create significant systemic risk.

Component 2, Expected-Loss Screening, applies to every candidate investment that goes beyond the Component 1 floor, such as extending internal network monitoring to systems not covered by CIP-015-1's mandatory scope, securing DER aggregator communications, integrating additional threat-intelligence feeds, or expanding participation in information-sharing programs. For each candidate, the utility estimates the expected loss the investment is intended to avert and applies a Gordon-Loeb-style ceiling to the proposed spending. Candidates whose proposed cost exceeds the ceiling are rejected outright or resized; they are not approved on the strength of a qualitative threat narrative alone.

Component 3, Real-Options Staging, applies to investments that pass Component 2 assessment. Rather than assuming an immediate full-scale investment, the framework evaluates whether capital should be committed in stages. For example, a utility may begin with a pilot deployment and expand only if performance targets are met and technical guidance becomes clearer. This approach may create greater value under uncertainty in both the threat environment and regulatory requirements.

Component 4, Incentive-Adjusted Portfolio Ranking, evaluates the remaining investments after Components 2 and 3. These investments are considered alongside other utility capital projects, such as transmission upgrades, generation interconnection, and distribution system hardening. A common metric, such as an incentive-adjusted internal rate of return, is used to rank all projects. Investments that qualify for Order No. 893 incentives are evaluated using a lower effective cost of capital. Nonqualifying investments are evaluated using the utility's standard weighted average cost of capital. This approach

enables cybersecurity investments, including those supporting renewable energy and DER assets, to be compared directly with other competing capital priorities.

4.3 A Real Precedent: The CES-21 Program

No utility has yet used the incentive on which Component 4 is based. According to FERC's most recent tracking, no application for cybersecurity incentive treatment under Order No. 893 has been filed or approved (Federal Energy Regulatory Commission 2025b). Morgan Lewis attributed this lack of participation to the incentive's narrow eligibility criteria and limited expected benefits relative to the uncertainty of the application process (Morgan Lewis 2024). This reflects the current state of the field rather than a limitation of this study. Accordingly, the illustration below relies on a better-documented historical precedent: California's CES-21 program.

CES-21 predates CIP-013-2, CIP-015-1, and Order No. 893 by approximately a decade. It therefore cannot be evaluated against regulatory instruments that did not yet exist. Instead, it is used as evidence of the capital-allocation challenges those later measures were intended to address. All financial figures discussed below are drawn directly from California Public Utilities Commission (CPUC) decisions. No values have been estimated, scaled, or assigned to a hypothetical utility. Any conclusions regarding the implications of the framework are the author's interpretation and should be distinguished from the historical record.

In December 2012, the CPUC authorized California Energy Systems for the 21st Century (CES-21), a joint research program involving Pacific Gas and Electric Company, Southern California Edison, and San Diego Gas & Electric in partnership with Lawrence Livermore National Laboratory. The program focused on industrial control system cybersecurity and grid-integration research under high-renewable-penetration scenarios. Decision 12-12-031 authorized up to \$30 million annually for five years, representing total funding of \$152.19 million. Costs were allocated among PG&E, SCE, and SDG&E at 55%, 35%, and 10%, respectively (Joint Utilities of California 2016).

After California Senate Bill 96 (2013) narrowed the program's scope to cybersecurity and grid-integration research, the CPUC adopted Decision 14-03-029 in March 2014. The decision reduced the authorized budget to \$35 million over the same five-year period, including franchise fees and uncollectibles, and revised the cost-sharing allocation to 50%, 41%, and 9% (Joint Utilities of California 2016). This represented an approximately 77% reduction from the original budget. Because the program had been narrowed specifically to cybersecurity and grid-integration research, the reduction fell most heavily on the type of investment examined in this paper.

