Systematic Analysis of Critical Factors for Value Management in Cybersecurity

Vicente Merchán-Rodríguez, *Member, IEEE,* and Danny Zambrano-Vera

***Abstract*—Existing studies indicate that cybersecurity ranks among the top priorities for IT spending in telecommunications organizations, and that value management is critical for defining effective cybersecurity policies and strategies that enable efficient resource allocation. This study aims to analyze and synthesize existing research on the critical factors underpinning the strategic relevance of value management in the cybersecurity of telecommunications organizations. A systematic literature review (SLR) following the PRISMA methodology was conducted across three phases: planning, execution, and reporting. The Consensus tool was used to search the Semantic Scholar, IEEE Digital Library, Scopus, and ScienceDirect databases, yielding 950 articles. After rigorous screening and eligibility assessment, 49 key articles were selected for qualitative synthesis. Python-based tools were used for bibliometric analysis. Results show that 2023 recorded the highest publication output, with the journal Sustainability leading in article distribution. Inter-institutional collaboration and organizational culture emerged as the themes generating the greatest research interest. Six recurring categories were identified, consolidating the critical success factors (CSF) of value management in cybersecurity within telecommunications companies. The findings suggest that effective cybersecurity value management requires a holistic, risk-based approach that integrates human, technical, and strategic dimensions. Organizations must prioritize continuous adaptation and resilience against evolving threats by leveraging collaborative ecosystems and information-sharing mechanisms. Furthermore, embedding cybersecurity within broader business, innovation, and value-creation agendas is essential for sustaining competitive advantage and stakeholder trust. Compliance with standards and the application of economic models for risk quantification ensure regulatory alignment and long-term financial sustainability.**

Link to graphical and video abstracts, and to code: https://latamt.ieeer9.org/index.php/transactions/article/view/10932

***Index Terms*—value management, cybersecurity, critical success factors, telecommunications.**

I. Introduction

THE Netskope's 'Cloud and Threat Report 2025' [1] reveals that the lack of robust cybersecurity strategies in the telecommunications sector represents a critical and growing risk; it highlights that many operators still lack comprehensive policies for the constant monitoring of cloud and web traffic, which facilitates espionage campaigns such as those perpetrated by Salt Typhoon, which achieved persistent and stealthy access to telecom networks. A recent study examines proactive cybersecurity strategies in the telecommunications sector and highlights that effective digital security management significantly strengthens corporate reputation, user trust, and organizational value [2]. Another study found that cybersecurity contributes between 11% and 20% to the value of each strategic initiative in which it is involved at the business level, with an estimated median of US$36 million per initiative, making cybersecurity a strategic driver of growth in the telecommunications sector [3].

According to Watson & Bergman [3], there are six key areas of value creation where cybersecurity actively participates, so we have each of these with their respective and potential contribution margins: 1. Technology adoption and construction (54%); 2. Strengthening brand trust and reputation (56% - 72%); 3. Improved customer experience (48%); 4. business transformation and innovation (11% and 20% of the value generated); 5. Expansion into new markets (35%), and 6. Development of new products (36%).

According to Chitopoulos [4], telecommunications companies occupy a unique position as guardians of the global digital infrastructure and must continually innovate to remain competitive. In addition, each new technology deployed, whether 5G, IoT, cloud computing, among others, expands the attack surface while generating value for customers, users, and shareholders. This paradox forces operators to make strategic decisions: investing more in cybersecurity can slow technology adoption, while prioritizing innovation without adequate controls exposes them to significant risks.

Cybersecurity strategies have positioned themselves as a key element in the security of contemporary companies, encompassing a wide variety of approaches, from emerging threat strategies and the role of artificial intelligence [5], [6], [7], [8] to regulatory and compliance frameworks [9], [10], [11]; through risk management and organizational resilience as a fundamental strategy [12], [13].

Value management practices applied to cybersecurity in the telecommunications sector are an emerging field that seeks to integrate principles of maximizing organizational performance with the formulation of digital protection strategies. The BS EN 12973:2020 standard [14] defines Value Management (VM) as a holistic concept oriented towards strategic decision-making by integrating principles, drivers, and tools to maximize organizational performance [15]. In the context of telecommunications, applying these practices is critical to transforming cybersecurity from a cost center to a strategic value multiplier.

Some studies on VM practices in organizations cover theoretical approaches, practical frameworks and applications in various sectors, exploring repetitive activities, competencies

The associate editor coordinating the review of this manuscript and approving it for publication was Cesar Azurdia (Corresponding author: *Vicente Merchán R.*).

Vicente Merchán R., and D. Zambrano-Vera are with the Universidad de las Fuerzas Armadas, Sangolquí, Ecuador (e-mails: vrmerchan@espe.edu.ec, and dizambrano@espe.edu.ec).

and conceptual models that integrate value management to maximize the potential of investments in information systems, even defining some of these practices on a model based on structural, process and relational competencies [16]; identification of drivers and long-term value creation [17]; value management in decision-making and innovation [18]; and, barriers to the adoption of value management as a strategic proposal for improvement [19].

Rowe [20] points out that SLR is a valuable research method, especially for achieving objectives such as summarizing existing work, examining current contributions and findings, and outlining alternative frameworks or prior research paths. SLR, as a research method, is a means of identifying, evaluating, and interpreting all available research and answering research questions [21], [22]; therefore, it is a crucial component of this research process. It allows a critical focus on the existing primary evidence on the critical value management factors for the design or formulation of cybersecurity strategies in telecommunications companies. A well-executed SLR can identify critical value management success factors for formulating cybersecurity strategies and reveal patterns and trends that might go unnoticed in isolated studies [23].

The objective of this work is to analyze and synthesize existing studies on critical factors that support the importance of value management in cybersecurity processes of telecommunications organizations. This study is classified as a secondary study because it is a review of primary studies. This work is pertinent to Ecuador's Ministry of Telecommunications because it is leading the update of the national cybersecurity policy and strategy.

The work is organized as follows: in section 2, we provide an overview of cybersecurity and value; Section 3 describes the method used for this review; Section 4 presents the results of the review after first providing an overview of the studies, the research methods used, the quality of the method and a description of the studies; Section 5 discusses limitations, strength of evidence, and future studies; and, section 6 concludes the work.

II. Background

A. Cybersecurity

Cybersecurity is a broad concept within information security, encompassing technologies, practices, policies, and measures to protect information systems, computer networks, devices, and data from unauthorized access, malicious attacks, data theft, fraud, and other risks in the digital world [24].

According to Schiliro [25, p. 11], 'Cybersecurity is the collection and coordination of resources, including personnel and infrastructure, structures and processes, to protect cyberspace-enabled networks and computer systems against events that compromise integrity and property rights, resulting in some type of loss'.

Some material perspectives related to cybersecurity that we can consider are:

- 'Security has been defined as a process of protecting an object from physical damage, unauthorized access, theft, or loss, maintaining a high level of confidentiality and integrity of information about the object, and making information about that object available whenever needed' [26, p. 66].
- 'The activity or process, skill or capability, or state by which information and communications systems and the information contained therein are protected and/or defended against damage, unauthorized use or modification, or exploitation' [27, Sec. C].
- 'Protect individuals, society, organizations, and nations from cyber risks. With the note: «Protecting means keeping cyber risk at a tolerable level» [28, Sec. 3.6].

