Chapter 1
The economic perspective on cybersecurity

JEANNE C.M. VALLETTE D'OSIA, ELENA RAGAZZI, UGO FINARDI

CNR-IRCrES, Consiglio Nazionale delle Ricerche – Istituto di Ricerca sulla Crescita Economica Sostenibile, Strada delle Cacce 73, 10135 Torino, Italia

Corresponding author: jeannecharlottemarievallettedosia@cnr.it

ABSTRACT
This chapter of the Quaderno IRCrES *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* reviews the literature on two main aspects, the concepts on which the economic analysis of cybersecurity is built on, and the methods, both theoretical and empirical, developed to assess the value of cybersecurity. Itis therefore divided in two parts. First, regarding the broad perspective of economics applied to cybersecurity, we tackle the discussion on the nature of cybersecurity as a public good, the market failures hampering the right allocation of resources within investment in cybersecure systems, and thus, the regulation policies and general awareness on the topic. Then, we review the approaches and models developed for cybersecurity estimations, followed by a focus on the studies addressing cybersecurity's value within critical infrastructure sectors. The review demonstrates a literature on the topics of cybersecurity economics already significant, revealing different schools of economics employed in cybersecurity, as well as multidisciplinary approaches and, in turn, various models for cybersecurity investment. Yet, developing economically viable cybersecurity strategies still calls for representative data on cyberattacks as well as the adaptation of evaluation techniques to individual behaviours, and system's complexity.

KEYWORDS: Cybersecurity, critical infrastructures, public good, market failures, estimation methods.

DOI: 10.23760/2499-6661.2025.24_01
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
Vallette d'Osia, J.C.M., Ragazzi, E., & Finardi, U. (2025). The economic perspective on cybersecurity. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 11-25). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_01

This chapter reviews and discusses a selection of research works related to the economic evaluation of cybersecurity. In specific, the first section covers the topics of the purposes, problems, and challenges of the economic analysis of cybersecurity, the challenges related to protecting the continuity of electricity service, and the regulation and awareness of socioeconomic factors. The second section delves deeper into the specific issue of estimating the value of cybersecurity. Consequently, it discusses the approaches and models developed to understand the economic value of cybersecurity and the evaluation of cybersecurity for critical infrastructures.

1 PREVIOUS RESEARCH ON THE ECONOMIC VALUE OF CYBERSECURITY

Economic studies tackle numerous topics related to the economic evaluation of cybersecurity. A non-exhaustive list of the main topics can be outlined as follows:

1. Economic studies on the appropriate level of investment in cybersecurity. These studies combine economic and engineering approaches to highlight the correct balance between investment in cybersecurity and expenditure, considering the diminishing marginal levels of cybersecurity with linearly increasing costs. The literature is eminently empirically driven.
2. Studies on the economic aspects related to regulation and policies for cybersecurity.
3. Studies related to cybersecurity metrics, both in terms of identifying economic metrics and considering the metrics themselves as leverage points for proper corporate or regulatory management of cybersecurity. Also in this case, the papers have an interdisciplinary focus, with numerous references to engineering and computer science.

However, most of these topics, along with others not explicitly listed, fall outside the specific focus of this work, which instead concentrates on the specific issue of evaluating and measuring the value assigned to cybersecurity by end-users. This is a specific topic aimed at providing data and evidence functional to policy design and the fine-tuning of regulation, and which can therefore, at least in a broad sense, fall into group 2.

This section will address some topics relevant to our discussion. It will begin with an analysis of the scientific literature related to the purposes, problems, and challenges of the economic analysis of cybersecurity (in general, regardless of the sector of application). The second subsection, in turn, will examine the topic of regulation and awareness of the socioeconomic aspects of cybersecurity.

1.1 Purposes, problems and challenges of the economic analysis of cybersecurity

The concept of cybersecurity has long been associated with the protection of Information Technology (IT) structures and the data they transmit, manage, and store, thus defining a set of predominantly technical studies. However, the complexity of its evolution and its crucial role in sectors such as electricity production and distribution have generated new challenges regarding understanding its value and the proper allocation of resources for its implementation. Cybersecurity also deals with protecting data from malicious use by third parties. Aligning with this view, Craigen, Diakun-Thibault & Purse (2014) define cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (p. 17).

Since the academic field of cybersecurity is highly interdisciplinary, it is treated and discussed in numerous scientific sectors, approached through themes such as risk management, prevention, or public cybersecurity. The perspective and context in which it is studied influence its interpretation: the more or less pronounced characteristics of a public good with which it can be characterized depend precisely on the context.

In market-driven contexts, such as industrial sectors where data protection is closely tied to corporate strategies (i.e. companies for which information is a strategic input), sectors where reputation is an essential competitive factor (e.g. banks), or sectors where cybersecurity is offered as an intrinsic feature of a sold product (i.e. when equipment is acquired with embedded cybersecurity), cybersecurity can be treated as a private good. However, in contexts such as national security or critical infrastructures, where legal, social, and ethical issues are at stake, the concept of cybersecurity as a public good better applies. Kianpour, Kowalski & Øverby (2022), advance the concept of cybersecurity as public good performing an agent-based modelling experiment. In this way they demonstrate that an important challenge for society as a whole is posed by the presence of free-riders, that is, actors who benefit from a (public) good without contributing to it, weakening the development and stability of the society of information.

