DOI: 10.15649/2346030X.3669
Aibi revista de investigación, administración e ingeniería. Volume 12, Number 2, Pág 41-48, May - August 2024, ISSN 2346-030X

Economic model of an information security framework implementation for Colombian organizations

Juan Carlos Serna[1], Aixa Eileen Villamizar-Jaimes[2], Silvana Lorena Vallejo[3]
[1,2,3]Tecnológico de Antioquia, *Medellín - Colombia*
ORCID: [1]*0009-0000-4093-0120*, [2]*0000-0002-4070-1763* [3]*0000-0002-6770-0840*

Received: December 12, 2023.
Accepted: April 05, 2024.
Published: May 01, 2024.

***Abstract*—** The limited understanding of how information security management impacts organizational economies hinders management's decision-making process regarding investments in security frameworks. This challenge, coupled with the increasing threats and vulnerabilities in computer systems, reinforces cybercrime and leads to substantial financial losses. While economic models incorporating cybersecurity variables have been developed, they do not fully evaluate the implementation of a specific security framework within a specific country's context. The proposed model aimed at economically justifying the implementation of a cybersecurity framework in Colombian organizations, thereby contributing to companies' strategic direction and economic growth. The model integrates a security framework released by the Colombian government with significant contributions from selected economic models in a systematic literature review. This integration results in a novel economic model that can be implemented across several kind of companies.

Keywords: model, economic, framework, investments.

*Corresponding author.
Email: aixa.villamizar@tdea.edu.co (Aixa Eileen Villamizar Jaimes).
Peer reviewing is a responsability of the Universidad de Santander.

How to cite this article: J. C. Serna, A. E. Villamizar-Jaimes y S. L. Vallejo, "Economic model of an information security framework implementation for Colombian organizations", *Aibi research, management and engineering journal*, vol. 12, no. 2, pp. 41-48 2024, doi: 10.15649/2346030X.3669

I. INTRODUCTION

The implementation of cybersecurity controls relies on various factors, including company size, available budget, strategic roadmap, business type, and crucially, clear management support. Numerous approaches have been proposed to mitigate security risks in both companies and governments, particularly in developed countries [1]. These strategies encompass cybersecurity awareness, the implementation of security frameworks and best practices, investments in human talent, sharing common and relevant global threats through knowledge transfer [2].

In many cases, management refrains from investing in cybersecurity controls due to the lack of clarity regarding their economic impact [3]. The technical and managerial concepts of cybersecurity often fail to integrate with the economic foundations of each business. Additionally, discussions on cybersecurity typically revolve around risk management and quantification, focusing on losses incurred from cyberattacks. Cybersecurity professionals struggle to convey information security needs in economic terms to demonstrate the effects of investments on a company.

Information security sources such as ISO 27001 and the National Institute of Standards and Technology (NIST) framework recommend several investments in cybersecurity controls. These controls are supported by threat knowledge, risk analysis, and attack analysis, which are typically explained in technical language and require specialized training in computer systems, which may not be common among company management personnel.

II. THEORETICAL ANALYSIS

Below are the most representative theoretical concepts used in this research.

The cybersecurity economy is a concept that encompasses everything related to the protection of information and communication technologies (ICT) applications designed for the development of economic activities, which typically face cybercrimes, resulting in financial losses and impacting the progress of activities in government and businesses [4]. This economy can be based on existing models focused on productivity or economic growth, considering factors such as human capital and the positive effects of ICT, but also incorporating external factors associated with cybersecurity.

By definition, a model is the relationship between data or variables and is worked through concepts, whose validity will be determined by their ability to reproduce or represent a real-life system. When introducing external factors related to cybersecurity, the model will have to continue representing the behavior of the system.

The impacts on organizations or governments caused by cybercrimes or incidents can be considered as externalities of the system. Economists use this term to describe the side effects of transactions, which can be positive, such as scientific research, or negative, such as pollution. Numerous externalities can be found when analyzing investment in security since it depends on the efforts of various sectors within an organization [5].

The implementation of a specific security framework, therefore, constitutes an externality that can be included in an economic model and can affect a company's productivity. Other externalities may not be associated with good security practices and may be influenced by other fields such as legislative [6]. However, this study focuses only on the effect of actions aimed at information protection from the engineering perspective.