As we can see, the conceptualization of cybersecurity ranges from IT policies and infrastructure to processes, with DHS's definition guiding our literature review.

Recent systematic reviews of cybersecurity strategies in the telecommunications sector highlight several emerging threats and corresponding protective measures. These studies emphasize the need for multi-layered security approaches, advanced technologies, and collaborative efforts among stakeholders to improve resilience against cyberattacks. Such is the case with ransomware and APTs as critical infrastructure threats [29], the transition to 5G integrating AI and ML [30], and zero trust architecture [31]. While these reviews underscore the importance of robust cybersecurity measures, they also reveal gaps in current practices, suggesting that continued adaptation and investment in cybersecurity are vital to the telecommunications sector's resilience in the face of evolving threats.

B. Value

In research, the term value is rarely defined in isolation, but linked to an object: quality, satisfaction, attitudes, co-creation of value, axiological values, etc. Even so, traits are repeated: evaluation, desirability, and judgment. In the Dictionary of the Royal Spanish Academy [32], value is defined as: 'Degree of usefulness or aptitude of things to satisfy needs or provide well-being or delight'.

Value from the perspective of IT governance and management frameworks is primarily understood as the positive impact of IT investments and services on business performance and objectives, rather than as a purely technical attribute. In the specific case of IT governance, 'IT business value' is defined as the impact of information technology on organizational performance at the process and organizational levels, including efficiency and competitiveness [33]. This value is a direct consequence of good IT governance practices (e.g., COBIT and ITIL) [33], [34].

A systematic review of the benefits of IT initiatives proposes that IT value is a multidimensional set of informational, transactional, transformational, and strategic benefits that contribute to organizational outcomes [35]. These

benefits include, for example, better decision-making information, transaction automation, process changes, and new strategic capabilities [35].

C. Value Management

The term value management was introduced in 1974 by the U.S. General Services Administration, which refers to it as a group decision-making process used to increase or achieve value in areas ranging from the development of business strategies to the solution of technical problems [36]. Its application is based on three key concepts: 1. a function that defines needs in terms of purpose, without associating them with specific solutions; 2. a cross-functional team that incorporates diverse knowledge and perspectives to enrich the analysis; and 3. A structured and creative process that allows an alternation between creativity and analysis (lateral and vertical thinking) [37].

The Institute for Value Management (IVM) [38] defines value management in academic terms as a conceptual and methodological approach that guides existing management systems towards the systematic creation of sustainable value, through value-based and role-based thinking, collaborative behavior, and the use of structured methods to optimize the relationship between stakeholder needs and resources used.

According to the EN 1325:2014 [39] and EN 12973:2020 [40] standards, value management is an underlying concept that is applied within current management systems and approaches, based on value- and function-oriented thinking, and dedicated to motivating people, developing capabilities, promoting synergies and innovation, to maximize the overall performance of the organization.

Value management in cybersecurity has become a fundamental pillar for telecommunications companies, given the increasing sophistication of threats and the strategic importance of digital assets. The critical success factors (CSF) that reinforce the relevance of this management range from corporate governance, strategic intelligence and efficient asset management, to the development of an organizational culture oriented towards security and continuous innovation [41], [42], [43], [44], [45], [46], [47], [48], [49], [50]. Recent literature highlights that success in cybersecurity depends not only on technological solutions but also on alignment with business objectives, staff training, regulatory compliance, and the ability to anticipate and respond to incidents. These CSF enable telco companies to protect their competitive advantage, strengthen customer trust, and boost their resilience in a dynamic digital environment.

III. Method

Starting from the initial idea, a traditional literature review was carried out that evidenced the scarcity of specific publications. Although the concept of value has been studied in various disciplines, few works address its application to cybersecurity strategies, an emerging topic with a limited bibliography available.

Given this situation, an SLR was considered the most appropriate method to delve into the research topic. To ensure methodological rigor, the guidelines recommended by Kitchenham & Charters [22] were followed.

A SLR allows for the synthesis of large volumes of information and is especially useful for answering questions about the effectiveness of approaches or identifying gaps in knowledge [51]. The method consists of a structured process for identifying, evaluating, and methodically interpreting existing studies on a topic or phenomenon of interest [22] as shown in Fig. 1.

As a complement, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analyses) flowchart [52] was used to structure the process into three main phases: identification, screening, and eligibility and inclusion of studies.

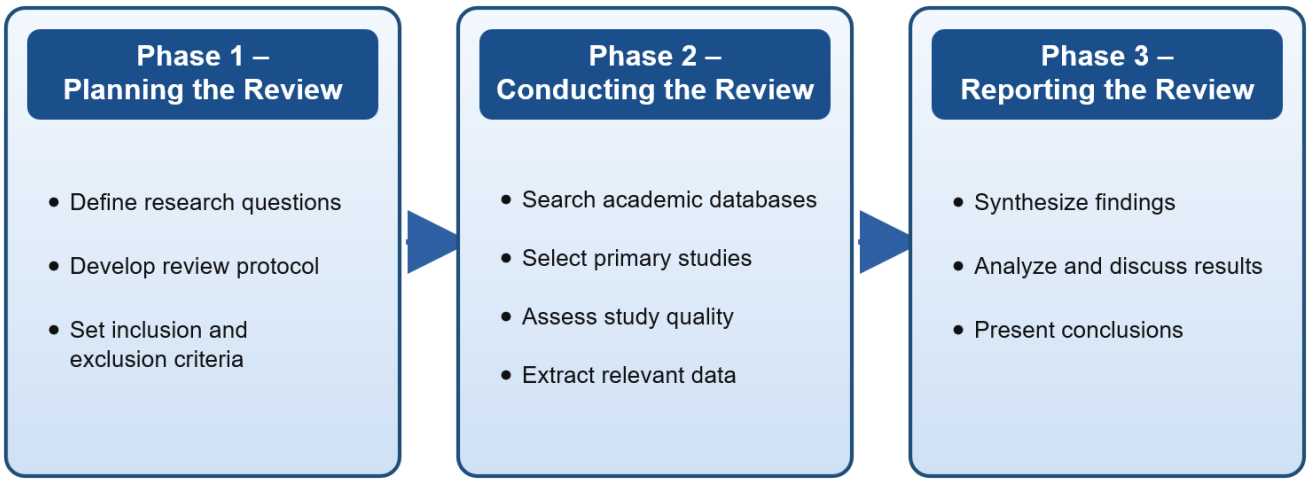


Fig. 1. Three-phase process followed for the SLR, adapted from Kitchenham & Charters [22].

A. Planning the Review

1) **Research Question**

RQ: What are the critical factors that underpin the strategic relevance of value management in the

cybersecurity strategies of telecommunications organizations?

2) **Search Terms**

For this phase, the research question was considered. Therefore, Table I shows the key terms in Spanish and English to be entered into the selected databases.

TABLE I
SEARCH TERMS AND BOOLEAN STRINGS USED IN THE SYSTEMATIC DATABASE QUERY

Concepts	Chain
Value Management	'Value management' OR 'Value administration' OR 'Value creation' OR 'Value protection'
Cybersecurity	'cybersecurity' OR 'cyber security' OR 'IT security' OR 'Information Security'
Telecommunication	'Telecommunication' OR 'Telco'
Critical success factors	'success factors' OR 'risk factors'

3) **Bibliography Retrieval**

This study focuses on journal articles and proceedings. The search string was used in major online databases, including Semantic Scholar, IEEE Digital Library, Scopus, and ScienceDirect, which were selected for their complementary nature and relevance to the study.

a) Inclusion and exclusion criteria.