This perspective is extended by Taddeo (2019). Her work emphasizes the concept that critical infrastructures are enabled by the presence of robust systems, i.e., by those digital and information infrastructures that can remain functional notwithstanding the presence of attacks, or of errors. In this way they enhance social stability. The author studies data on cyberattacks, associating them with the specific state of cybersecurity, and then suggesting that cybersecurity should be framed within the scope of public good. Treating it as a club good (that is, the case of a good for which access is regulated by a cost, and thus excludable, but which is not rivalrous) in fact would not allow to consider properly its social implications. Nevertheless, the same author also put forward situations where cybersecurity is not a public good. It is the case of system resilience, which might undermine the privacy of users. The author concludes that "considering some of digital technologies or uses […] as public good will be a step in the right direction insofar as it done cautiously and to support policy and governance approaches that will foster tolerant […] and stable information societies" (p. 353, passim).

The role of governments in establishing contexts able to enhance cybersecurity, particularly supporting public cybersecurity is put forward by Asllani, White & Ettkin (2013), who compare cybersecurity with safety as a public good. The authors conclude that cybersecurity needs collective actions at all administration levels, besides a personal and organizational effort, in order to reach protection at national security level. Another parallel is performed by Mulligan & Schneider (2011) who propose treating cybersecurity as a public good adopting mechanisms similar to those used for public health. The target of public health, as well as of cybersecurity, is achieving a positive situation in a highly interdependent network. Moreover, authors highlight that the value of cybersecurity remained at the time of their work largely undetermined. In fact, both enterprises and clients were (and still are in most cases) neither able to attribute a price to confidentiality and integrity of information nor able to estimate the cost of the recovery from the effects of a cyberattack.

This first introductory step of our review, being a discussion of the public/private good dichotomy applied to cybersecurity, aims to help foster a better understanding of the core argument, as well as the related market failures highlighted by the economic losses generated by informatic violations. Moore (2010) in discussing the economics of cybersecurity, describes some important economic challenges: information asymmetries, misaligned incentives, and externalities. These three are relevant features of market failures, and as such deserve to be discussed.

The concept of misaligned incentives refers to situations where, in a transaction, the objectives of the different parties do not coincide. For example, a company may pay its subcontractors a fixed fee to secure their work, but the subcontractors may fail to complete the work on time precisely because of the certainty of receiving a fixed income.

Information asymmetries arise when, in an economic relationship, not all parties are aware of the same information. A typical case of information asymmetry is real estate transactions, where one party (the seller) is aware of all the information about the property's condition (including any structural or legal issues) that may not be disclosed to the buyer.

Externalities, finally, are defined as the effects of an activity that falls on an external party without the agent receiving compensation (positive externalities) or, conversely, that the party suffering harm receives compensation (negative externalities). A typical case of the former is knowledge spillovers, where those who produce knowledge, for example by studying a new production technology, see their invention partially exploited by others without receiving compensation. Note that knowledge is a classic example of public good. A typical case of the latter is environmental issues, where, for example, a company that pollutes via its production process causes harm to the surrounding residents without them receiving compensation.

When dealing with information asymmetries, Moore (2010) underlines the fact that firms are not incentivized in sharing information, in particular when violations are involved, due to the possible problems in reputation or in exposing own vulnerabilities. This causes, in turn, a lack of reliable and transparent data, which might cause therefore a suboptimal level of investment in cyber protection. The context of insufficient circulation of information on cyberattacks, thus, might cause an incorrect allocation of resources regarding firms both using and producing cybersecurity assets. Organizations, in fact, might underestimate incidents and vulnerabilities; security system sellers, by their side, might invest at suboptimal level in reliable security measures, in particular if customers might not be willing to pay a price for protection. This, in turn, might create a situation where investments are misaligned with effective risk.

Accounting and market data can be used to measure the correlation existing between cybersecurity practices and firm performance. This strategy was followed by Al Amosh & Khatib (2024) on a sample of firms quoted in the Australian stock market. Results show a positive impact of increased cybersecurity disclosure on the performance. Transparency mitigates information asymmetry and consequently reduces conflicts between management and stakeholders. Information asymmetries existing between sellers and buyers engaged in electronic transactions can distort the security levels from those deemed adequate. This thesis is demonstrated by Nagurney & Nagurney (2015) through a game theory model.

A further challenge to the cybersecurity economy is relative to the presence of externalities. Different types of externalities can take place: for instance, network externalities, externalities of insecurity, and interdependent security (Moore, 2010). Network externalities depend on the growing benefit for each network member at the growth of the network dimension. This in turn causes a growth in the net value of the platform, favouring dominant firms. Network externalities might explain the presence of unsafe operating systems, as the competition among sellers arises before an emphasis on security is set. Moreover, security of an internet protocol depends also on the prompt update of one's system by part of all users once a problem arises. On the other side externalities of insecurity issues are generated when compromised sites endanger other ones. For instance, botnets cause more social than private losses, since their objective is not the single, network-connected PC, but routers and web servers. This fact might cause further underinvestment protection against social risk. Last but not least, interdependent security takes place when some actors benefit from protective actions put in action by other ones. This might cause freeriding and underinvestment.

Finally, as previously mentioned, the interdependence of security occurs when protective actions benefit some actors but may simultaneously discourage their investments, leading to a free-riding situation. Investments in security can also be discouraged by situations where the resilience of an entire network is equal to that of its weakest link: in a situation where companies are interconnected, they are discouraged from investing in security if they know that others are not doing so either. This, in turn, creates vulnerabilities at the network level.

Cybersecurity presents some features of public good that exacerbate the problem of incentives misalignment, notwithstanding the fact that security decisions are mainly taken by market actors. Bauer & van Eeten (2009) studied a methodology to understand how the markets of cybercrime and cybersecurity coevolve. In this way they examine the offer of security incentives for different stakeholders, in the context of interdependent communication and information systems. Interviewed actors in this context show conflicting incentives, as well as hindering externalities. The authors emphasize that actors in an ICT (Information and Communication Technology) ecosystem, such as internet service providers or software vendors, have in some cases expressed conflicting incentives. Moreover, in cases where the same actors shared common incentives toward improving security, these were hindered by the presence of externalities, since "end-users perceive no incentive to secure their machines" (p. 714).