Some previous works related to the theme of this research can be grouped as follows:

- The contribution made by [4] shows the possibility of extending a model, including cybersecurity as a contributing factor to the economic growth of an organization.
- [7] Discusses the lack of awareness of economic advantages as an obstacle to proper investment in a cybersecurity risk management system.
- The works carried out by Anderson in 2001 and 2009 account for the risk mitigation strategies adopted in developed countries since that time, as well as the global vision required for their management; where engineers can collaborate with economists and legislators to strengthen good security practices in organizations.
- [8] Propose a methodology for cost-based risk estimation.

III. METHODOLOGY

In line with the purpose of studying the economic effect of the implementation of cybersecurity frameworks in Colombian organizations, the design of the research to be carried out is descriptive in scope [9] and with a mixed approach.

The primary objective of this study was to develop a model that evaluates the economic impact of implementing an information security framework in Colombian organizations, aiming to justify investments and facilitate decision-making processes. To achieve the objective, a three-phase research methodology is proposed. The first phase involves conducting a systematic literature review that specifically focuses on economic models related to information security. In the second phase, a comprehensive characterization of the global standards is performed, aiming to identify the most suitable framework that can effectively represent the Colombian context. The third phase integrates the compatible findings from the literature review with the selected framework to develop the new economic model. Figure 1 illustrates this procedure, showing that stages 1 and 2 could be conducted in parallel.

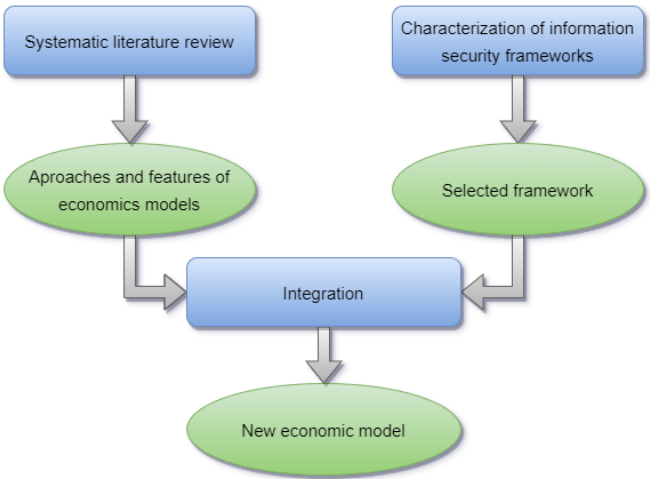

Figure 1: Research Design.
Source: Authors' own creation.

IV. RESULTS

a. Systematic literature review of economic models

We carried out a systematic literature review focused on economic models that incorporate information security. It explores secondary works derived from these models and examines their applications in specific organizational scenarios.

1. *Review Design*

To start the review, we formulated two key questions: Firstly, which models demonstrate the economic impact of information security on organizations? Secondly, what research papers have been generated from the application of these economic models?

To facilitate the search process, we conducted a survey using relevant documents and their corresponding keywords. As a result, the following search string was obtained: (return AND security AND investment AND economic AND cybersecurity AND "Security Information" AND model).

We established some search criteria, including papers from 2012 onwards were included, relevance to at least one of the questions, and availability of the complete versions. Table 1 provides an overview of the search process, which yielded 117 papers and 10 matches across the consulted databases. Finally, 20 publications were selected based on the established criteria.

Table 1: Findings from database review, including matches.

Databases	Founded papers	Selected papers	Matches
Scopus	34	12	0
Science Direct	68	4	7
Google Scholar	15	4	3
Totals	117	20	10

Source: Authors' own creation.

2. *Review Results*

By means of the analysis of the chosen papers, we identified various approaches and methods that incorporate information security into economic models, aiming to support investments, facilitate decision-making, and maximize profits. By categorizing these contributions based on their approach and shared characteristics, the classification presented in Table 2 was obtained.

Table 2: Paper Classification by Approaches.