CES-21 predates CIP-013-2, CIP-015-1, and Order No. 893. Consequently, it cannot be assessed using Components 1 and 4 of the proposed framework. In addition, publicly available CPUC decisions do not indicate that the original funding request was evaluated against an explicit expected-loss threshold of the type proposed in Component 2. Viewed through the lens of the framework, the episode illustrates the potential consequences of the absence of such an anchor. A discretionary cybersecurity investment

proposal without a transparent loss-based justification was reduced by roughly three-quarters following legislative intervention. This adjustment was substantially larger than the phased investment approach envisioned under Component 3. Whether a Gordon-Loeb-style analysis would have altered the outcome cannot be determined from the public record, and no such claim is made here. The record does, however, provide a documented example of the challenge Component 2 seeks to address: a cybersecurity capital request lacking a defensible basis for determining its appropriate scale.

More than a decade later, the underlying issue remains. FERC's estimate for CIP-015-1 includes only administrative compliance costs, such as paperwork and recordkeeping. It estimates annual costs of \$32,116 per affected entity across approximately 400 of NERC's 1,636 CIP-compliant entities (Federal Energy Regulatory Commission 2025a). The estimate does not include technology acquisition, implementation, or integration costs. Utilities therefore continue to rely on external benchmarks when evaluating cybersecurity investments. IBM reported an average global data-breach cost of \$4.44 million in 2025 and an average industrial-sector breach cost of \$5.56 million in 2024 (IBM 2025; IBM 2024). While useful, these figures do not provide a grid-specific estimate of expected cyber loss. At the same time, no utility has yet used the Order No. 893 incentive. Together, these conditions highlight a persistent challenge: utilities must justify discretionary cybersecurity investments without a systematic method for determining whether proposed spending is appropriately sized. The challenge is becoming more significant as an estimated 217 GW of additional DER capacity is projected to be deployed by 2028 (Utility Dive 2024).

5 Discussion

5.1 Implications For Utility Capital Planning

For utility capital planners, the framework's main value is that it provides a structured approach to decisions that are often made informally or in response to immediate pressures. This is especially important for cybersecurity investments related to DERs and renewable resources, which fall largely outside current compliance requirements. As the example in Section 4.3 demonstrates, utilities do not need proprietary data to begin applying the framework. Published benchmarks, such as IBM's breach-cost estimates and FERC's compliance-burden estimates, can provide initial inputs for Components 1 and 2. The CES-21 experience also illustrates the risks of advancing a discretionary cybersecurity investment without a clear analytical basis.

The framework's loss-based ceiling offers a defensible method for evaluating discretionary cybersecurity spending. It helps distinguish investments supported by quantified risk exposure from those justified primarily by qualitative threat concerns. At the same time, it recognizes that DER aggregation can create system-level risks that exceed those suggested by a device-level assessment. The framework also treats investment timing as a real-options decision. This approach is particularly relevant as CIP-015-1 implementation, DER cybersecurity technologies, and DER deployment continue to evolve. Finally, incorporating Order No. 893 eligibility into the investment appraisal process allows utilities to account

for the incentive's potential value at the outset of capital planning. Although no utility has yet used the incentive, considering it early in the decision process may improve investment prioritization and funding strategies.

5.2 Implications For Regulators and Policy Makers

For state and federal regulators, the framework provides a consistent way to evaluate cybersecurity capital requests. Utilities could show whether a proposed investment is required for compliance, supported by an expected-loss assessment, staged over time, or eligible for Order No. 893 incentives. This would also help regulators compare cybersecurity spending across utilities and assess whether DER-related security investment is keeping pace with renewable energy growth.

The lack of utility participation in the Order No. 893 incentive (Federal Energy Regulatory Commission 2025b; Morgan Lewis 2024) may indicate that its eligibility requirements, financial benefits, or filing risks warrant further review. The framework highlights this issue but does not seek to resolve it.

A practical challenge remains. Component 2 relies on expected-loss estimates, yet utilities may be reluctant to disclose such information in public proceedings because of security and competitive concerns. Addressing this issue is beyond the scope of this paper, but some form of confidential review may be necessary for the framework to function in practice.

