Taxonomy of Cyber Risk Mitigation Cost Benefit Analysis Methods for Energy Infrastructure

Kam Hwei Syn, Yvonne; Jones, Kevin; Tam, Kimberly; Rawlinson-Smith, Robert

Published in:
Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience, CSR 2024

DOI:
10.1109/CSR61664.2024.10679375

Publication date:
2024

Document version:
Publisher's PDF, also known as Version of record

Taxonomy of Cyber Risk Mitigation Cost Benefit Analysis Methods for Energy Infrastructure

Yvonne Hwei Syn Kam
School of Engineering, Computing and Mathematics,
University of Plymouth,
England, United Kingdom
yvonne.kamhweisyn@plymouth.ac.uk

Kevin Jones
University of Plymouth,
England, United Kingdom
kevin.jones@plymouth.ac.uk

Robert Rawlinson-Smith
School of Engineering, Computing and Mathematics,
University of Plymouth,
England, United Kingdom
robert.rawlinson-smith@plymouth.ac.uk

Kimberly Tam
School of Engineering, Computing and Mathematics,
University of Plymouth,
England, United Kingdom
kimberly.tam@plymouth.ac.uk

2024 IEEE International Conference on Cyber Security and Resilience (CSR) | 979-8-3503-7536-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/CSR61664.2024.10679375

***Abstract*— Cybersecurity is a critical aspect for the energy industry to defend against cyber attacks. However, justifying the costs of cybersecurity measures is essential. A cost-benefit analysis (CBA) is commonly used to support decision-making for risk mitigation, helping to identify strategies that optimally balance mitigation costs and risk reduction. In this survey, we analyse existing approaches and provide a taxonomic overview of methods for cyber risk mitigation cost-benefit analysis, focusing on key aspects that determine their applicability to energy systems. The survey includes both general and contextual works, employing various methodologies for CBA, whether analytical or criteria-based. We conclude with an analysis of future directions based on recent developments in these methods. As an emerging area, this taxonomy could serve as a foundation that can be expanded with more data from other publications in the field, offering an opportunity to advance knowledge in energy systems.**

Keywords—energy, cyber, risk, mitigation, cost benefit analysis, taxonomy, survey

I. Introduction

A DNV report [1] stated that energy executives anticipate an increase in cyber attacks on the energy industry. They expect these attacks to cause operational shutdowns (85%) and damage to energy assets and critical infrastructure (84%). Additionally, 74% foresee environmental harm, and 57% anticipate fatalities as a result of such attacks. Similarly, a report [2] by the Alan Turing Institute highlighted the growing threats faced by the offshore wind energy industry. Forbes reported 2,365 cyberattacks in 2023, affecting 343,338,964 victims [3]. Given the prevalence of these attacks, cybersecurity is crucial for the energy industry to protect itself.

A. Cyber security spending and justification

In this research, we are concerned with cyber risk mitigation. NIST defines cyber risk as risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system [4]. However, cybersecurity solutions for cyber risk mitigation can be costly and therefore need to be justified in an organisation. Gartner forecasted spending to increase to $215 billion in 2024, an increase of 14.3% from 2023 [5]. The number of cybersecurity solutions available, and their range of capabilities and costs, makes cost benefit analysis a critical part of an organisations cybersecurity strategy [6].

Because an organization's cybersecurity investment has financial considerations, there should be justification for investment in mitigation measures. When determining the most effective strategy, a cost-benefit analysis (CBA) becomes crucial. The CBA can be used to analyse and evaluate between mitigation measures.

A cost-benefit analysis is the process used to measure the benefits of a decision, minus the costs associated with taking that action [7]. A cost benefit analysis (CBA) is commonly utilised to support decision-making in risk mitigation. With a CBA, risk mitigation strategies that strike an optimal balance between the costs of mitigation measures and the resulting risk reduction can be identified [8].