Approach	Titles
A1: Optimal investment (Gordon Loeb) /ROI/ROSI	Dangerous games: A literature review on cybersecurity investments [10] Cybersecurity investment allocation for a multi-branch firm: Modeling and optimization [11] Enterprise security investment through time when facing different types of vulnerabilities [12] Optimal information security expenditures considering budget constraints [13] Optimal information security investment in a Healthcare Information Exchange: An economic analysis [14] Cyber kpi for return on security investment [15] Framework for calculating return on security investment (ROSI) for security-oriented organizations [16] Towards integrating insurance data into information security investment decision making [17] Managing the investment in information security technology by uses of a quantitative modeling [18]
A2: Stakeholders contribution	Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem [19] Optimum spending on cybersecurity measures[11]
A3: Cost-benefit model	Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker (Paul & Zhang, 2021) Quantifiable & comparable evaluations of cyber defensive capabilities: A survey & novel, unified approach [21]

Approach	Titles
A4: Decision making	Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning [22]
A5: Game theoretic	Information sharing vs. Privacy: A game theoretic analysis [23] A game theory model of cybersecurity investments with information asymmetry [24] Establishing evolutionary game models for CYBer security information EXchange (CYBEX) [25]
A6: Resource-based view and organizational learning theory	A multi-Theoretical literature review on information security investments using the resource-based view and the organizational learning theory [26]
A7: Security events study	Information security breaches and IT security investments: Impacts on competitors [27]
A8: Risk Management	Risk management, firm reputation, and the impact of successful cyberattacks on target firms [28]

Source: Authors' own creation.

b. Characterization of information security frameworks

1. Recognized information security Standards.

Cybersecurity standards encompass both general frameworks and sector-specific models designed for particular market segments. The following list highlights the most renowned models, chosen based on their prominence in previous works and their recurrent utilization in the field [29].

- ISO27000 Set (International standards about security information)
- NIST (National Institute of Standards and Technology)
- PCI DSS (Payment Card Industry Data Security Standard)
- CIS Controls (Center for Internet Security)
- CSA (Cloud Security Alliance) CCM (Cloud Control Matrix)
- GPDR (General Data Protection Regulation)
- OWASP (Open Web Application Security Project) SAMM (Software Assurance Maturity Model)

Special attention will be given to the features of general models that apply to any type of company, notably the NIST CSF and the ISO/IEC 27001 standard. Research conducted by [29] and [30], comparing and characterizing the ISO/IEC 27001 and NIST CSF standards, revealed that these models share common traits. However, their differences make them complementary in the establishment of a comprehensive system for managing cybersecurity and information security.

2. Security Standards in Colombia

Ministry of Information Technology and Communications (Min TIC) has introduced the Information Security and Privacy Model (MSPI) built upon the ISO27001 standard and the laws on personal data protection, transparency, and access to public information. The MSPI primary objective is to safeguard information assets and ensure transparent management practices within public entities [31]. This model comprises five phases as shown in Figure 2, corresponding to PDCA (Plan, Do, Check, Act) cycle and diagnosis for the implementation through the objectives, goals, and tools. The MSPI evaluates the disparity between the current level of maturity and the optimized level that can be achieved through the implementation and continuous improvement of the model. It defines five maturity levels: nonexistent, initial, repeatable, defined, managed, and optimized. Min TIC customizes international best practices, specifically ISO27001 and NIST, to suit the unique context of Colombian Organizations. They provide a concrete framework and supportive tools to facilitate the MSPI implementation.

Figure 2: MSPI phases including Planning, Implementation, Performance evaluation, continuous improvement, and diagnosis.
Source: Authors' own creation.

c. *Aspects for model integration*

The MSPI framework structure can be compared with the structure from other models that describe several economic approaches. As a basis to integrate the economic effect in the MSPI model by incorporating economic components. From those approaches, A1 and A3 were considered essential as they provide economic elements for the development of an integrated economic model based on the MSPI. This inclusion does not compromise the generality of the model and ensures easy implementation within an organization. Other approaches were disregarded for the new model due to their redundancy within the MSPI stages or the potential for excessive granularity. For example, the A2 approach focused on the contributions of various stakeholders, was not considered due to the stakeholder kinds in a Company can vary significantly based on their specific characteristics.