Dacus & Yannakogeorgos (2016) also elaborate an incentive structure apt at motivating defence cybersecurity agents to put a larger effort into securing their environments. The authors underline also the fact that information asymmetries (different priorities between cybersecurity service suppliers and customers) and incentive misalignment (misaligned motivations between the two) can generate moral hazard. In other words, this can happen when the priorities of cybersecurity service providers differ from those of their clients, and when their motivations are not aligned. In their case study, related to contractual operators of the U.S. Department of Defense, the effort dedicated to security codes or network defence is lower than desired by the government.

In conclusion, cybersecurity presents characteristics and social implications similar to those of public security or public health, which are commonly defined as “public goods”. Moreover, the economic challenges, specifically misaligned incentives, information asymmetries, and externalities, of cybersecurity lead to market failures, limiting the optimal level of investment in secure systems. In addition to causing an underestimation of the concept of cybersecurity as a public good, these market failures highlight the need for public intervention.

1.2 Regulation and awareness of socioeconomic aspects

An emblematic case in terms of public intervention to mitigate market failures as well as cyber risk is that of the General Data Protection Regulation (GDPR)[1] implemented in the European Union. Aimed at harmonizing the legislation on data protection at the global level (for every Member State of the European Union) in 2016, the GDPR has since been criticized for imposing a significant administrative burden, particularly due to extensive bureaucratic requirements. This, in turn, stems from a lack of transparency in the logic underlying some provisions, even in cases where data usage is easily understandable. In this context, Li et al. (2023) conducted a systematic review of empirical evidence on the evaluation and revision of the GDPR. Their synthesis mentions other common criticisms of the GDPR, such as the lack of enforcement against big tech companies, the inadequacy of imposed sanctions, and design flaws (including for instance excessive reliance on consent). Although the GDPR is far from being a general failure, their work shows that the complexity and internal contradictions among its various components can lead to conflicts and inefficiencies during implementation.

It is instead Moore (2010) who examines two different regulatory approaches to cybersecurity, the ex-ante and the ex-post strategies, as possible solutions to the economic barriers it must face. Ex-ante strategies entail the proactive adoption of security policies by the firms. The lack of information on risks or standards (in particular in a continuously evolving horizon) makes often this approach ineffective. Ex-post strategies, on the other hand, design regulation considering firms as responsible for failures and adverse outcomes. The problem here is that of unreliability and immaturity of firms towards implementing adequate prevention strategies, or of lack of financial capability to refund damages. To address these shortcomings, Moore proposed improving information disclosure to reduce information asymmetry, which must be considered the main obstacle to effective regulation. He also argued that information disclosure can motivate companies to improve their practices, support the common right to knowledge, and create publicly available data on security incidents. This, in turn, could foster collective awareness. Despite these benefits, it is important to note that, as demonstrated by the GDPR experience, the presence of regulations is not sufficient to achieve full disclosure of cyberattack information by companies. As discussed in the previous section, misaligned incentives among different parties, fear of losing trust and reputation, and the increased risk of hackers exploiting disclosed information to discover system vulnerabilities all significantly hinder the disclosure of specific attack information. Therefore, disclosure cannot be considered a condition for regulatory effectiveness but must itself be the subject of regulation and incentivization, also leveraging the results of research activities on information technologies for secure data sharing.

[1] G.D.P. Regulation (GDPR) (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). (OJ L 119, p. 1-88).

A more precise and relevant field to study for the purpose of this Quaderno is the regulation of cybersecurity within the electricity sector as the final aim is to understand the value of cybersecurity when it comes to electricity supply.

The introduction of new forms of regulation, distinct from state ownership and monopoly control, for the electricity sector, is a relatively recent development. It is not only justified by the essential nature of the service for daily life and the fact that electricity is a strategic input for all production processes; as long as this service was managed by vertically integrated companies directly or indirectly controlled by the state, regulation was minimal, and priority management occurred through executive acts. Only with the start of the privatization process and the introduction of competition in certain stages of the process did it become necessary to produce regulations (defining foundational principles) and technical regulatory acts (what is required of market operators) and economic acts (in simple terms, "who pays for what") to protect collective social and economic interests. The issue of cybersecurity became the subject of this regulatory activity somewhat out of order on the basis that most facilities are now managed through remote controls.

Technical regulation is based on a series of prescriptions derived from the state of the art of technological knowledge, but it often neglects to consider the implications that economic and human aspects, such as costs or awareness, can have on the implementation process. For example, when the NERC-CIP standard was imposed as mandatory for electric operators in North America, the cost of compliance for less mature operators proved to be extremely high, to the point that some reportedly preferred to pay the substantial fines imposed on non-compliant entities rather than immediately bear the cost of compliance.

Regulation of the electric power systems is particularly needed in those situations where the different components – production, transmission, distribution – are unbounded and subject to the free market. In this situation the strategic nature of electricity compels policy makers to regulate the market, as well as the technical issues. The presence of norms, defining fundamental principles, technical regulations, defining what market operators must do, and economic regulations, defining who pays for what, ensures the protection of collective social and economic interests. Cybersecurity is obviously one of the objects of such normative activity, due to its strategic nature in the contemporary context of dependence of critical infrastructures from cyber networks. In these contexts of competition and free market the task of regulating energy markets is entrusted to specific bodies which, together with other tasks, also have to deal with the regulation of cybersecurity.

These facts suggest that policymakers should carefully balance regulatory demands with sector-specific incentives, paying particular attention to situations where short-term costs (especially those borne by companies) may outweigh long-term benefits (especially systemic ones). There is a need for regulatory frameworks that enforce compliance with rules but also create positive incentives for utilities to invest in long-term resilience and innovation. Indeed, this would improve both economic efficiency and system reliability.