Studies published in Spanish and English between 2020 and 2026 were considered, including research and review articles, peer-reviewed papers, book chapters, and conference proceedings addressing the research topic. This time range was selected because it coincides with the publication of the BS EN 12973:2020 value management standard and the consolidation of technologies such as 5G, IoT, and edge computing in telecommunications. These developments have redefined cybersecurity requirements and attack surfaces. Excluded materials included preprints, blog entries, web content, theses, technical reports, gray literature, presentations, case reports, and white papers.

b) Quality Assessment Checklist.

Selected studies were evaluated using a set of key questions assessing their relevance to the research object. Each article was examined for explicit focus on value management critical success factors and coverage of cybersecurity or closely related domains. Responses were coded on a trichotomous scale (Yes, Partially, No).

c) Tools and techniques for data visualization and management.

The analysis employed AI tools: Asta.allen, Consensus, and Python, to support the identification, filtering, and synthesis of literature on critical success factors for value management in cybersecurity within telecommunications organizations.

B. Conducting the Review

Initially, 950 articles were obtained through a search using keywords relevant to the study. This resulted in 49 articles, as shown in Fig. 2.

The recovered articles were imported into BibTeX format from the Parsifal tool to manage them centrally.

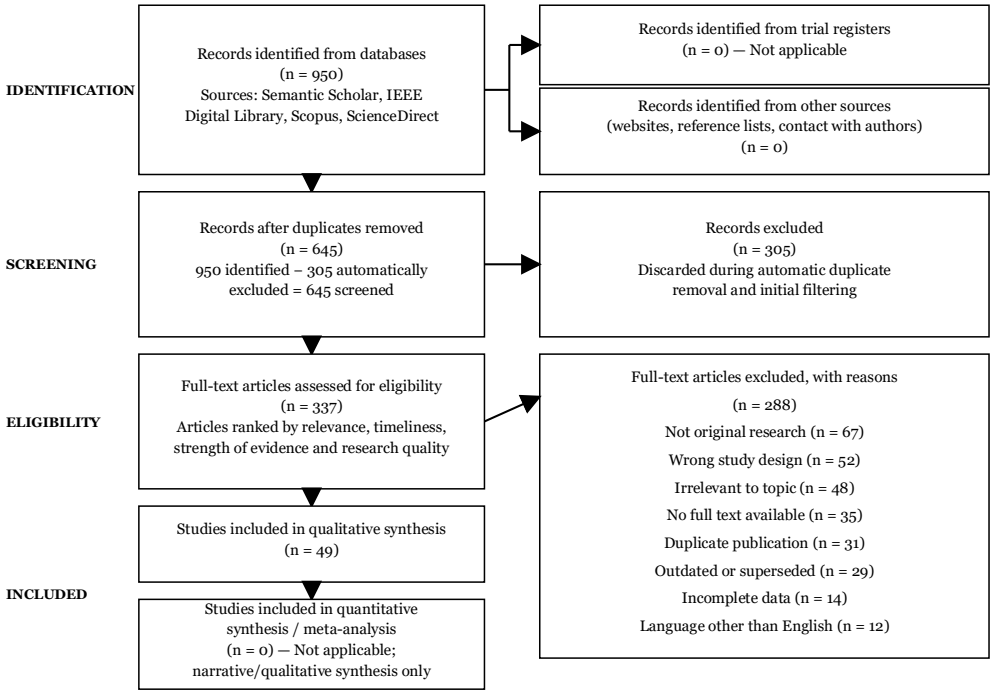


Fig. 2. PRISMA flow diagram summarizing the identification, screening, eligibility assessment, and inclusion of studies.

IV. Results

A. Publication Time Trends

Fig. 3 shows the temporal distribution of the 49 studies selected for the review between 2020 and 2025. The number of publications increased from 3 in 2020 to 7 in 2021, 13 in 2022, and 15 in 2023, then to 6 in 2024 and 5 in 2025. This distribution provides an initial descriptive view of the literature included in the review and shows that most of the selected evidence is concentrated between 2022 and 2023. However, publication frequency alone is insufficient to explain the critical factors that support value management in cybersecurity, nor should it be taken as evidence of the evolution or relevance of the research field. Therefore, this temporal characterization is used only as a starting point for the analysis of results, which is subsequently extended to examine the thematic patterns, critical success factors, and relationships identified across the selected studies.

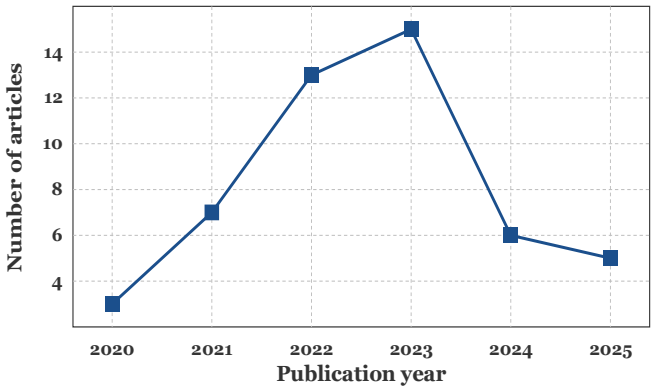


Fig. 3. Temporal distribution of the 49 included studies by publication year (2020–2025).

B. Author Productivity

Fig. 4 shows that Sawik, Saqib, and Islam recorded two verified publications each, while the other authors contributed one. Although this result points to limited recurrence among the ten most productive authors, it would be misleading to associate this pattern with a lack of scholarly interest. The figure reflects only the literature published and indexed during the period examined; consequently, it does not capture the full extent of ongoing research on value management in the telecommunications and cybersecurity fields. From a bibliometric perspective, this pattern suggests moderate fragmentation and shared leadership within the field.

The time required by journals and publishers to review, approve, edit, and index manuscripts is one factor that may help explain the relatively low publication frequency observed. This process can postpone the visibility of recent studies, particularly near the cutoff date of the analysis. This balanced structure may reflect a developing research field characterized by horizontal participation, where multiple contributors engage at similar levels of productivity. For this reason, the results should be regarded as a snapshot of the scientific output available at a specific point in time, rather than as a definitive indication of the international academic community's interest in the topic.

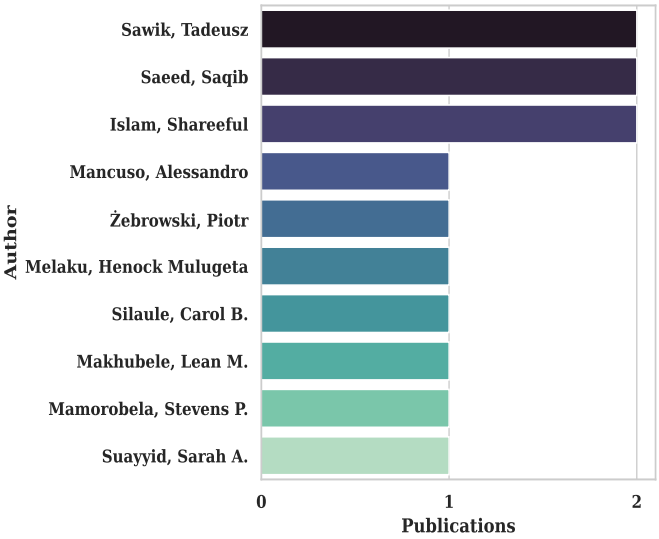


Fig. 4. Ten productive authors identified in the reviewed literature, ranked by number of verified publications on value management and cybersecurity.