II. Background

A. Risk Treatment Process

Fig. 1 illustrates the process of risk treatment. The stages of establishing the context and risk assessment are prior and necessary steps before the stage of risk treatment. Under risk treatment, there are the stages of mitigation analysis and mitigation evaluation. Under the step of mitigation analysis, firstly the controls or mitigation measures under consideration are determined. Cybersecurity risk estimation estimates the prospective residual risk after implementation of the controls. If the estimated residual risk from implementation of a control is acceptable, the control goes through the step of mitigation evaluation.

In mitigation evaluation, the quantitative and qualitative costs and benefits of (or set of) controls are estimated. The difference in prospective losses after implementing the control compared to doing nothing constitutes the benefits. The costs of the control are the costs of implementing the control and any related losses in the implementation.

The costs and benefits can be quantitative or qualitative. **Quantitative** data is information about monetary quantities, it can be counted, measured, and expressed using numbers. Examples are cost of mitigation and potential savings from the mitigation. **Qualitative** data is descriptive and conceptual, categorised based on traits and characteristics that can be observed but not measured [9].

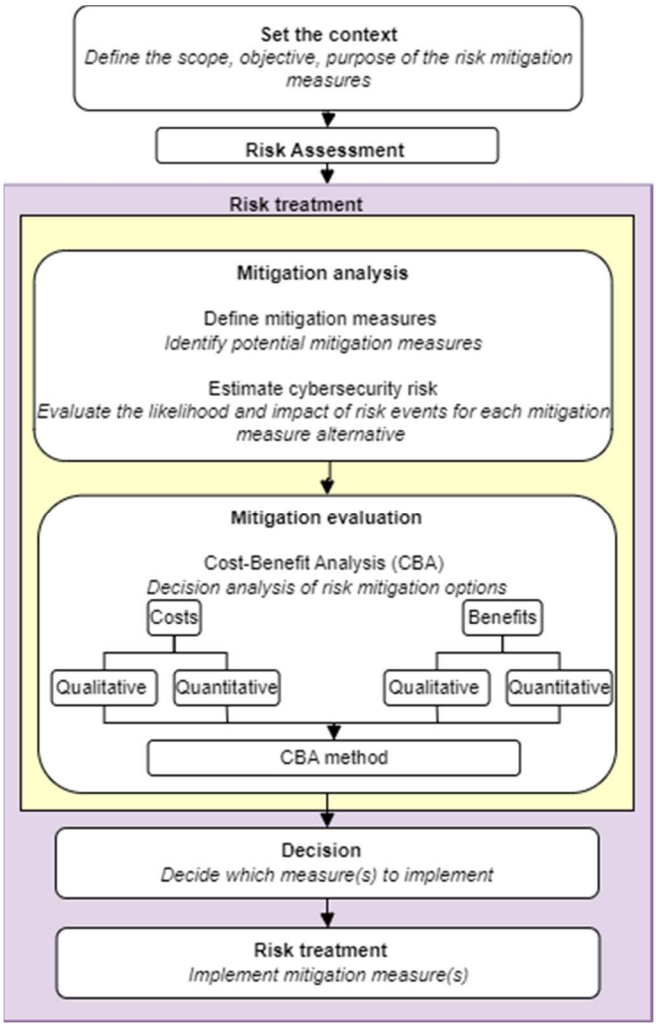

Fig. 1. Overview of process of risk treatment

Examples are reduced risk, effectiveness and ease of use. However, inherently qualitative data can also be expressed quantitatively. For example, subject matter experts (SMEs) can rank data into numerical values, or convert qualitative information into estimated quantitative values using calculations based on related quantities. An example of this is expressing risk in monetary terms.

A CBA is performed with the cost benefit data using the chosen CBA method. Thereafter, the decision is made and if selected, the control measures are implemented.

B. Area of application

This paper focuses on infrastructure in the energy industry, specifically on the convergence of Information Technology (IT) and Operational Technology (OT), known as IT/OT. This convergence creates cyber-physical systems (CPS), which integrate sensing, computation, control, networking, and analytics to interact with the physical world. CPS are a result of the IT/OT convergence, providing a unified ecosystem [10].

The cost-benefit analysis (CBA) for IT/OT systems differs from that for purely IT systems due to different types of losses, considerations, and priorities. Cyber-physical systems can experience physical losses, which might have more severe consequences, including environmental and human impacts. Mitigation measures in OT systems can be disruptive and require careful planning around maintenance schedules, unlike IT systems where updates are more routinely implemented.