A specific work on the topic of cybersecurity regulation within the electricity sector has been undertaken by Ragazzi, Stefanini, Benintendi, Finardi & Holstein (2020) who elaborated a set of guidelines for energy regulators. The authors highlighted two main typologies of regulation that regulators can use in order to regulate investments in cybersecurity. The first one is the Performance-based regulation (PBR). PBR is based on incentives, as it emphasizes the achievement of specific results, measured with the use of metrics. Regulators establish ex-ante target results of security, while operators design strategies apt at achieving the target, which are verified ex-post. The second one is the Cost-of-service regulation. In this case regulators identify ex-ante protection strategies and then approve the strategic plans of the utilities, which make expenses. PBR entails the presence of mature operators, able to self-protect their assets. Cost of service, on the other hand, while assuring coverage of expenses leaves the decision of the protection strategy to the regulator. PRB can be also designed to reduce operational costs and promote efficiency of service and investments, as well as energy efficiency.

These results are outlined by Brown & Sappington (2023) in their assessment of the impact of incentive-based regulations in the electricity sector. The assessment is performed by observing the effects of PBR on items such as network reliability, efficiency of investments on the network, or promotion of environmental objectives.

Leszczyna (2019), in his work "Cybersecurity in the Electricity Sector", outlines guidelines for a systematic approach to cyber protection in electrical system facilities. In this work, the author emphasizes how a lack of awareness among stakeholders in the electricity sector can have negative impacts. For example, he explains how the acceptance of significant investments in secure and reliable technologies depends on the awareness, among both company managers and consumers, of the benefits, costs, and risks associated with modern electricity systems. Indeed, regulators will find it more difficult to approve increases in electricity tariffs aimed at enhancing the cybersecurity of electrical systems when consumers are unaware of the importance of more secure technologies, which are consequently linked to higher energy prices. The same author argues that to efficiently protect the IT resources of entities, consumers must take their role as active observers seriously (i.e., being able to report unusual activities), and employees must be aware of the potential risks associated with their activities. These behaviours can be fostered through appropriate training interventions within companies and adequate consumer information and awareness tools. The data collected through the survey methodology presented in this report can also be used to understand such awareness in the population and, if collected systematically through repeated surveys over time, the effectiveness of awareness campaigns.

Another problem related to the lack of awareness lies in the accountability and evaluation of regulators. For example, there is no performance evaluation framework for the Data Protection Authorities (DPAs) of the GDPR. Buckley, Caulfield & Becker (2024) have studied what professionals consider to be the objectives of data protection regulators and how their efficiency is evaluated. The results show a discrepancy between the presumed objectives attributed to regulators and the criteria used to evaluate them in current practice.

To sum up, the GDPR exemplifies the challenges of public intervention in cybersecurity, revealing the need for an harmonious legal framework as a condition for a European market for data while generating important administrative burdens and implementation inefficiencies. Especially in the sector-specific case of the electricity industry, the public good characteristics of cybersecurity motivate the need for regulation as well. More precisely, regulatory strategies must address the core issue of information asymmetry. First, regulated entities often possess better information than regulators regarding the actual conditions of industrial sectors. Consequently, especially in mature electrical systems like Italy's, regulatory methods must be designed to induce regulated companies to use their information to achieve regulatory objectives and beyond. A second consideration must be made on the issue of risk awareness within the different parts of regulated organizations, which is a necessary condition for an efficient regulatory framework. The broad scope of these challenges suggests significant parsimony in regulatory production, especially in mature electrical systems, considering the possibility of acting on other levers, such as the valorisation and promotion of technological innovations, participatory approaches for sharing regulatory objectives with regulated entities, or the collaborative construction of guidelines.

2 METHODS TO MEASURE AND UNDERSTAND THE ECONOMIC VALUE OF CYBERSECURITY

This section enters more deeply into the core of this review. Its purpose, in fact, is to discuss the different approaches dealing with the problems of the economic evaluation of cybersecurity. In doing so, it reviews the content of a selection of works, trying to describe the state-of-the-art of scientific research on the topic of the economic value of cybersecurity. As the following of this section will show, several methods apt at this scope exist. These methods entail different models of cost and investment estimation. A part of such models is theoretical and concentrated on specific aspects. Nevertheless, they are still noteworthy for their contribution to the general framework. An initial introductory subsection will describe the existing approaches and models aimed at understanding this value. The second subsection, on the other hand, will go into greater detail by addressing the challenges of evaluating cybersecurity for critical infrastructures, with particular attention to those in the electrical system. Table 1 summarizes the literature review, highlighting the approaches and main contributions of each selected study.

2.1 Approaches and models for understanding the economic value of cybersecurity

This section provides a review of selected works aimed at describing the state of the art in scientific production on the topic of the economic value of cybersecurity. Currently, there is a wide range of methods useful for this purpose, implemented primarily through various investment models and cost estimations of cybersecurity. Many of these models are theoretical, developed using game theory approaches, and focus on very specific aspects, which are nonetheless noteworthy for their contribution to the general picture.

Both Haapamäki & Sihvonen (2019) and Kianpour, Kowalski & Øverby (2021) have conducted literature reviews on the topic of cybersecurity.

Kianpour et al. (2021) adopt a broader perspective. Doing so, they examine the economics of cybersecurity as an interdisciplinary field and highlight its evolution toward dynamic and generalizable models. Indeed, they categorize the models into four different approaches: financial analysis, microeconomics, managerial approaches, and combinatorial approaches. Financial analysis often employs theoretical decision-making methods based on traditional risk assessment but is limited by its inability to capture the strategic nature of cybersecurity. It is often considered that game theory models, part of the microeconomic approach, are more robust. This is so because these methods account for interactions between companies and those carrying out strategic attacks or interdependent organizations. The authors also highlight a limitation of game theory models, which aim to maximize utility while practical cybersecurity decisions must also address cyber risk mitigation, compliance, profitability requirements, and cultural adaptation.