5.3 Limitations and Boundary Conditions

This framework is a conceptual synthesis and has several limitations. First, estimating expected losses from grid cybersecurity incidents, especially those involving DER aggregators, remains difficult. The IBM breach-cost figures used in Section 4.3 are broad industry averages rather than grid-specific estimates. Similarly, GAO's finding that DOE's cybersecurity risk assessment methodology was outdated suggests that a reliable grid-specific alternative is not yet available (U.S. Government Accountability Office 2019). The CES-21 example also predates CIP-013-2, CIP-015-1, and Order No. 893. It illustrates the consequences of an unanchored cybersecurity investment request but does not represent a direct application of Component 2.

Second, the Gordon-Loeb model was developed for general information-security investments and may not fully capture electric-grid cybersecurity risks, particularly those with broader reliability and public-safety impacts.

Third, real options analysis requires estimates of uncertainty that can be difficult to develop in a rapidly changing regulatory, threat, and DER environment.

Fourth, FERC's cost estimate for CIP-015-1 includes only paperwork and recordkeeping costs. No published estimate currently captures the technology and integration costs of compliance, making it difficult to define Component 1's compliance floor precisely.

Finally, the framework has not been tested using an actual utility capital plan or threat assessment. It is presented as a methodology rather than a validated decision tool. Applying the framework to utility-specific data is the next step before it can support real-world capital allocation decisions.

5.4 Future Empirical Research Agenda

Several areas of empirical research are needed to move this framework from a conceptual model to a validated decision tool. First, case studies using anonymized utility capital-planning data could examine whether the four-component framework produces different and more defensible investment decisions than current practices, particularly for DER-related cybersecurity investments. Second, research is needed to develop expected-loss estimates specific to grid cybersecurity incidents and DER-aggregator compromise, reducing reliance on broad industry benchmarks such as IBM's breach-cost averages. Third, the lack of utility participation in the Order No. 893 incentive program warrants investigation. Future studies should examine the factors limiting participation and assess whether changes to the incentive structure or eligibility requirements could increase its use. Once utilities begin filing for the incentive, comparative analysis could provide insight into how regulators evaluate cybersecurity investment proposals in practice. Finally, sensitivity analyses of the framework's real-options component could assess how changes in uncertainty and DER growth affect investment recommendations and help evaluate the robustness of the framework under different assumptions.

6 Conclusion

This paper develops a conceptual framework for utility cybersecurity capital allocation. It integrates four elements that have previously been treated separately: the compliance floor established by NERC CIP-013-2 and CIP-015-1 standards, the loss-based investment ceiling implied by the Gordon-Loeb model, the timing flexibility provided by real options analysis, and the incentive-adjusted cost of capital created by FERC Order No. 893. The framework is applied to cybersecurity risks associated with distributed energy resources (DERs) and inverter-based renewable technologies, which are expanding rapidly but remain largely outside the scope of current mandatory standards.

The paper's contribution is methodological rather than empirical. Although each component is well established in the regulatory or academic literature, their integration into a single sequential appraisal process has not previously been proposed. The illustrative example draws on published evidence, including FERC compliance-cost estimates, IBM breach-cost benchmarks, Wood Mackenzie DER growth projections, and the historical experience of California's CES-21 program.

Empirical evidence sufficient to fully validate the framework remains limited. CIP-015-1 was approved only in 2025, and no utility has yet made use of the Order No. 893 incentive. As implementation experience emerges, future research should test and refine the framework. This work will help assess whether cybersecurity investment practices are evolving in step with DER expansion and the broader energy transition.

Declarations

Competing interests:

The authors have no competing interests to declare that are relevant to the content of this article.

Funding:

No funding was received for conducting this study.

Author Contribution

S.D.A.-S. conceived the review, designed the search strategy and inclusion criteria, conducted the literature search, synthesized the findings, and drafted the manuscript. K.M.-B. contributed to literature screening, assisted with thematic categorization of the reviewed studies, and critically revised the manuscript. I.L. contributed to the critical appraisal of the reviewed literature and reviewed the manuscript for intellectual content. All authors reviewed and approved the final manuscript.

Acknowledgements:

Not applicable.

Data availability:

Not applicable. All sources analyzed are publicly available and are cited in the reference list.