Integrating a new model to illustrate the economic effects of implementing an information security framework in a Colombian organization involves extending the current model developed by Min TIC, having into account the economic features proposed by [16] in their six-phase framework for calculating the Return on Security Investment (ROSI) into the MSPI. The MSPI structure is maintained while expanding its applicability range; phases 4 and 5 of the cost-benefit analysis of [21], including specific calculations for the total cost of implementing cybersecurity measures; and the performance evaluation and continuous improvement stages were enhanced with the metrics suggested by [15]. These metrics served as valuable indicators for decision-making regarding the implementation, maintenance, or modification of information security controls, which are ultimately viewed as economic investments. By incorporating these modifications into the Min TIC model, we propose the Economic Model of Information Security and Privacy (MESPI). Table 3 illustrates how MSPI interacts with the A1 and A3 approaches to the integration of MESPI.

Table 3: Integration of MSPI with A1 and A3 approaches.

MSPI General Stages	**ROSI Framework** [16]	**Cost-benefit** [21]	**Cyber KPIs** [15]
Diagnosis	Not modified	Not modified	Not modified
Planning	Phases 1 and 2	Not modified	Not modified
Implementation	Phases 3, 4 and 5	Calculating the total cost of security implementation	Calculation of security metrics
Performance evaluation	Phase 6	Not modified	Security metrics evaluation
Continuous improvement	Not modified	Not modified	Not modified

Source: Authors' own creation.

d. *MESPI Model*

1. *Diagnosis*

This phase aims to create a knowledge base for the organization through the collection of information, its processing using the evaluation tool and the result of the company maturity state about security topics. This stage does not require modifications in its content.

2. *Planning*

Planning activities included in the MSPI are comparable to those described in phases 1 and 2 of the framework for calculating ROSI in organizations developed by [16] but in the former information assets are not quantified.

The economic value of an asset is the product of its physical cost and critical value. The expression "physical cost" is not always literal and sometimes reflects different book values. The following equation is then obtained:

$$asset\ value = \text{asset's physical cost} * \text{criticality value}$$

To obtain the criticality value of an asset, a weight must be assigned to each component of the CIA security triad (confidentiality, integrity, availability) as follows:

$$criticality\ value = \mathrm{C} + \mathrm{I} + \mathrm{A}$$

The framework proposes a value between 1 and 5 for each component, which is reflected in a criticality value between 3 and 15. Adding these estimates to the asset values modifies the planning stage to continue building the MESPI.

3. *Implementation*

The objectives set by the MSPI in this phase correspond to the creation of a risk-and-threat treatment plan. It is coherent that in the implementation phase, the recommendations of the framework for calculating the ROSI in phases 3, 4 and 5 are added, where the procedure for calculating the ROSI according to the vulnerabilities, their probability of materialization and impact, the annual loss, and the cost-benefit analysis of the investments in information security are described.

Threat modelling becomes the fundamental element for the calculations developed in this section and to obtain the final value of the ROSI it is necessary to start by calculating the probability that a threat will materialize, using the Bayesian theorem. For instance, if there is a threat X that can materialize through vulnerabilities A, B and C, it is necessary to calculate the probability of materialization associated with each threat.

$$\mathrm{P(A/X)} = \frac{\mathrm{P(X/A)} * \mathrm{P(A)}}{\mathrm{P(X/A)} * \mathrm{P(A)} + \mathrm{P(X/B)} * \mathrm{P(B)} + \mathrm{P(X/C)} * \mathrm{P(C)}}$$

$$\mathrm{P(B/X)} = \frac{\mathrm{P(X/B)} * \mathrm{P(B)}}{\mathrm{P(X/A)} * \mathrm{P(A)} + \mathrm{P(X/B)} * \mathrm{P(B)} + \mathrm{P(X/C)} * \mathrm{P(C)}}$$

$$\mathrm{P(C/X)} = \frac{\mathrm{P(X/C)} * \mathrm{P(C)}}{\mathrm{P(X/A)} * \mathrm{P(A)} + \mathrm{P(X/B)} * \mathrm{P(B)} + \mathrm{P(X/C)} * \mathrm{P(C)}}$$

In summary, the total probability of an attack associated with threat X is:

$$P(X) = P(A/X) + P(B/X) + P(C/X)$$

This procedure should be repeated for each threat identified in the threat modelling. Another value to be determined is the impact, which corresponds to the potential loss associated with a particular threat and is calculated as follows:

$$\text{Impact} = \sum_{n=1}^{i} \text{exposure factor}_i * \text{asset value}_i * \text{recovery cost}_i$$

Where i is the number of assets, the value of each asset is found in the planning phase, the recovery cost corresponds to the economic value of getting the operation back to its normal state and the exposure factor in the portion of the asset that would be exposed.