In CBA of energy OT systems, the potential disruption caused by mitigation methods must be considered. Control measures should be chosen based on their potential impact, costs, and effectiveness in the specific context of the energy OT environment, which differs significantly from purely IT systems. Disruptions must also be considered in IT, however, if an issue arises, network equipment can often be shut down or isolated for troubleshooting, which is less feasible in OT environments where shutting down is rarely an option.

Information security has mostly been applied to enterprise IT networks, resulting in more research on CBA for IT compared to OT [11], [12], [13], [14], [15], [16], [17]. Previous works on CBA of IT mitigation measures may not be directly applicable to converged IT/OT systems, although some standard cost benefits remain the same. Energy OT differs from general OT in that disruptions can have higher severity due to its role as critical infrastructure. Energy availability impacts other businesses, infrastructure (such as hospitals and transport), and public welfare (including safety and environmental concerns).

Energy OT can and do use existing CBA methods for IT and OT since energy networks consist of IT/OT networks, which are connected to physical processes for energy production, transmission, and distribution. However, at times there is a need for CBA customized to energy OT, as evidenced by papers that consider energy-specific factors like mass disconnect power [18], and grid frequency and voltage deviations [19]. However, these could be too specific to apply to other applications. Thus, general IT, general OT, and context-specific energy OT CBAs can apply at different times to different parts of the energy IT/OT network but each have limitations. General IT and OT CBA cost modeling may not cover the specific needs of energy OT, while contextual methods, being more specific, may not apply to other areas within energy OT. To clarify the field, this paper aims to survey the range of CBA methods applicable to energy OT.

Limited research has been conducted on quantifying the cost-benefit trade-offs of security tools in OT applications [20]. Few surveys [21], [22] exist on cyber risk quantification and taxonomies for cyber risk treatment, and these do not focus on cyber risk mitigation CBA methods for energy infrastructure. This gap justifies the focus of this work, which aims to curate and classify existing knowledge to advance the field.

The proposed taxonomic survey provides a framework for assessing the suitability of CBA methods for the energy sector. It classifies methods based on general or contextual applicability, the method of the CBA, the output of the CBA, and the cost-benefit factors considered.

The remainder of this work is organized as follows: Section 3 explains the proposed taxonomy and analyzes various methods. Section 4 presents a discussion and outlines future directions. Finally, Section 5 concludes the study.

III. TAXONOMY

The aim of presenting a taxonomy is to clarify the domain in terms of the types and applicability of the CBA methods for energy systems. The methods describe various types of

CBA methods for different use cases. Understanding the different types of CBA and their use cases enables the selection of the most appropriate one for a specific application.

The proposed taxonomy is shown in Fig. 2. We first divide the methods based on breadth of application into general and contextual. General methods are those which can fit a wider range of use cases. These methods are suitable for general application in energy systems. Contextual methods are those which are not so easily generalised for adapting into different use cases. Reasons for this could include being designed for a specific setting or context, or requiring specific data collection setups or criteria parameters that may not align with the needs of a particular use case.

Both contextual and general methods can be divided into the type of CBA method, which are: based on multicriteria or calculated analytically. Analytical methods calculate CBA using a formula which results in a numerical number. For example, the CBA method employed could be for example, cost benefit differences, Return on investment (ROI), or Payback period.

Criteria-based are methods that use multicriteria analysis (MCA) methods to determine the CBA. MCA generally includes these stages: developing options, identifying objectives and criteria to evaluate the options, weighting the criteria, and scoring the impacts of options against the criteria to rank them. In some MCA procedures, rather than scoring or weighting, the performances of options are simply presented using tables, graphs, or diagrams [23].