As for Haapamäki & Sihvonen (2019), they focus on the topic of accounting, organizing the work around specific themes: cybersecurity and information sharing, investments in cybersecurity, internal audits and cybersecurity controls, disclosure of cybersecurity activities, and security threats and breaches.

Despite their different focuses, both articles emphasize the critical need for practical insights aimed at improving decision-making for professionals and policymakers. Both also highlight the value of interdisciplinary approaches and demonstrate how the interaction between operational and macroeconomic considerations is crucial in defining effective cybersecurity practices.

To grasp the diversity of disciplines seeking to elicit the economic value of cybersecurity, the analysis of these theoretical approaches will primarily focus on game theory-based articles that analyse specific aspects and obstacles to cybersecurity, as explained in Section 1.1, and secondarily on studies adopting risk management approaches, which include both the topic of optimal amount of investments as well as strategic and organizational issues regarding how firms deal with cybersecurity risks.

In the realm of game theory, Nagurney & Nagurney (2015) developed a game theory model applicable in cases of information asymmetry. More specifically, their model applies to electronic transactions between sellers and buyers at the time of product purchase. Sellers are aware of their investment in cybersecurity, while buyers are only aware of the average security of sellers. Additionally, sellers compete with each other by maximizing their expected profits and investing in cybersecurity. However, it should be noted that their model does not consider the impacts of imposing minimum requirements, for example, by a regulatory body.

Companies that are part of an interconnected network are vulnerable to the propagation of third-party risk through weak nodes in supply chains. Therefore, Dash, Sarmah, Tiwari, Jena & Glock (2024) studied the optimal cybersecurity investment strategy in a two-tier supply chain. To this end, they examined a model where retailers are interconnected with a single supplier. This work is also based on game theory and aims to improve companies' ability to manage complexities in practical situations. Consequently, they explore the possible connections between different types of cyberattacks, the interconnected nature of companies, and the role of mandatory cybersecurity insurance. The results confirm that optimal levels of cybersecurity investment are higher in the case of targeted attacks, such as denial of service or website defacement, compared to opportunistic attacks, such as spam emails or viruses.

For instance, also Ghadge, Weiß, Caldwell & Wilding (2019) deal with cyber risk in supply chains from another perspective. In order to respond to their research question on “how can organisations manage cyber risk on supply chains?” (p. 224) they perform a systematic literature review with an apt methodology, and a thematic analysis of the reviewed works. As a result, authors propose an integrated model of cybersecurity and advocate the role of organization processes in this model.

For their part, Franco, Künzler, von der Assen, Feng & Stiller (2024) developed a metric called “Real Cyber Value at Risk” (RCVaR). It is based on real information from public cybersecurity reports. This information is used in combination with economic methods to predict the costs and risks associated with cyberattacks on companies. This approach provides individualized and quantitative monetary estimates of the impacts of cybersecurity and addresses the limitations of the original CVaR metric, initially proposed by the Cyber Resilience Initiative of the World Economic Forum in 2015. In particular, the RCVaR metric addresses the drawback of probability-based estimates induced by CVaR by conducting cost and risk estimates for real organizations.

The quantification and communication of cyber risk should be carried out through quantitative methods. This idea underlies the work by Bentley, Stephenson, Toscas & Zhu (2020). Their article addresses two specific gaps in literature. The first concerns the lack of use of open data on cyber incidents, while the second concerns the lack of quantitative research on the effect of mitigation strategies. Their first model is therefore adapted to “real-world” data. The authors, in fact, developed a multivariate model that quantifies losses resulting from cybersecurity risks. In specific, this model accounts for different types of attacks and the interdependence between them. Additionally, the authors constructed a second model in this work. This second model aims to separate the frequency and severity of attacks to focus instead on the effect of different mitigations. This approach is extremely useful for professionals and policymakers who wish to optimize mitigation strategies toward specific objectives.

Wang, Neil & Fenton (2020) also propose a quantitative model for cyber risk assessment. In this article, the authors develop an extension of the existing Factor Analysis of Information Risk (FAIR) model (Jones, 2006) to make it more flexible and extensible. The FAIR model alone provides a methodology and tool for calculating and analysing cyber risk. However, the model has limitations in managing causal reasoning for all types of defence-attack contexts and in dealing with different statistical distributions and functions. To address these issues, the authors implemented the FAIR model using Bayesian Networks (FAIR-BN). These networks are known for their broad applicability in probabilistic reasoning. Furthermore, they constructed a combined approach incorporating a process-oriented model and a defence-attack game, called Extended FAIR-BNs (EFBNs). This series of models allowed them to remain consistent and compatible with the original model while providing better insights into the causal mechanisms underlying cyber events and their associated economic consequences.

A further strategy can be found in the guidelines for managers. It is the case of the work of Lee (2021) who develops a cyber risk management instrument. This instrument is organized into four levels, relative to the “cyberecosystem layer” (the external cyber-environment), the “cyberinfrastructure layer” (technological and human aspects of cybersecurity management), the “cyber risk assessment layer” (risk identification, quantification, analysis) and the “cyberperformance layer” (implementation and improvement). The model highlights the need for organizations to understand not only the internal structure of cybersecurity but also the external environment. In this way, the author provides tools for organizations to increase their awareness of changes in cybersecurity trends at the industry level. Consequently, this enables their response strategies to be faster and more efficient. Finally, the author discusses a cyber risk assessment process and provides a real-world example to illustrate continuous performance improvement and cost analysis for cybersecurity.