C. Distribution by Journals

Fig. 5, the dominance of Sustainability, which alone accounts for slightly more than one-fifth of the 49 reviewed studies, indicates that a significant portion of the academic discourse is absorbed by interdisciplinary venues encompassing sustainability, management, technology, and systemic transformation. The Journal of Cybersecurity and Privacy's notable presence, capturing nearly one-sixth of publications, reflects the field's strong connection to security, privacy, and technological governance. At the same time, IEEE Access, Sensors, and Neural Computing and Applications reinforce its applied and technological dimensions, together accounting for over a quarter of the corpus and signaling a substantial engineering-oriented readership. SA Journal of Information Management, International Journal of Information Technology, and Pressacademia further extend this scope into organizational, technical, and economic dimensions of value management, even though each contributes a comparatively modest 5.3% share.

Additionally, Risk Analysis and the International Journal of Production Research demonstrate that the topic is approached from the perspectives of risk management, decision-making, and production systems, together representing another fifth of the total output. This layered structure—one dominant outlet, a secondary tier of four journals at 10.5%, and a long tail of four more at 5.3%—suggests a field still consolidating its primary publication venues rather than converging on a single specialized journal. Overall, the distribution underscores the field's interdisciplinary nature, where sustainability, security, technology, and management converge across diverse editorial spaces, reflecting the multifaceted character of value management research in cybersecurity and its resonance across engineering, business, and policy-oriented scholarly communities.

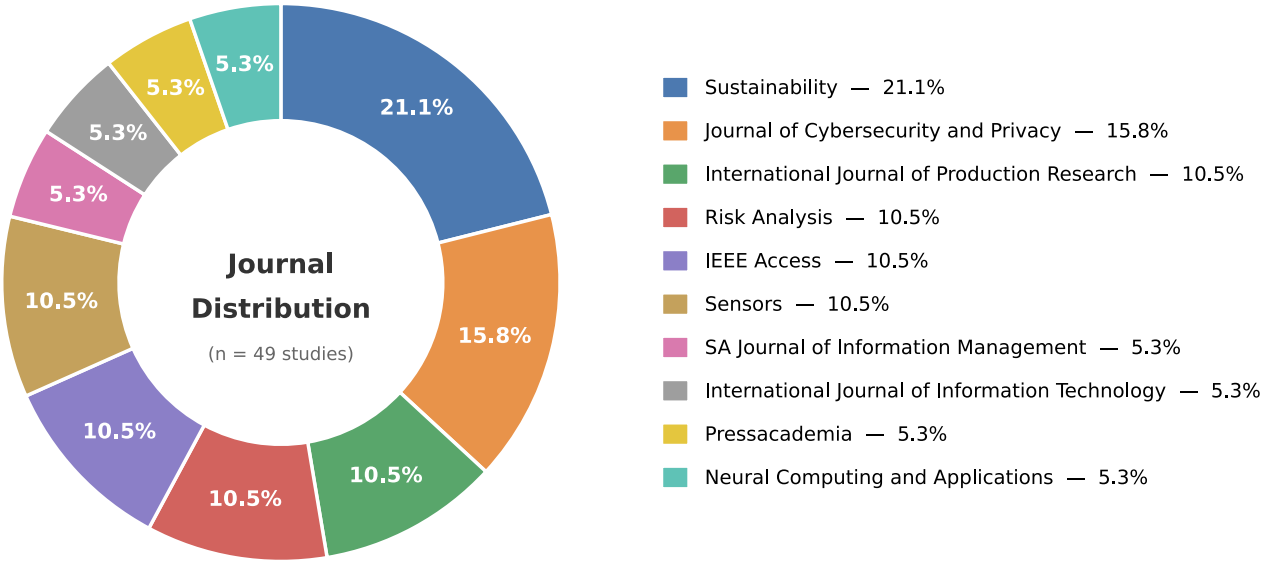


Fig. 5. Distribution of the 49 included studies across the journals with the highest publication counts.

D. Impact of the Works (Citations)

Fig. 6 shows the distribution of citations per publication, revealing a pronounced asymmetry. Most articles have fewer than 60 citations, while a small number reach much higher values, creating a long right tail in the distribution. Specifically, 31 of the 49 included studies, nearly two-thirds of the sample, accumulate fewer than 40 citations, while only five publications exceed 120, underscoring how rapidly citation frequency declines as the tail extends toward higher values, a pattern that favors median-based rather than mean-based summary statistics for this dataset. One publication with approximately 600 citations clearly stands out from the rest of the observations, highlighting an extreme value in the dataset under analysis.

The marked asymmetry and the presence of extreme values call for cautious interpretation of descriptive measures based on the arithmetic mean, given their sensitivity to observations of large magnitude. From this perspective, the observed distribution should be interpreted considering its asymmetry, to prevent the influence of a small subset of highly cited publications from shaping the understanding of the overall behavior of the analyzed scientific output. In view of the presence of an outlying datum, the authors identified the manuscript "Organizational Resilience: A Valuable Construct for Management Research?", which has approximately 600 citations. Its main contributions include, first, a review of criteria and constructs that facilitate understanding of firms' adaptive capacities in times of adversity or turbulence, and second, a methodological proposal for measuring resilience from a business-oriented perspective, regardless of the firm's classification, domain, or size.

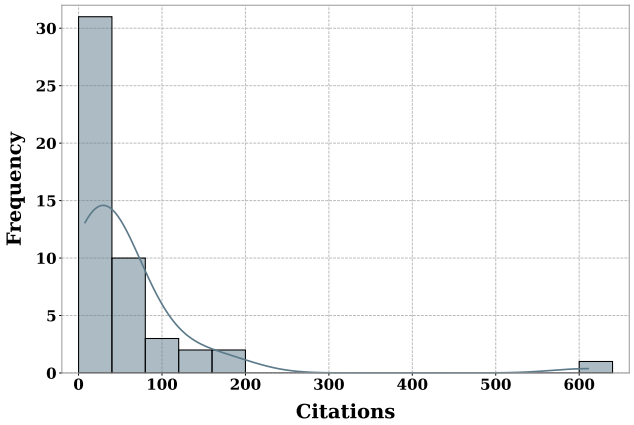


Fig. 6. Distribution of citation counts across the 49 included studies.

E. Types of Publications

Fig. 7 shows a moderate negative linear relationship (r = -0.34), suggesting that, in general, articles published in more recent years tend to receive fewer citations than those published in previous years. This behavior is consistent with the temporal logic of the scientific system, given that older documents have had greater visibility in reading and citation. At the same time, recent works have not yet completed their natural cycle of impact accumulation.

The negative slope of the linear regression curve, together with the dispersion of the points, shows that the relationship is not strictly deterministic; Although the time of publication influences the volume of citations, it is also true that there are old articles with relatively low impact, as well as publications from intermediate years that have reached high citation levels. This suggests that, in addition to the temporal effect, other

relevant factors are involved, such as the article's perceived quality, the journal's visibility, thematic relevance, and the contribution's innovative nature, among others.