Having the impact and the probability of materialization of the threat, it is possible to find the annual loss for all assets concerning a threat or the whole system, as follows:

$$\text{Annual loss} = \text{Impact} * \text{probability}$$

$$\text{Total annual loss} = \sum_{k=1}^{n} \text{annual loss} * \text{Probability}_k$$

Where k is a threat identifier and n is the total number of threats.

Through a cost-benefit analysis, the total value of the security investment is calculated:

$$\text{CTotal} = \sum \text{CBreach}_i + \text{CDefense}$$

Where the CBreach corresponds to the total expected annual loss (estimated value) and the defense cost is composed of an initial installation cost CI, a base operation cost CB, a cost associated with an alert review (detection of real attacks and false positives) CT and an incident response cost CIR.

The total security investment cost associated with the controls implemented is:

$$\text{CTotal} = \sum \text{CBreach}_i + C_I + C_B + C_T + C_{IR}$$

Finally, the ROSI is calculated as follows:

$$\text{ROSI} = \frac{\text{Total annual loss} - \text{CTotal}}{\text{CTotal}}$$

Also in this phase, it includes the creation of twenty key cybersecurity metrics proposed by [32] to evaluate the profitability of organizations according to their cybersecurity management system and which serves as additional support to ROSI and continuous improvement. The twenty metrics are grouped into six categories: thwarted attacks, vulnerabilities and threats, asset coverage, human and process capabilities, monitoring and capacity, and incident detection.

4. Performance evaluation

This phase of the MSPI includes the follow-up and review activities established in the previous stages or iterations of the PDCA cycle, as well as their respective documentation.

To bring the model to be a MESPI it is proposed to add the following activities: Period ROSI analysis, and evaluation of security metrics.

Additionally, security metrics are analyzed and compared with previous periods and in the context of the implemented security controls as input to demonstrate the effectiveness of economic investments for security purposes.

5. Continuous improvement

At this point, all the results of the analyses carried out in the continuous improvement phase must be available, allowing the following activities to be executed in the MESPI model:

- Definition of corrective actions against security non-conformities resulting from audits or internal reviews.
- Definition of actions for improvements in the management of the security system by the analysis of its metrics.
- Definition of economic actions resulting from the review of ROSI analysis and security metrics according to the company's profitability. These corrective actions may involve changes in policies, controls, technology, and budget.

e. Proposed model validation

To validate the economic model proposed in this study, we conducted a focus group using the expertise of seven cybersecurity professionals. These experts provided valuable insights from their practical experience in the field as well as their academic perspectives. The participants

consisted of engineers with significant expertise in technical domains, information security strategy, and governance. Some of them were also affiliated with the academic sector through their involvement in teaching. Based on the results of a feasibility assessment carried out during the session, the following conclusions were drawn:

- All experts agree that the proposed model effectively integrates security measures and their economic impact on organizations. It is suitable for implementation in both public and private companies.
- MESPI is perceived to have a moderate implementation complexity. Five experts expressed confidence in its global implementation within their organizations, while two suggested partial application, aligning with current organizational demands.
- The model's applications include supporting senior management in security investments, evaluating cybersecurity management systems, vendor selection, and assessing the effectiveness of existing security measures.
- In academia, experts suggest incorporating the MESPI model into engineering and information security programs, particularly in postgraduate education, to meet the growing demand for skilled professionals.