In conclusion, this section shows that there is a range of works, not extensive but significant, aimed at discussing economic approaches to security evaluation. However, it is important to emphasize that, within the various specific topics addressed so far, research on the economics of cybersecurity in critical infrastructures remains relatively scarce and scattered across highly differentiated specific topics. This fact must be highlighted given the primary role of critical infrastructures at the societal level. According to Gordon, Loeb, Lucyshyn & Zhou (2015), for example, a cybersecurity breach could shut down an entire sector connected to a critical infrastructure, endangering the entire economy and national defence of a country. This leads us to examine the topic more deeply in the following section.

2.2 Cybersecurity assessment within critical infrastructures

In 2019, the OECD published a report titled Good Governance for Critical Infrastructure Resilience (OECD, 2019). In this report, the OECD defines critical infrastructures as those that enable the delivery of key services in sectors such as telecommunications, energy, water supply, transportation, or finance; these are key systems that represent the “backbone of the functioning of our modern and interconnected societies” (p. 18). The European Union, for its part, defines critical infrastructures as follows: “‘critical infrastructure’ an element, system or part thereof located in the Member States that is essential for the maintenance of vital societal functions, health, safety, security and economic and social well-being of citizens and whose disruption or destruction would have a significant impact in a Member State due to the impossibility of maintaining such functions.”. Additionally, the more restrictive concept of ‘European critical infrastructure’ or ‘ECI’ is also introduced, defined as “critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States” (Council Directive 2008/114/EC, 2008). This definition underscores the transnational nature that certain infrastructures can have. Eleven sectors have been identified (energy, transportation, banking, health, drinking water, wastewater, digital infrastructures, public administration, space, and food production, processing, and distribution) whose infrastructures, falling within this definition, will need to be catalogued by 2026. Among these, energy infrastructures are likely to be the most represented on the list due to their wide-ranging impacts.

Cyberattacks on critical infrastructures, if successful, can have repercussions on society as a whole, even at a transnational level, resulting in significant social costs. At the same time, as reported in the previous section, this may not be the case for entities or companies that are not integrated into large-scale networks. To verify whether the scientific literature has addressed this issue, we will now examine studies that focus on the economic evaluation of cybersecurity in the context of critical infrastructures.

The body of literature studying the economic efficiency of measures aimed at making critical infrastructures more resilient is relatively scarce. To address this gap, Rulleau (2023) uses a Discrete Choice Experiment (DCE), conducted through a survey, to evaluate the preferences of residents of the “Eurometropolis” of Strasbourg (France) regarding the resilience of their drinking water distribution network in the event of a cyberattack. Using an econometric model, the author concluded that most respondents positively valued resilience measures aimed at mitigating some effects of cyberattacks. Another important observation is the lack of knowledge and familiarity among the general public regarding the functioning of the drinking water distribution network. This issue, potentially extendable to other critical infrastructure sectors, could compromise the accuracy of the economic evaluation of cybersecurity in these contexts.

On their side, Lis & Mendel (2019) opt for an approach centred on critical infrastructure system operators. The authors emphasize how cybersecurity implementation efforts should aim to ensure the availability, reliability, efficiency, and self-healing of critical infrastructures. As a tool to achieve these objectives, they propose an application of the Return on Security Investment (ROSI) indicator to evaluate the efficiency of cybersecurity efforts within a critical infrastructure. However, they also highlight that the lack of data on cyberattacks prevents the estimation of the costs and benefits associated with such attacks. Additionally, they propose an organizational methodology, “Identify, Protect, Detect, Respond, and Recover” (IPDRR). This methodology is designed to serve as a guide for critical infrastructure providers and policymakers and “consists of a set of activities and outcomes that are common across the critical infrastructure sector." (p. 38). This framework could also help capture the costs and benefits resulting from cyber breaches. Finally, the authors conclude with a recommendation to implement blockchain technologies to better protect critical infrastructures from cyber threats.

As previously mentioned, the body of literature analysing investment models and cost estimation of cybersecurity in the context of critical infrastructures is not particularly extensive. However, thanks to the interdisciplinary nature of cybersecurity, some studies have approached the problem from other perspectives, such as risk management frameworks (Paté-Cornell, Kuypers, Smith & Keller, 2018; Kure & Islam, 2019). Both works focus on risks quantification rather than cybersecurity value assessment as they stress the importance of systematically identifying and analysing risks and vulnerabilities to protect the organization's key assets.

Addressing another aspect of the economics of cybersecurity in critical infrastructures, Massacci, Ruprai, Collinson & Williams (2016) explored the topic of regulation. To this end, they developed a game theory model that examined the effectiveness of different regulatory systems and the optimal social outcome for public policymakers. This model, linked to public policies on cybersecurity, captures the hybrid nature of regulations for critical infrastructure operators, which vary between risk-based and rule-based systems. The first type of system is based on fines imposed by policymakers in the event of a security breach, leaving operators to decide their own security investment profile. The second, on the other hand, is based on the role of policymakers, who are tasked with conducting a risk assessment and imposing sanctions on operators for non-compliance. The authors clarify that, depending on the combination of incentives, operators might stop investing in cybersecurity and focus solely on compliance (and vice versa). Furthermore, the authors conclude that the maturity threshold of a Critical National Infrastructure Operator (CNIO) is important in choosing the regulatory system. In their view, more mature CNIOs in terms of security should be subject to a risk-based framework, while less secure ones should follow rules.

To summarize, the literature emphasizes the critical importance of cybersecurity measures in ensuring the resilience of critical infrastructures. However, significant challenges remain in quantifying the economic efficiency of such measures, primarily due to the scarcity of representative data on cyberattacks. Regulatory frameworks, through their role in providing risk assessment tools, could help clarify the value of cybersecurity in critical infrastructures.