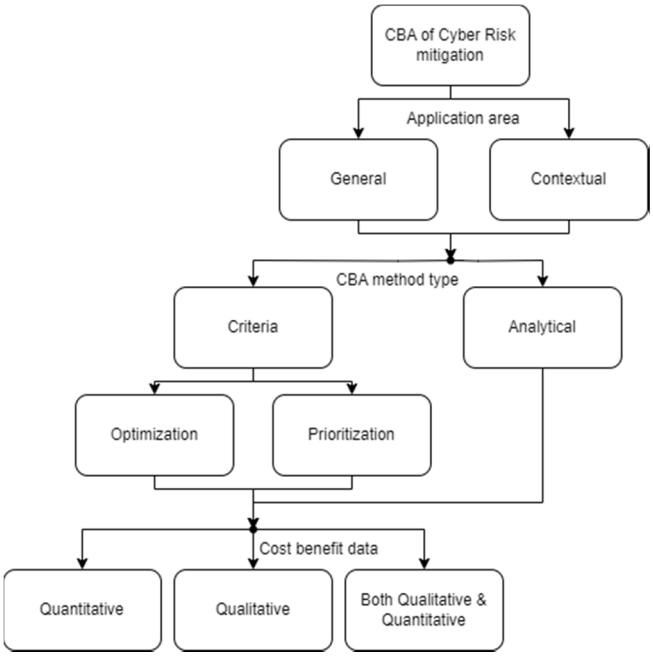

Fig. 2. Taxonomy of methods for cyber risk mitigation cost benefit analysis

Criteria-based methods are further divided into the methods used to determine the performance of options, namely, prioritisation and optimisation. While prioritisation methods concentrate on ranking alternatives, optimisation methods aim to find optimal solutions that balance multiple objectives.

The CBA methods work with input data. The types of data a CBA method works with are quantitative, qualitative or a combination of both.

The next section describes the taxonomy categories, with examples of existing works that fall within them. Table 1 shows the surveyed works in the categories.

A. Application area: General or Contextual

For researchers or practitioners seeking to select suitable cyber risk mitigation CBA methods for their use case, knowledge on the area of applicability of the methods is essential. Therefore, the taxonomy first categorizes the methods by application area into general and contextual. Table 1 also shows the setting or industry that the method is based in.

General methods can be applied for use on energy systems or customised for different use cases. Some factors contribute to the broader applicability of these methods. They may be widely applicable because they address common costs. Methods implemented for information security cyber risk mitigation e.g. [24] ,[25], [26], [27] have standard cost models which are not specific to an industry and could be generally applied to energy IT/OT. However, though general, the method [27] considers a larger number of costs and benefits, which may not all be suitable. The method in [28] considered the NIST Cybersecurity Framework (CSF) and Cybersecurity Capability Maturity Model (C2M2) maturity levels in their CBA, which has general applicability. These costs and benefits are non-domain-specific thus the methods are considered generally applicable.

Contextual methods have their own defined structure in order for the method to be used: e.g. risk assessment setups, data collection sources, parameters, cost model, which means it may be challenging to customise and adapt the method to a different use case. Contextual methods are specific to the context or intended application. Some are contextual because they are supposed to be for a field-specific use case. For example, [20] is a method for cyber physical resilience of wind turbine generators against attacks. The metrics considered included generation penalty derived from wind site power production and local voltage measurements. Similarly, [19] was meant to address the cybersecurity of hybrid AC/DC grids, and considered field specific metrics such as AC grid frequency & DC voltage deviations. Other examples that included metrics that were field specific include [29], [18], [30].

Certain methods assume certain input prerequisites and set up before being able to use the method. For example, host/network data collection in [31] or network configuration information in [12], which are use case specific, and require software configuration in the context of computer networks. The method in [32] has a testbed with the deployed security framework components and needs inputs such as events and logs from several signatures based sensors.

Some other methods were categorised as contextual because the costs and benefits considered are fixed. Examples are those methods which are using optimisation of costs and benefits based on criteria [32],[11]. The limitation with optimisation is that the criteria are predefined in each of the works and are not easily changed, added or removed to suit a use case. These could make the method contextual because

these choices may not be the alternatives and criteria which fit the needs of a use case. An exception is [28]; despite its use of optimization, it was considered generally applicable because it employed standard NIST CSF controls and Maturity Indicator Levels (MIL) as criteria, which are for general use and not intended to be altered.