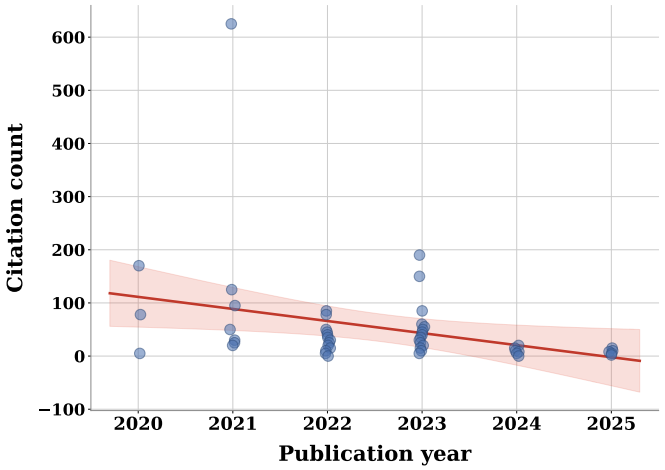


Fig. 7. Correlation between publication year and citation count (r = -0.34).

F. Impact of Categories

Fig. 8 shows the average number of citations across the analyzed thematic categories, revealing a heterogeneous distribution of citation impact among the publications considered. The category "Interagency collaboration and regulatory best practices" exhibits the highest average number of citations, with values near 165–170 citations per publication, whereas the remaining categories average only 25-50 citations per publication, with Organizational culture, Financial optimization, and Technology integration clustering near 48–50, while CTI and Governance trail near 38 and 27. Although these differences allow identification of variations in citation impact among the categories analyzed, their interpretation should be approached with caution. The average number of citations is a cumulative indicator that may be influenced by the time elapsed since publication, as older studies are more likely to have higher citation counts than those published more recently. Consequently, part of the differences observed between categories may reflect the temporal accumulation of citations rather than differences in citation impact associated with each topic. Likewise, Fig. 6 shows a pronounced asymmetry in the citation distribution due to outlying data, so comparisons based on the mean should be interpreted with caution, given the possible influence of a small number of highly cited publications on this statistic. Finally, the results should be understood as a descriptive characterization of citation behavior across thematic categories, rather than as conclusive evidence of the greater scientific relevance of one category over the others.

At a second level of impact, "Organizational culture and internal awareness", "Financial optimization and efficient allocation of resources", and "Technological integration and automation" appear, each with relatively close averages of 45-50 citations. This intermediate grouping suggests that these categories also have academic relevance, though with a narrower scope of influence than the leading category. On the other hand, the categories "Focus on Threat Intelligence and Predictive Analysis (CTI)" and "Governance and Adaptive Leadership in Cybersecurity" have the lowest citation averages, ranging from approximately 25 to 40 citations. These results cannot be interpreted as negative or incipient; rather, they demonstrate their scientific rigor to smaller audiences, or they may reflect a shorter bibliometric exposure time compared to categories with a longer history.

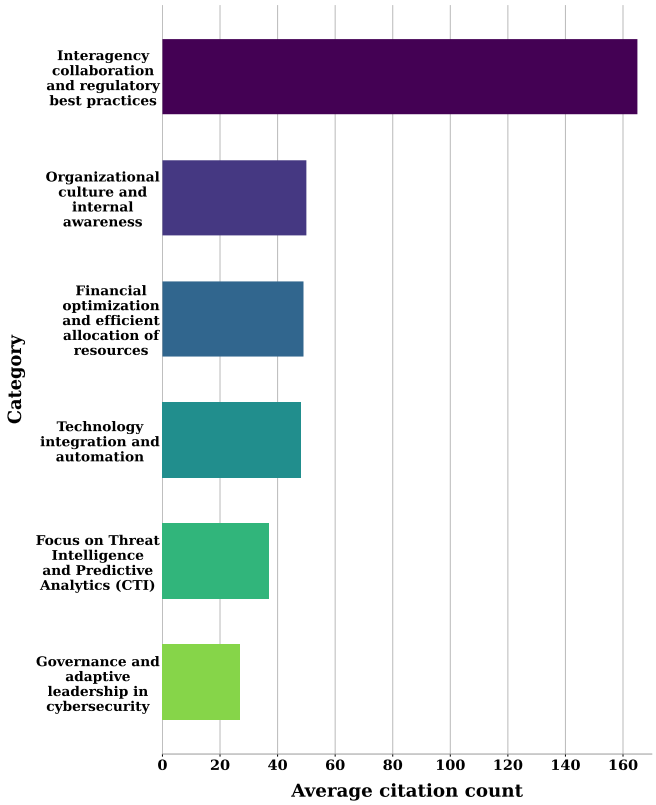


Fig. 8. Average number of citations per publication across the six critical success factor (CSF) categories.

G. Evolution

Fig. 9 reveals a heterogeneous and dynamic distribution of research categories between 2020 and 2025, reflecting the field's thematic evolution in response to emerging priorities and conceptual maturation. The most prominent finding is the peak of Governance and Adaptive Leadership in Cybersecurity in 2023, reaching 6 publications, the highest value in the entire matrix. This concentration suggests that scientific discourse in that year was particularly oriented toward governance frameworks, strategic leadership, and adaptive capacity in cybersecurity management.

Financial Optimization and Efficient Resource Allocation also showed notable activity, with 4 publications in 2022 and 3 in 2023, reflecting growing academic interest in translating cybersecurity strategies into economically viable decisions. Similarly, Organizational Culture and Internal Awareness consolidated in 2022 with 3 publications, underscoring a temporary but significant focus on human factors and the internalization of organizational security practices.

Technological Integration and Automation maintained a relatively stable presence throughout the period, ranging between 1 and 3 publications per year, with an early peak in 2020. This consistent trajectory suggests it constitutes a transversal and persistently relevant research line, though without the pronounced peaks observed in governance or resource allocation categories.

Inter-institutional Collaboration and Regulatory Best Practices, and Focus on Threat Intelligence and Predictive Analysis (CTI) exhibited lower, intermittent volumes. The former appeared sporadically in 2021, 2023, and 2025, while CTI reached its highest output in 2023 with 2 publications. Notably, despite its limited publication frequency, inter-institutional collaboration registered the highest average citation impact (Fig. 8), reinforcing the important distinction between thematic productivity and thematic influence; a few highly cited contributions can define a category's scientific weight regardless of publication volume.