V. CONCLUSIONS

Through the integration of MSPI and incorporating the contributions of [16], [21], and [15], we have developed MESPI, a novel economic model. MESPI introduces several key concepts, including the calculation of ROSI (Return on Security Investment), the assessment of the total cost of security implementation, and the computation of essential metrics for evaluating the security management system. This integration significantly enhances the decision-making process for security investments by management, while also enabling its implementation within Colombian organizations. Furthermore, MESPI benefits from its alignment with the MSPI guidelines, making it well-suited for adoption in Colombian organizations due to shared language and specific directives. MESPI provides the flexibility to make decisions regarding specific security investments or the entire information security management system of an organization. Its applicability extends to public, private, and diverse business organizations. Based on MESPI features, we propose the following areas for future research:

- Creation of dedicated guidelines for MESPI that complement the existing guidelines of MSPI. These additional guidelines will simplify the calculation of economic variables incorporated in the new model.
- Implementation and iterative refinement of the MESPI model within an organization to calibrate its parameters and validate the accuracy of probabilistic data. This process will be particularly valuable as more historical information about the company becomes accessible.
- Automation of MESPI and its integration with information security systems to streamline the data loading process from various sources. This automation will significantly improve the efficiency of calculations and metrics.

VI.REFERENCES

[1] R. Anderson and T. Moore, "Information security: Where computer science, economics and psychology meet," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 367, no. 1898, pp. 2717–2727, 2009, doi: 10.1098/rsta.2009.0027.

[2] E. M. Ahmed, "Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth," Journal of the Knowledge Economy, vol. 12, no. 1, pp. 412–430, 2021, doi: 10.1007/s13132-020-00627-3.

[3] A. A. Alahmari and R. A. Duncan, "Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs," in 2021 IEEE International Conference on Computing, ICOCO 2021, 2021, pp. 115–121. doi: 10.1109/ICOCO53166.2021.9673554.

[4] E. M. Ahmed, "Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth," Journal of the Knowledge Economy, vol. 12, no. 1, pp. 412–430, Mar. 2021, doi: 10.1007/s13132-020-00627-3.

[5] R. Anderson and T. Moore, "Information security: where computer science, economics and psychology meet," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 367, no. 1898, pp. 2717–2727, Jul. 2009, doi: 10.1098/rsta.2009.0027.

[6] R. Anderson, "Why information security is hard - an economic perspective," in Seventeenth Annual Computer Security Applications Conference, IEEE Comput. Soc, 2001, pp. 358–365. doi: 10.1109/ACSAC.2001.991552.

[7] A. A. Alahmari and R. A. Duncan, "Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs," in 2021 IEEE International Conference on Computing (ICOCO), IEEE, Nov. 2021, pp. 115–121. doi: 10.1109/ICOCO53166.2021.9673554.

[8] A. Panou, C. Ntantogian, and C. Xenakis, "RiSKi," in Proceedings of the 21st Pan-Hellenic Conference on Informatics, New York, NY, USA: ACM, Sep. 2017, pp. 1–6. doi: 10.1145/3139367.3139426.

[9] J. Abreu, "Hipótesis, método & diseño de investigación (hypothesis, method & research design)," Daena: International Journal of Good Conscience, vol. 7, no. 2, pp. 187–197, 2012.

[10] A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," J Econ Surv, vol. 36, no. 1, pp. 157–187, 2022, doi: 10.1111/joes.12456.

[11] T. Kissoon, "Optimum spending on cybersecurity measures," Transforming Government: People, Process and Policy, vol. 14, no. 3, pp. 417–431, 2020, doi: 10.1108/TG-11-2019-0112.

[12] Y. Miaoui and N. Boudriga, "Enterprise security investment through time when facing different types of vulnerabilities," Information Systems Frontiers, vol. 21, no. 2, pp. 261–300, 2019, doi: 10.1007/s10796-017-9745-3.

[13] A. Schilling and B. Werners, "Optimal information security expenditures considering budget constraints," in Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings, 2015. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85011024539&partnerID=40&md5=45602e3470140f27013a253c6b52a88d.

[14] C. D. Huang, R. S. Behara, and J. Goo, "Optimal information security investment in a Healthcare Information Exchange: An economic analysis," Decis Support Syst, vol. 61, no. 1, pp. 1–11, 2014, doi: 10.1016/j.dss.2013.10.011.