B. *Method of performing CBA: Analytical or criteria-based*

The method of computing CBA is divided into *analytical* or *criteria*-based. Analytical method means using a formula to solve for a particular set of variables to calculate its value, which requires quantitative values. CBA methods in [20],[29],[30],[24] are examples in this category. Most in this category calculate the cost benefit by using differences between the loss scenario and implementation costs of the controls [20],[30]. For [29], the CBA was a projection of the savings gained from using control measures against cyber threat events. The method in [24] compared between assigned quantitative policy numbers which denote attack difficulty.

The criteria-based methods were divided further into the methods for determining the performance of the mitigation controls - prioritisation and optimisation. Methods [26], [27] used prioritisation methods such as Analytical Hierarchy Process (AHP) model to select the ranking of controls. Examples of methods that employ optimization techniques to find optimal solutions balancing multiple objectives include [11],[12],[19],[18],[31],[32].

C. *Cost benefit data types: Quantitative and Qualitative*

The common quantitative costs presented were the scenario losses from cyber threat events and implementation costs of the controls. The papers [20] and [30] broke the implementation costs down into capital, maintenance, labour/installation. The authors of [30] made further breakdowns for several scenarios of control measures. Others proposed cost effectiveness, ROI and budget. In reference [18], rather than conducting cost modelling, they used illustrative costs of control measures. The work in [29] considered simplified costs in buckets according to the scale of impact of the cyber incident {minor, major, catastrophic}. The cost was based on risk score rather than actual cost estimates and did not consider the cost of implementing the controls.

A few contextual methods derived the quantitative costs and benefits from non-monetary quantities. These were such as cyber and physical resilience derived from wind site power production and local voltage measurements [20], AC grid frequency & DC voltage deviations [19].

The common qualitative measure was risk reduction from the control measures. The objective of these methods was to mitigate cyber risk thus the common benefit sought would be reduction in risk in some form or other, which is present in all the methods. The risk related measures were such as scale of impact of incident, cyber and physical resilience, effectiveness of mitigation measures, return on attack, attack difficulty, defence probability, number of threats affected by control, and negative cost effect of countermeasure, and MIL. Though risk is not inherently monetary or quantitative, the measure to approximate risk can be quantitative, for example, cyber and physical resilience [20]. Additionally, qualitative measures such as MIL are expressed as numbers to denote ranking [28]. As such, risk related measures can be expressed variously as qualitative and quantitative depending on its composition.

Other qualitative costs and benefits encountered were compatibility of mitigation measures, geographical location, geopolitical context, installed rated power, usability and perceived ease of use.

IV. Discussion and Future Directions

Most of the methods surveyed were contextual and highly specialised to the application area. For example, methods like [19] had context specific costs and benefits such as AC (alternating current), DC (direct current) and VSC (voltage source converters) quantities. The advantage is that it is suited and detailed for the particular context. However, it may be challenging to customise and adapt the method to a different circumstance. Some works e.g. [32], consider a set of costs and benefits that are applicable for cyber physical systems, including energy OT. The advantage is that such a method could be implemented into a suitable general energy OT application. However, the cost modelling is incorporated into the formulas of the method thus one could not easily add other costs and benefits to be considered. A way forward could be to build in customisability to the method where descriptions can be given on which parts of the method could be modified and how to modify it. Perhaps future methods could have add-on costs/benefits that can be added or removed.

For general methods e.g. [24],[25], the methods have the advantage of broad applicability to energy systems. The downside is, they do not cover the costs and considerations that are specific to the energy cyber physical domain. General methods could overlook considerations of the specific field, leading to limited depth in cost-benefit analysis due to their non-specialization. To address this, methods that incorporate a general setup, data collection, costs and benefits, with the ability to add customisation of the relevant costs and benefits of the intended target area could be explored.

The CBA methods used were mostly different with much variability from the input data collection and setup required by the methods, the mitigation controls, to the costs and benefits considered where it is difficult to compare the results obtained by each method. A question arises: If a particular set of alternative cyber risk mitigation controls was compared between these methods, would they have a different outcome and how would one judge between them? Perhaps future work could compare and evaluate methods for efficacy and accuracy in selection. These could give some incentive for the industry to implement these methods.