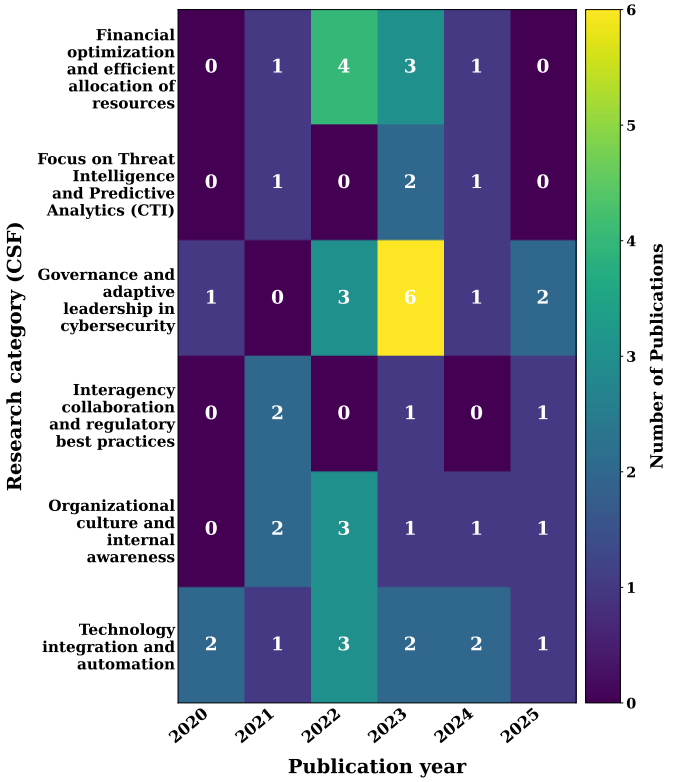


Fig. 9. Year-by-year evolution (2020–2025) of publications across the six critical success factor (CSF) categories, illustrating shifting research priorities over time.

H. Word Cloud

Fig. 10 shows a strong semantic concentration around terms that clearly delineate the thematic core of the field under analysis. The most prominent concepts: Cybersecurity, Framework, Security, Value, Management, Risk, Intelligence, Assessment, Resilience, and Infrastructure, indicate that the literature is primarily structured around the strategic management of cybersecurity, risk assessment, organizational resilience, and the formulation of conceptual and regulatory frameworks.

The visual dominance of Cybersecurity confirms its role as the central axis of articulation in scientific discourse. Its association with Framework, Management, Assessment, and Risk signals that academic production extends beyond isolated technical understanding, adopting analytical and strategic approaches to measuring and strengthening organizational threat-response capacity.

The prominence of terms such as Resilience, Infrastructure, Telecommunication, Industry, and Information reflects a clearly applied orientation that links the field to specific organizational environments, critical infrastructure, and productive sectors. Meanwhile, concepts like Intelligence, Threat, Digital Transformation, Compliance, Governance, and Trust reveal a research agenda that transcends conventional technical protection, encompassing anticipatory intelligence, regulatory alignment, and organizational governance. This reinforces the multidimensional and interdisciplinary nature of the domain, integrating technological, organizational, normative, and strategic components into a unified analytical perspective.

Finally, the recurrence of expressions such as Literature Review and Systematic Literature suggests a significant proportion of synthesis and conceptual structuring studies, indicative of an ongoing process of theoretical consolidation. Collectively, the word cloud confirms that the field has matured toward a comprehensive understanding of cybersecurity, in which technical, economic, regulatory, and organizational dimensions converge.



Fig. 10. Word cloud of terms extracted from the titles of the 49 included studies, highlighting the most frequent concepts in the reviewed literature.

I. Segmentation

Fig. 11 shows the classification of the selected publications into three clusters using k-means, with publication year and number of citations as the two input variables. Since the analysis was based on these two readily interpretable variables, clustering was used as a complementary descriptive approach to examine the distribution of publication recency and citation visibility across the reviewed literature.

The results show that Cluster 0 mainly comprises publications from 2023 to 2025 with low to moderate citation counts, consistent with their shorter time to accumulate citations. Cluster 2 is formed mostly by studies published

between 2020 and 2022 and presents greater variation in citation counts. This dispersion suggests that publication age alone does not explain citation visibility, as studies published in similar periods may still exhibit markedly different citation trajectories. Factors such as thematic relevance, journal visibility, and the extent to which a study becomes useful to subsequent research may also contribute to these differences.

Cluster 1 contains a single publication from 2021 with a substantially higher citation count than the rest of the corpus, clearly separating it from the other studies in the analysis. Rather than interpreting this case as evidence of a distinct level of scientific maturity or quality, it is more appropriately considered an outlier in the reviewed set of citations. Overall, the three clusters show that the literature does not exhibit a uniform citation pattern across publication years; instead, citation visibility varies with both recency and individual study trajectories. This segmentation therefore provides an additional descriptive perspective that complements the subsequent thematic and qualitative analysis of the critical success factors identified in the review.

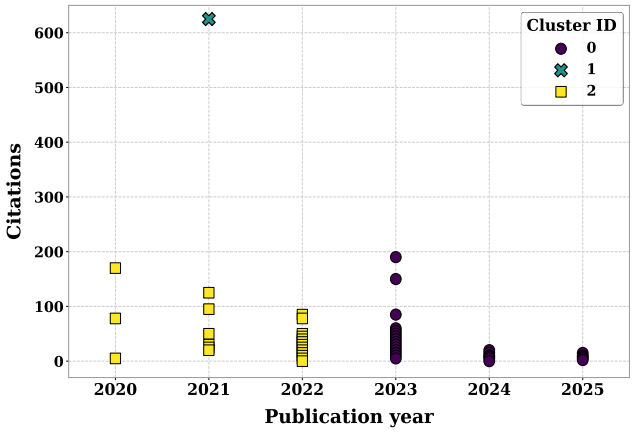


Fig. 11. K-means clustering of the 49 included studies by publication year and citation count.

J. Text Mining

Fig. 12 illustrates a thematic distribution in which risk management, literature review, and cybersecurity are the most recurrent emerging patterns. Risk management ranks as the most frequent phrase, followed by literature review, with terms such as cyber security, supply chain, and systematic literature also showing a prominent presence. This pattern suggests that recent scientific production is oriented not only toward understanding digital threats but also toward the conceptual and methodological systematization of accumulated knowledge.

The prominence of supply chain signals the field's expansion into interorganizational scenarios and complex value chains, where risk exposure extends beyond the boundaries of a single institution. Overall, emerging themes consolidate around three core areas: risk management, the development of analytical frameworks, and cybersecurity applied to organizational and supply chain environments. This reinforces the hypothesis that the field is evolving toward a broader, interdisciplinary research agenda focused on developing management models that are transferable to real-world contexts.

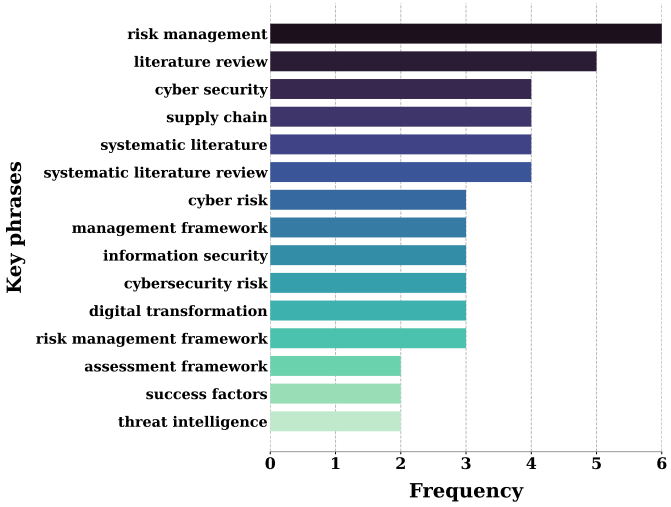


Fig. 12. Frequency of key phrases identified through text mining of the reviewed literature.

K. Categories and Critical Factors

The following section addresses the research question: What critical factors underpin the strategic relevance of value management in the cybersecurity strategies of telecommunications organizations? Table II shows the identified categories, their corresponding descriptions, and the critical success factors (CSF) associated with each.