References

1. Federal Energy Regulatory Commission (2023a) Internal network security monitoring for high and medium impact bulk electric system cyber systems. Order No. 887, Docket No. RM22-3-000. Federal Register, 9 February 2023
2. Federal Energy Regulatory Commission (2023b) Incentives for advanced cybersecurity investment. Order No. 893, Docket No. RM22-19-000. Federal Register, 3 May 2023
3. Federal Energy Regulatory Commission (2025a) Critical infrastructure protection reliability standard CIP-015-1: cybersecurity, internal network security monitoring. Federal Register, 2 July 2025
4. Federal Energy Regulatory Commission (2025b) Cybersecurity incentives. FERC, Washington, DC. <https://www.ferc.gov/incentives/cybersecurity-incentives>

5. Gordon LA, Loeb MP (2002) The economics of information security investment. *ACM Trans Inf Syst Secur* 5:438–457. <https://doi.org/10.1145/581271.581274>
6. IBM (2025) 2025 cost of a data breach report: navigating the AI rush without sidelining security. IBM Think, Armonk, NY. <https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai>
7. IBM (2024) Cost of a data breach: the industrial sector. IBM Think, Armonk, NY. <https://www.ibm.com/think/insights/cost-of-a-data-breach-industrial-sector>
8. Joint Utilities of California (2016) 2016 joint utilities annual report: CES-21 program. Filed with the California Public Utilities Commission, San Francisco, CA. https://www.cpuc.ca.gov/-/media/cpuc-website/divisions/energy-division/documents/infrastructure/energy-research-development-and-deployment/2016-jointutilitiesannualreport_ces-21program.pdf
9. Martins J, Marques RC, Cruz CO (2015) Real options in infrastructure: revisiting the literature. *J Infrastruct Syst* 21:04014026. [https://doi.org/10.1061/\(ASCE\)IS.1943-555X.0000188](https://doi.org/10.1061/(ASCE)IS.1943-555X.0000188)
10. Meier H, Christofides N, Salkin G (2001) Capital budgeting under uncertainty: an integrated approach using contingent claims analysis and integer programming. *Oper Res* 49:196–206. <https://doi.org/10.1287/opre.49.2.196.13531>
11. Morgan Lewis (2024) Why haven't FERC cybersecurity incentives incentivized cybersecurity investments by electric utilities? Morgan Lewis, Washington, DC. <https://www.morganlewis.com/pubs/2024/09/why-havent-ferc-cybersecurity-incentives-incentivized-cybersecurity-investments-by-electric-utilities>
12. National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. NIST, Gaithersburg, MD. <https://doi.org/10.6028/NIST.CSWP.29>
13. North American Electric Reliability Corporation (2020) CIP-013-2: cyber security, supply chain risk management. Approved by NERC Board of Trustees 5 November 2020; approved by FERC 18 March 2021
14. North American Electric Reliability Corporation (2022) Cyber security for distributed energy resources and DER aggregators. NERC Security Integration and Technology Enablement Subcommittee, Atlanta, GA
15. US Department of Energy (2018) Multiyear plan for energy sector cybersecurity. DOE, Washington, DC
16. US Department of Energy (2022) Cybersecurity considerations for distributed energy resources on the U.S. electric grid. Office of Cybersecurity, Energy Security, and Emergency Response and Office of Energy Efficiency and Renewable Energy, DOE, Washington, DC
17. US Government Accountability Office (2019) Critical infrastructure protection: actions needed to address significant cybersecurity risks facing the electric grid. GAO-19-332. GAO, Washington, DC
18. US Government Accountability Office (2021) Electricity grid cybersecurity: DOE needs to ensure its plans fully address risks to distribution systems. GAO-21-81. GAO, Washington, DC
19. Utility Dive (2024) US to add 217 GW of distributed energy resource capacity through 2028, Wood Mackenzie projects. Utility Dive, 3 July 2024. <https://www.utilitydive.com/news/wood-mackenzie->

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [floatimage1.png](#)