Some inputs to the CBA are not as straightforward as monetary costs. Some methods, such as [12], have converted conventionally various nonquantitative indicators such as risk into monetary quantities in order to work with them mathematically. The advantage is the ability for computation. However, they are not readily convertible and may be subject to debate. Other methods have retained risk = impact x probability [30], which is a more standard definition. However, it is known to be difficult to estimate measures like probability of attack [30]. How the method to estimate the input parameters impacts the CBA could warrant further investigation.

Energy and broadly OT systems prioritise certain factors such as availability. It is possible that some mitigation controls could have some adverse effect on the OT systems such as latency and disruption, especially on legacy components. Among the literature, there is some consideration [26], [32] but not most. Factors that impact energy OT systems could be given cost consideration in future works.

In summary, the limitations of the CBA methods being used were that some methods were too general, lacking the granularity to make them particularly useful to specific applications in energy systems. Conversely, CBA methods that were specific to a particular application were not readily applicable for other purposes. Methods that were tied to a particular set up (such as network configuration, inputs, data collection, sensors, formulas) are not easily applied into a different system and further investment could be needed for the set up. Lessons learned for future works of CBA for energy systems would be to design methods that are more readily applicable, with less requirements as well as being more customisable towards an application.

V. Conclusions

This paper proposes a taxonomy and survey of cyber risk mitigation cost benefit analysis methods for energy infrastructure. Our survey covers works that are general as well as contextual, analytical or criteria-based and using different methodologies for performing the cost benefit analysis. Analysing the works with regards to the proposed taxonomy, we have discussed future directions that might improve the applicability, comparability and comprehensiveness of CBA methods for energy systems.

As an emerging area, we expect this work could be a basis that can be expanded with a larger data set from other publications in the field.

Acknowledgment

This research was funded by a Supergen ORE PhD Studentship at the University of Plymouth and FRGS Grant (FRGS/1/2015/ICT04/MMU/03/6).

TABLE I. Existing Work Mapped to the Proposed Taxonomy

Ref	Setting/ Area	Application area	CBA type	CBA form	Quantitative Costs/benefits	Qualitative Costs/benefits
[29]	Electricity transmission and distribution	Contextual	Analytical	In proportion to risk score	Scenario loss	Scale of impact of incident {minor, major, catastrophic}, function of control, control availability by site and over time, control effectiveness, threat routes, profile, likelihood, and types
[20]	Wind power	Contextual	Analytical	Payback period	Capital, maintenance, labour, cyber and physical resilience	-
[30]	Solar nanogrids	Contextual	Analytical	Cost difference	Scenario loss, implementation cost	Geographical location, Geopolitical context, Installed rated power
[18]	Electric power grid	Contextual	Criteria	Optimisation	Illustrative mitigation measures' costs	Mass disconnects, compatibility & effectiveness of mitigation measures
[12]	Computer networks	Contextual	Criteria	Optimisation	ROI, budget	usability
[19]	Hybrid AC/DC Grid	Contextual	Criteria	Optimisation	AC grid frequency & DC voltage deviations, VSC injection states & magnitudes	-
[31]	Computer networks	Contextual	Criteria	Optimisation	Asset value, defense cost	Return on attack
[32]	Cyberattacks on CPS	Contextual	Criteria	Optimisation	Cost of Asset, loss of control and salary	Payoff gain, negative cost effect of countermeasure. Future: operational costs, response time, impact index, impacts on properties, finance & human lives
[11]	Information security	Contextual	Criteria	Optimisation	Implementation cost	Number of threats affected by control
[24]	Information security	General	Analytical	Quantitative policy numbers	-	Attack difficulty
[28]	ICS	General	Criteria	Optimisation	Rank-weight comparison	Maturity indicator level (MIL)
[25]	Information security	General	Criteria	MCA using graph	Implementation cost, Loss from attack	Defence probability
[26]	Smart grids	General	Criteria	Prioritisation	Cost-effectiveness	security effectiveness, scalability, integration & compatibility, performance impact, manageability and usability, compliance & regulatory requirements, resilience & redundancy, vendor support & collaboration, future readiness, network segmentation, patch management, threat intelligence, vendor & supply chain security
[27]	Information security	General	Criteria	Prioritisation	Implementation cost	Perceived ease of use, and effectiveness