Table II provides a categorized, general overview of the reviewed papers.

10% of studies propose: a Bayesian framework to optimize value decisions in cybersecurity of critical infrastructures and cite telecommunications networks as a case study; analysis of costs vs. impact of DDoS attacks on ISP providers; study cybersecurity value indicators in mobile network nodes; assess supply chain risks in fiber operators; quantify losses due to breaches and propose a system for prioritizing investments in security.

57% propose risk assessment frameworks based on the theory of value, cybersecurity ROI, and probabilistic frameworks (e.g., Bayesian, Monte Carlo) applicable to any critical infrastructure, without specific implementation in telecommunications; and governance and adaptive leadership studies in cybersecurity that discuss value management principles but lack sectoral examples.

32% propose methodologies for quantifying pure risk (e.g., vulnerability metrics, attack simulations) without any reference to value or network contexts; analysis of compliance frameworks or regulations that mention telecommunications as an actor among many other sectors.

Among the main limitations are the lack of uniform metrics and indicators as there is no common taxonomy to measure the value added or protected in telecommunications services; little empirical evidence in the field when presenting real cases reported by operators, and studies are usually based on simulated or generic data; finally, there is a lack of comparisons before and after implementing value frameworks, so that the effectiveness of management cannot be robustly evaluated.

TABLE II

CRITICAL SUCCESS FACTORS RELEVANT TO DIFFERENT CATEGORIES

Category	Description	Relevant CSF	Title
Interagency collaboration and regulatory best practices	Cooperation between organizations and compliance with regulations and standards, facilitating collective defense and coordinated response.	Inter-Agency Cooperation and Collaborative Policies to Strengthen Resilience to Threats	[41]
		Strategic alliances with key players in the digital ecosystem	[42]
		Partnership with secure suppliers and periodic third-party evaluation	[53]
		Effective coordination with regulators and government entities	[54]
Organizational culture and internal awareness	Recognize that the weakest link is often the user. It includes awareness, organizational culture, and insider threat management. Many studies highlight the development of a strong internal culture in which employees serve as the first line of defense.	Fostering a strong organizational culture and standards to avoid insider threats	[55]
		Management and continuous updating of cybersecurity staff competencies and skills	[56]
		Awareness and continuous training of end users	[47]
		Sensitive data management strategies to reduce vulnerabilities	[57]
		Use of periodic tests and simulations (cybersecurity exercises) to verify effectiveness	[58]
		Strengthening internal communication and timely reporting of incidents	[59]
		Training and technological updating programs specific to security teams	[60]
		Design of specific security change management programs	[61]
Governance and adaptive leadership in cybersecurity	Organizational ability to adjust cybersecurity policies and processes in the face of changes in threats, regulations, and objectives, with active and flexible leadership.	Adaptive and dynamic governance as a basis for confronting emerging threats	[45]
		Standardization through regulatory frameworks adjusted to the telecommunications sector	[62]
		Rapid response and continuous post-incident learning to minimize impacts	[63]
		Developing clear identity management and access policies	[48]
		Integration of new international regulations for industry compliance	[64]
		Adoption of methodologies for periodic assessment of risks and vulnerabilities	[65]
		Enforce strict access and privilege control policies	[66]
		Implementation of contingency and disaster recovery plans integrated into the processes	[67]
		Definition and systematic review of security policies aligned with the organizational strategy	[68]
		Senior management involvement and the existence of cybersecurity committees	[69]
		Implementation of regular and external audits in cybersecurity	[44]
		Consistent alignment of security strategy with business objectives	[70]
		Customization of security policies according to the type of customers	[50]
Technology integration and automation	It comprises technological infrastructure, encryption, and network security (ICT). It is the technical execution that protects the integrity and availability of data. Relevance of incorporating advanced technologies (AI, automation, structured frameworks) as key enablers to protect value.	Driving technological innovation (AI, automation, deep learning) as a catalyst for protection	[71]
		Application of a holistic approach that integrates processes, people, and technology in the management of value in cybersecurity	[72]
		Implementation of automated systems for incident detection and response	[46]
		Agile incorporation of scalable technology solutions based on business growth	[73]
		Deployment of critical network segmentation and isolation strategies	[74]
		Sustainability and integration of long-term security solutions into the infrastructure	[75]
		Automation and orchestration of incident response processes	[76]
		Continuous, centralized monitoring of security events	[77]
		Adaptability of cybersecurity architecture to new technologies and threats	[78]
		Diversifying defense technologies to reduce single points of failure	[79]
		Integration of robust encryption mechanisms into systems and communications	[80]
Focus on Threat Intelligence and Predictive Analytics (CTI)	Focuses on incident resilience by minimizing downtime and maintaining operations after attacks. Threat intelligence and advanced analytics enable proactive cybersecurity, support investment decisions, and help anticipate, detect, and mitigate risks.	Integration and effective application of threat intelligence (CTI) to anticipate and mitigate risks	[81]
		Prioritization of emerging risks through artificial intelligence and analysis of large volumes of data	[82]
		Proactive assessment of exposure to new and emerging threats	[83]
		Digital Forensics Application for Lessons Learned and Process Improvement	[43]
Financial optimization and efficient allocation of resources	It focuses on financial efficiency, seeking the maximum return on investment (ROI) and cost-benefit ratio of installed security tools. Mathematical and decision-making models that maximize cybersecurity return on investment and are aligned with the business strategy are a recurring CSF.	Probabilistic model-based optimization for effective cybersecurity investment	[84]
		Using mathematical models to maximize return and efficiency on cybersecurity investment	[85]
		Risk-based prioritization for security decisions	[86]
		Measuring and demonstrating the value of cybersecurity investment in terms of business continuity	[87]
		Implementation of clear and tangible metrics to evaluate cybersecurity performance	[88]
		Ongoing economic evaluation and alignment of security investment with business objectives	[89]
		Application of cost-benefit analysis to justify investments in cybersecurity	[90]
		Establishing cybersecurity-specific key performance indicators (KPIs)	[91]
		Prioritization of investments based on potential impact and criticality of the service	[92]

Table III presents the results of a thematic analysis using Non-negative Matrix Factorization (NMF) theme modeling. Six key themes were identified in the 49 studies: 1. Intelligence and risk management frameworks; 2. Organizational culture and norms; 3. Innovation and alignment frameworks with objectives; 4. Competitive advantage and dynamic strategy; 5. Human factors management and awareness-raising; and 6. Digital transformation in telecommunications.

The topics shown in Table III synthesize the main findings of the studies and provide a structured overview of research and practical priorities in value management for cybersecurity processes in telecommunications.

V. Discussion

The six CSF categories identified from the literature synthesis challenge and enrich the interpretation of the COBIT 2019 and ITIL frameworks in the domain of cybersecurity for telecommunications.

First, adaptive governance and leadership in cybersecurity deepens and specializes the dynamic principle of the COBIT governance system (design factors, threat landscape, risk profile) and the governance of the ITIL SVS Service Value System, guiding them to security decisions that are sensitive to change and directly linked to value, risk, and resources in critical infrastructures. In turn, technology integration and automation together with the focus on threat intelligence and predictive analytics reinterpret the information and technology dimension of ITIL and COBIT's services, infrastructure and application components, shifting the focus from supporting technology to advanced capabilities as central enablers of resilience, continuity and economic and strategic justification of security investments.