Since the primary focus of our project is on the specific case of the electricity sector, chapter 4 of this Quaderno IRCrES (Vallette d'Osia, Finardi & Ragazzi, 2025) concentrates on an overview of approaches and methodologies studying the economic value of cybersecurity within that specific sector.

3 CONCLUSIONS

Overall, the reviewed literature highlights that cybersecurity exhibits some features of a public good, creating conditions for market failures such as misaligned incentives, externalities, and information asymmetries. These dynamics justify some form of public intervention. At the same time, the electricity sector provides a particularly complex case: while cybersecurity can be framed as a regulatory concern similar to other dimensions of electricity service (such as service continuity), the design of effective policies is hindered by information asymmetry, a lack of risk awareness, and a lack of a clear regulation typology with accountable and evaluated regulators.

Despite growing recognition of the economic relevance of cybersecurity, contributions that explicitly address the role of cybersecurity in critical infrastructures, and especially in power systems, remain relatively limited. This is notable given the systemic importance of such infrastructures. Furthermore, while the literature emphasizes the resilience benefits of cybersecurity, the economic value of protective measures remains difficult to assess, largely due to limited availability of data on cyber incidents and their impacts.

Taken together, these insights suggest that future research and policy must focus on better integrating economic analysis into the study of cybersecurity in critical infrastructures. This involves not only addressing persistent information asymmetries and data gaps (which could prove impossible in real world conditions) but also exploring regulatory and collaborative approaches that foster innovation, risk awareness, and efficient investment in security. By doing so, the field can move toward a more systematic understanding of the value of cybersecurity and its essential role in safeguarding critical infrastructures.

Table 1. Summary of analyzed studies regarding the economic value of cybersecurity

Study	Approach	Main contribution
Section 2.1. Approaches and models for understanding the economic value of cybersecurity		
Haapamäki & Sihvonen (2019)	Systematic literature review	Focus on accounting, identifies a framework made of 4 research themes: cybersecurity and information sharing, investments in cybersecurity, internal audits and cybersecurity controls, disclosure of cybersecurity activities, and security threats and breaches.
Kianpour, Kowalski & Øverby (2021)	Systematic literature review	Critical assessment of the literature on economics of cybersecurity, under 4 approaches: financial analysis, microeconomics, managerial approaches and combinatorial approaches. Cybersecurity is an interdisciplinary field evolving towards dynamic and generalizable models.
Ghadge, Weiß, Caldwell & Wilding (2019)	Systematic literature review	This work investigates cyber risk management in supply chain contexts and develops a conceptual model of cybersecurity. Authors advocate raising risk awareness, standardized policies, collaborative strategies and empirical models for creating supply chain cyber-resilience.
Nagurney & Nagurney (2015)	Game theory model	Authors build a model applicable in cases of security information asymmetry which provides the equilibrium product transactions between sellers and buyers (on the Internet), and the security levels of the sellers.
Dash, Sarmah, Tiwari, Jena & Glock (2024)	Game theory model	This paper explores the possible connections between different types of cyberattacks, the interconnected nature of companies, and the role of mandatory cybersecurity insurance. The results confirm that optimal levels of cybersecurity investment are higher in the case of targeted attacks, compared to opportunistic ones.
Franco, Künzler, von der Assen, Feng & Stiller (2024)	Quantitative metric, "Real Cyber Value at Risk"	The authors predict the costs and risks associated with cyberattacks on companies. This approach provides individualized and quantitative monetary estimates of the impacts of cybersecurity and addresses the limitations of the original CVaR metric shift from probability estimations to quantitative data computation).
Bentley, Stephenson, Toscas & Zhu (2020)	Quantitative model for risk assessment	Investigates different types of cyber incidents and the effect of mitigation strategies. The best mitigation strategy depends on whether the objective is to avoid extreme damages or to reduce average losses. The methodology allows for estimating the costs of cyberattacks and provides guidance in selecting the most effective mitigation measures.

Wang, Neil & Fenton (2020)	Quantitative model for risk assessment	Extension of a model that provides a methodology and tool for calculating and analyzing cyber risk. Provides both a methodology and a tool for cybersecurity risk analysis and calculation.
Lee (2021)	Quantitative model for risk assessment	Proposes a cyber risk management framework based on 4 layers (cyber ecosystem / cyber infrastructure / cyber risk assessment / cyber performance), which gives tools for organizations to increase their awareness of changes in cybersecurity trends at the industry level.
Section 2.2. Cybersecurity assessment within critical infrastructures		
Rulleau (2023)	Discrete Choice Experiment	This article presents an assessment of the preferences of individuals regarding the resilience of their drinking water distribution network which is subject to a cyber-attack. The results show: - a lack of knowledge and familiarity with the functioning of the distribution network might compromise the accuracy of economic valuation exercises, - regarding individual characteristics, the main factors influencing choices are linked risk perception, - desirability of mitigating measures against cyber-attacks.
Lis & Mendel (2019)	Return on Security Investment (ROSI) quantitative indicator & organizational risk management framework	Provides a methodology and recommendations to follow for blockchain technologies for critical infrastructure providers and policymakers to capture the costs and benefits resulting from cyber breaches.
Paté-Cornell, Kuypers, Smith & Keller (2018)	Quantitative model for risk assessment	Proposes a general cyber risk analysis framework with its application through three examples (database analysis, smart grid optimization, dynamic software management), showing how to quantify risks and identify optimal mitigation strategies.
Kure & Islam (2019)	Conceptual risk management framework	Focuses on three major aspects of risk management (assets identification, vulnerability, and threat assessment and risk identification) and uses an example from the SCADA system of a power grid.
Massacci, Ruprai, Collinson & Williams (2016)	Game theory model	Discusses the effectiveness of different regulatory systems for critical infrastructure operators and the optimal social outcome for public policymakers.