[15] C. Onwubiko and A. Onwubiko, "Cyber kpi for return on security investment," in 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), IEEE, 2019, pp. 1–8.
[16] T. Yaqoob, A. Arshad, H. Abbas, M. F. Amjad, and N. Shafqat, "Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations," Future Generation Computer Systems, vol. 95, pp. 754–763, 2019, doi: https://doi.org/10.1016/j.future.2018.12.033.
[17] D. W. Woods and A. C. Simpson, "Towards Integrating Insurance Data into Information Security Investment Decision Making," in 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2018, pp. 1–6. doi: 10.1109/CyberSA.2018.8551375.
[18] R. Bojanc, B. Jerman-Blažič, and M. Tekavčič, "Managing the investment in information security technology by use of a quantitative modeling," Inf Process Manag, vol. 48, no. 6, pp. 1031–1052, 2012, doi: https://doi.org/10.1016/j.ipm.2012.01.001.
[19] Z. Rashid, U. Noor, and J. Altmann, "Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem," Future Generation Computer Systems, vol. 124, pp. 436–466, 2021, doi: 10.1016/j.future.2021.05.033.
[20] J. A. Paul and M. Zhang, "Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker," Eur J Oper Res, vol. 291, no. 1, pp. 349–364, 2021, doi: 10.1016/j.ejor.2020.09.013.
[21] M. D. Iannacone and R. A. Bridges, "Quantifiable & comparable evaluations of cyber defensive capabilities: A survey & novel, unified approach," Comput Secur, vol. 96, p. 101907, 2020, doi: https://doi.org/10.1016/j.cose.2020.101907.
[22] E. Weishäupl, E. Yasasin, and G. Schryen, "Information security investments: An exploratory multiple case study on decision-making, evaluation and learning," Comput Secur, vol. 77, pp. 807–823, 2018, doi: 10.1016/j.cose.2018.02.001.
[23] M. Ezhei and B. Tork Ladani, "Information sharing vs. privacy: A game theoretic analysis," Expert Syst Appl, vol. 88, pp. 327–337, 2017, doi: 10.1016/j.eswa.2017.06.042.
[24] A. Nagurney and L. S. Nagurney, "A game theory model of cybersecurity investments with information asymmetry," NETNOMICS: Economic Research and Electronic Networking, vol. 16, no. 1–2, pp. 127–148, 2015, doi: 10.1007/s11066-015-9094-7.
[25] D. Tosh, S. Sengupta, C. A. Kamhoua, and K. A. Kwiat, "Establishing evolutionary game models for CYBer security information EXchange (CYBEX)," J Comput Syst Sci, vol. 98, pp. 27–52, 2018, doi: https://doi.org/10.1016/j.jcss.2016.08.005.
[26] E. Weishäupl, E. Yasasin, and G. Schryen, "A multi-Theoretical literature review on information security investments using the resource-based view and the organizational learning theory," in 2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015, 2015. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126603063&partnerID=40&md5=01e728bc68f1617459291cb267d49d31.
[27] C. Y. Jeong, S.-Y. T. Lee, and J.-H. Lim, "Information security breaches and IT security investments: Impacts on competitors," Information & Management, vol. 56, no. 5, pp. 681–695, 2019, doi: https://doi.org/10.1016/j.im.2018.11.003.
[28] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," J financ econ, vol. 139, no. 3, pp. 719–749, 2021, doi: https://doi.org/10.1016/j.jfineco.2019.05.019.
[29] Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013," in CEUR Workshop Proceedings, 2022, pp. 21–32. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85143792195&partnerID=40&md5=6672f25624c8d26cff9b20cedaa8d232.
[30] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020, 2020. doi: 10.1109/NCETSTEA48365.2020.9119914.
[31] M. R. O. Díaz and P. E. S. Rangel, "National challenges for cybersecurity on a global level: An analysis for Colombia," Revista Criminalidad, 2020, [Online]. Available: http://www.scielo.org.co/scielo.php?pid=S1794-31082020000200199&script=sci_abstract&tlng=en.
[32] C. Onwubiko and A. Onwubiko, "Cyber KPI for Return on Security Investment," in 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), IEEE, Jun. 2019, pp. 1–8. doi: 10.1109/CyberSA.2019.8899375.