References

[1] R. A. Coveney, 'Energy executives expect more extreme cyber-attacks but defensive action is lagging, new DNV research reveals', DNV. Accessed: May 16, 2023. [Online]. Available: https://www.dnv.com/news/energy-executives-expect-more-extreme-cyber-attacks-but-defensive-action-is-lagging-new-dnv-research-reveals-224890

[2] A. Knack, Y. Kam, and K. Tam, 'Enhancing the Cyber Resilience of Offshore Wind', Centre for Emerging Technology and Security. Accessed: Jun. 25, 2024. [Online]. Available: https://cetas.turing.ac.uk/publications/enhancing-cyber-resilience-offshore-wind

[3] St. John, 'Cybersecurity Stats: Facts And Figures You Should Know – Forbes Advisor'. Accessed: Mar. 28, 2024. [Online]. Available: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

[4] C. C. CSRC NIST, 'cyber risk - Glossary | CSRC'. Accessed: Mar. 16, 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_risk

[5] Gartner, 'Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024'. Accessed: Mar. 28, 2024. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

[6] S. Freeman, J. Gentle, and T. Conway, 'Cyber Resiliency Within Offshore Wind Applications', *Marine Technology Society Journal*, vol. 54, no. 6, pp. 108–113, Nov. 2020, doi: 10.4031/MTSJ.54.6.10.

[7] Hayes, 'What Is Cost-Benefit Analysis, How Is it Used, What Are its Pros and Cons?', Investopedia. Accessed: Mar. 16, 2024. [Online]. Available: https://www.investopedia.com/terms/c/cost-benefitanalysis.asp

[8] O. Špačková and D. Straub, 'Cost-Benefit Analysis for Optimization of Risk Protection Under Budget Constraints', *Risk Analysis*, vol. 35, no. 5, pp. 941–959, May 2015, doi: 10.1111/risa.12310.

[9] 'BENEFITS: Qualitative and Quantitative Project Benefits', Fluid.Work Support. Accessed: Jun. 26, 2024. [Online]. Available: https://fluid.freshdesk.com/support/solutions/articles/24000034222-benefits-qualitative-and-quantitative-project-benefits

[10] Moore, 'Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024'. Accessed: Apr. 01, 2024. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl

[11] G. Uuganbayar, A. Yautsiukhin, F. Martinelli, and F. Massacci, 'Optimisation of cyber insurance coverage with selection of cost effective security controls.', *Computers & Security*, vol. 101, p. 102121, Feb. 2021, doi: 10.1016/j.cose.2020.102121.

[12] M. N. Alsaleh and E. Al-Shaer, 'Automated Cyber Risk Mitigation: Making Informed Cost-Effective Decisions', in *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Eds., Cham: Springer International Publishing, 2020, pp. 131–157. doi: 10.1007/978-3-030-33432-1_7.

[13] A. Dutta and E. Al-Shaer, '"What", "Where", and "Why" Cybersecurity Controls to Enforce for Optimal Risk Mitigation', in *2019 IEEE Conference on Communications and Network Security (CNS)*, Jun. 2019, pp. 160–168. doi: 10.1109/CNS.2019.8802745.

[14] M. N. Alsaleh, 'ROI-Driven Cyber Risk Mitigation Using Host Compliance and Network Configuration | Journal of Network and Systems Management'. Accessed: Feb. 13, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10922-017-9428-x

[15] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, 'Decision support approaches for cyber security investment', *Decision Support Systems*, vol. 86, pp. 13–23, Jun. 2016, doi: 10.1016/j.dss.2016.02.012.

[16] M. N. Alsaleh, G. Husari, and E. Al-Shaer, 'Optimizing the RoI of cyber risk mitigation', in *2016 12th International Conference on Network and Service Management (CNSM)*, Oct. 2016, pp. 223–227. doi: 10.1109/CNSM.2016.7818421.