4 BIBLIOGRAPHY

Al Amosh, H., & Khatib, S.F.A. (2024a). Cybersecurity Transparency and Firm Success: Insights From the Australian Landscape. *Australian Economic Papers*, *64*(2), pp. 189-204. https://doi.org/10.1111/1467-8454.12385

Asllani, A., White, C.S., & Ettkin, L. (2013). Viewing cybersecurity as public good: the role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues*, *16*(1), pp. 7-14.

Bauer, J.M., & Van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10-11), pp. 706-719. https://doi.org/10.1016/j.telpol.2009.09.001

Bentley, M., Stephenson, A., Toscas, P., & Zhu, Z. (2020). A Multivariate Model to Quantify and Mitigate Cybersecurity Risk. *Risks*, *8*(2), art. 61. https://doi.org/10.3390/risks8020061

Brown, D.P., & Sappington, D.E.M. (2023). D*esigning Incentive Regulation in the Electricity Sector*. [WP-2023-20. Research Brief]. MIT Center for Energy and Environmental Policy Research. https://ceepr.mit.edu/wp-content/uploads/2023/11/MIT-CEEPR-WP-2023-20-Brief.pdf

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), art. https://doi.org/10.1093/cybsec/tyae017

Council of the European Union. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). *Official Journal of the European Union*, L 345, pp. 75-82. http://data.europa.eu/eli/dir/2008/114/oj

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), pp. 13-21. https://doi.org/10.22215/timreview/835

Dacus, C., & Yannakogeorgos, P. A. (2016). Designing Cybersecurity into Defense Systems: An Information Economics Approach. *IEEE Security & Privacy*, *14*(3), pp. 44-51. https://doi.org/10.1109/MSP.2016.49

Dash, A., Sarmah, S.P., Tiwari, M.K., Jena, S.K., & Glock, C.H. (2024). Cybersecurity investments in supply chains with two-stage risk propagation. *Computers & Industrial Engineering*, 197, art. 110519. https://doi.org/10.1016/j.cie.2024.110519

Franco, M.F., Künzler, F., Assen, J. von der, Feng, C., & Stiller, B. (2024). RCVaR: An Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports. *Computers & Security*, 139, art. 103737. https://doi.org/10.1016/j.cose.2024.103737

Ghadge, A., Weiß, M., Caldwell, N.D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), pp. 223-240. https://doi.org/10.1108/SCM-10-2018-0357

Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), pp. 3-17. https://doi.org/10.1093/cybsec/tyv011

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), pp. 808-834. https://doi.org/10.1108/MAJ-09-2018-2004

Jones, J. A. (2006). An Introduction to Factor Analysis of Information Risk (FAIR). *Norwich University Journal of Information Assurance (NUJIA)*, *2*(1).

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(24), art. 13677. https://doi.org/10.3390/su132413677

Kianpour, M., Kowalski, S.J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, 116, 102493. https://doi.org/10.1016/j.simpat.2022.102493

Kure, H.I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications*, *4*(4), pp. 332–340. https://doi.org/10.1049/iet-cps.2018.5079

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), pp. 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Leszczyna, R. (2019). *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*. Springer International Publishing. Cham. ISBN:978-3-030-19538-0. https://doi.org/10.1007/978-3-030-19538-0

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2023). Mapping the Empirical Evidence of the GDPR's (In-)Effectiveness: A Systematic Review. *Available at SSRN*: http://dx.doi.org/10.2139/ssrn.4615186

Lis, P., & Mendel, J. (2019). Cyberattacks on Critical Infrastructure: An Economic Perspective. *Economics and Business Review*, *5*(2), pp. 24-47. https://doi.org/10.18559/ebr.2019.2.2

Massacci, F., Ruprai, R., Collinson, M., & Williams, J. (2016). Economic Impacts of Rules-versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers. *IEEE Security & Privacy*, *14*(3), pp. 52-60. https://doi.org/10.1109/MSP.2016.48

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International *Journal of Critical Infrastructure Protection*, *3*(3-4), pp. 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus*, 140(4), pp. 70-92. https://doi.org/10.1162/DAED_a_00116

Nagurney, A., & Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic Research and Electronic Networking*, *16*(1-2), pp. 127-148. https://doi.org/10.1007/s11066-015-9094-7

OECD. (2019). *Good Governance for Critical Infrastructure Resilience*. OECD Reviews of Risk Management Policies, OECD Publishing, Paris. https://doi.org/10.1787/02f0e5a0-en

Paté-Cornell, M.-E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis, 38*(2), pp. 226-241. https://doi.org/10.1111/risa.12844

Ragazzi, E., Stefanini, A., Benintendi, D., Finardi, U., & Holstein, D. K. (2020). *Evaluating the prudency of cybersecurity investments: Guidelines for Energy Regulators*. Washington DC: NARUC.

Rulleau, B. (2023). Household preferences for cyber-attack resilient water distribution networks: A latent class analysis of a discrete choice experiment in France. *Water Resources and Economics*, 43, art. 100230. https://doi.org/10.1016/j.wre.2023.100230

Taddeo, M. (2019). Is Cybersecurity a Public Good? *Minds and Machines*, *29*(3), pp. 349-354. https://doi.org/10.1007/s11023-019-09507-5

Vallette d'Osia, J.M.C., Finardi, U., & Ragazzi, E. (2025). Methods to assess the economic value of cybersecurity. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods (pp. 25-43). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_02

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, 89, art. 101659. https://doi.org/10.1016/j.cose.2019.101659