[17] A. B. Kayode and A. O. Ajoke, 'Cost-Benefit Analysis of Cyber-Security Systems', 2016.

[18] P. Żebrowski, A. Couce-Vieira, and A. Mancuso, 'A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems', *Risk Analysis*, vol. 42, no. 10, pp. 2275–2290, 2022, doi: 10.1111/risa.13900.

[19] J. Hou, S. Lei, Y. Song, L. Zhu, W. Sun, and Y. Hou, 'The Cost and Benefit of Enhancing Cybersecurity for Hybrid AC/DC Grids', *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4758–4771, Nov. 2023, doi: 10.1109/TSG.2023.3255250.

[20] M. Mccarty *et al.*, 'Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment', *IEEE Access*, vol. 11, pp. 15297–15313, 2023, doi: 10.1109/ACCESS.2023.3244778.

[21] D. W. Woods and R. Böhme, 'SoK: Quantifying Cyber Risk', in *2021 IEEE Symposium on Security and Privacy (SP)*, May 2021, pp. 211–228. doi: 10.1109/SP40001.2021.00053.

[22] I. D. Sánchez-García, T. S. Feliu Gilabert, and J. A. Calvo-Manzano, 'Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review', *Computers & Security*, vol. 128, p. 103170, May 2023, doi: 10.1016/j.cose.2023.103170.

[23] N. Mouter, M. Dean, C. Koopmans, and J. M. Vassallo, 'Chapter Seven - Comparing cost-benefit analysis and multi-criteria analysis', in *Advances in Transport Policy and Planning*, vol. 6, N. Mouter, Ed., in Standard Transport Appraisal Methods, vol. 6. , Academic Press, 2020, pp. 225–254. doi: 10.1016/bs.atpp.2020.07.009.

[24] W. Pieters, C. W. Probst, Z. Lukszo, and L. Montoya, 'Cost-effectiveness of security measures: A model-based framework'.

[25] I. Lee, 'Cybersecurity: Risk management framework and investment cost analysis', *Business Horizons*, vol. 64, no. 5, pp. 659–671, Sep. 2021, doi: 10.1016/j.bushor.2021.02.022.

[26] A.-A. Bouramdane, 'Cyberattacks in Smart Grids: Challenges and solving the Multi-Criteria Decision-Making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process', *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 662–705, 2023.

[27] R. Alexander, 'Using the Analytical Hierarchy Process Model in the Prioritization of Information Assurance Defense In-Depth Measures?—A Quantitative Study', *Journal of Information Security*, vol. 8, no. 3, Art. no. 3, Jul. 2017, doi: 10.4236/jis.2017.83011.

[28] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, 'Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis', *Future Generation Computer Systems*, vol. 105, pp. 410–431, Apr. 2020, doi: 10.1016/j.future.2019.12.018.

[29] J. D. Bewley, R. Zhang, T. Charton, and R. Wilson, 'Prioritisation and cost / benefit analysis of cyber security controls within existing operational technology environments', in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, Liverpool, UK: Institution of Engineering and Technology, 2020, p. 6 pp.-6 pp. doi: 10.1049/cp.2020.0033.

[30] P. J. Hueros-Barrios, F. J. Rodríguez Sánchez, P. Martín, C. Jiménez, and I. Fernández, 'Addressing the cybersecurity vulnerabilities of advanced nanogrids: A practical framework', *Internet of Things (Netherlands)*, vol. 20, 2022, doi: 10.1016/j.iot.2022.100620.

[31] S. Y. Enoch, C. Y. Moon, D. Lee, M. K. Ahn, and D. S. Kim, 'A practical framework for cyber defense generation, enforcement and evaluation', *Computer Networks*, vol. 208, p. 108878, May 2022, doi: 10.1016/j.comnet.2022.108878.

[32] H. A. Kholidy, 'Autonomous mitigation of cyber risks in the Cyber–Physical Systems', *Future Generation Computer Systems*, vol. 115, pp. 171–187, Feb. 2021, doi: 10.1016/j.future.2020.09.002.