Second, organizational culture and internal awareness and inter-institutional collaboration and regulatory best practices expand the dimension of organizations and people, partners and suppliers, and value streams of ITIL, as well as the components of culture, organizational structures, and compliance in COBIT, by showing that value protection in telecommunications depends as much on user and employee behavior as on coordination between operators, suppliers, and regulators.

Finally, the category of financial optimization and efficient allocation of resources puts the treatment of value in both frameworks under tension, as it forces an explicit connection between business objectives, return on investment, and the cost-benefit of cybersecurity controls and technologies and COBIT governance objectives and ITIL service financial management practices. Transforming security from a cost center to a strategic capacity for value creation and preservation. Together, the six categories articulate a set of CSFs to generate value that integrates IT governance and IT service management around value management in cybersecurity processes for telecommunications, challenging both models to evolve towards more value-oriented configurations, dynamic risk, and ecosystem cooperation.

The analysis confirms that inter-institutional collaboration and sound regulatory practices, when embedded within clearly defined and audited CSF frameworks, enhance the resilience and maturity of the digital ecosystem. However, persistent challenges remain in measuring resilience, sustaining partnerships, and adapting regulations to evolving threats. A cross-cutting challenge is translating collaborative intent into operational structures with defined roles, metrics, and information flows that can manage complex incidents and shifting regulatory contexts.

Governance and adaptive leadership in cybersecurity extend beyond strategic declarations; they are operationalized through context-specific policies, resilience metrics, continuous auditing, and active engagement by senior management. Empirical evidence on the comprehensive effectiveness of these factors remains limited, positioning the integration of regulatory frameworks, adaptive models, and business value creation as a central line for future research.

TABLE III
THEMATIC SYNTHESIS OF QUALITATIVE FINDINGS

Theme	Key terms	Findings
Risk intelligence and management	cyber, security, risk, intelligence, management, resilience, approach, threat, attacks	Threat intelligence and risk management frameworks strengthen organizational resilience to cyberattacks
Organizational culture and value	value, significantly, company, security, threats, impact, information, influence, compliance, internal	Standards and corporate culture significantly influence compliance and the perceived value of cybersecurity initiatives.
Innovation and alignment with objectives	innovation, framework, cybersecurity, critical, effectively, alignment, document, nist, objectives, value	The adoption of innovation frameworks (e.g., NIST) facilitates value creation by integrating cybersecurity with strategic objectives.
Competitive advantage and dynamic strategy	competitive, advantage, dynamic, future, cybersecurity, research, business, strategic, impact, management	Dynamic cybersecurity capabilities can be transformed into sustainable competitive advantage.
Human factors and awareness	factors, human, communication, effective, management, address, awareness, cybersecurity, education, gaps	Human factors management—through training and communication—is essential to reducing security breaches.
Digital transformation and operational efficiency	industry, digital, systems, transformation, risks, cybersecurity, adapt, comprehensive, efficient, performance	The digital transition in telecommunications requires adaptive risk management systems to maintain efficiency and performance.

Technological integration and automation yield concrete benefits in both preventive management and incident response; however, the human component and strategic alignment remain decisive, underscoring the need for hybrid rather than purely technological approaches. A key limitation of this review is the scarcity of evidence on certain proposed CSF and potential bias in the available bibliographic corpus, which warrants caution in generalizing findings and reinforces the need to broaden the evidence base in future work.

Organizations aspiring to manage value and resilience in cybersecurity must treat culture, awareness, and talent management as cross-cutting strategic priorities, with dedicated indicators and a long-term perspective that transcends isolated audits or one-off awareness campaigns. Identified limitations include a lack of robust metrics to assess cultural maturity, organizational resistance to change, and user fatigue due to escalating security demands. The core challenge is ensuring that the cultural evolution of cybersecurity shifts from reactive incident response to an integral component of the organization's strategic identity and value proposition.

VI. Conclusions

A. Contribution

The literature proposes theoretical models for managing specific value and risk in cybersecurity, but only a small number explicitly apply them to telecommunications networks or infrastructure providers. Although these direct studies recognize relevant risks and suggest preliminary metrics, the lack of empirical validation and shared standards prevents drawing the conclusion that operators are managing value coherently and in proportion to its impact. The main gap continues to be the absence of comprehensive value metrics and real cases that support the value-risk relationship in the telecom sector in a robust way.

Value management in cybersecurity is recognized as a fundamental strategic element in telecommunications. The CSF underpinning its importance is multidimensional, encompassing strategic governance and leadership, risk and asset management, threat intelligence, organizational culture, and dynamic technology integration aligned with business objectives.

Evidence indicates that technological integration and automation yield solid results only when embedded in a holistic approach that aligns technical capabilities, process coordination, investment decisions, and human behavior. Within this framework, organizational culture and internal awareness are not peripheral elements but necessary conditions, sustained through clear policies, continuous training, effective communication, and visible leadership commitment. The CSF linked to Threat Intelligence and Predictive Analytics (CTI) reinforces this holistic view, demonstrating that anticipation, prioritization, and systematic assessment tangibly enhance responsiveness to evolving risk environments.

From an economic perspective, financial optimization CSF converges on the need for formal models that guide investment decisions, quantify risk and value, and connect security spending to business impact, operational continuity, and service criticality. Granular indicators and periodic reviews enable focused monitoring and timely adjustments, ensuring effective resource allocation over the medium and long term. Critically, risk prioritization extends beyond technical analysis; it depends equally on governance quality and organizational maturity. The interaction among economic decisions, technical capabilities, and cultural practices ultimately explains how cybersecurity value is realized within telecommunications organizations.

B. Future Research

Among the main challenges identified are the absence of standardized metrics to measure the return on investment in cybersecurity, the difficulty in balancing technological innovation with compliance with regulatory requirements, the global shortage of specialized talent in the domain, and the growing complexity derived from the convergence of technologies such as artificial intelligence, Internet of Things, and blockchain [93], [94], [95]. However, the most important challenge this work will continue to address is the design of a comprehensive value framework for cybersecurity processes in telecommunications organizations.

Acknowledgments

The Economic and Administration Investigation Group and the Military Applications Research Center at Universidad de las Fuerzas Armadas ESPE supported this work. This manuscript was revised with the assistance of artificial intelligence tools (Perplexity and paper banana) to enhance its semantic clarity and correct grammatical issues.

References

[1] Netskope, “Cloud and Threat Report: 2025,” Netskope. Accessed: Sep. 28, 2025. [Online]. Available: https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-2025

[2] P. Barrios, “Telecom Cybersecurity Strategies That Protect Customer Information,” Valor Global. Accessed: Aug. 20, 2025. [Online]. Available: https://valorglobal.com/telecom-cybersecurity-strategies-that-protect-customer-information/

[3] R. Watson and R. Bergman, “Cybersecurity: From value protection to value creation | EY - Global,” Cybersecurity: From value protection to value creation | EY - Global. Accessed: Aug. 20, 2025. [Online]. Available: https://www.ey.com/en_gl/insights/consulting/how-can-cybersecurity-go-beyond-value-protection-to-value-creation

[4] Chitopoulos, “Amid Cyberthreats, Telecom Companies Must Balance Security with Innovation,” Cyber Defense Magazine. Accessed: Feb. 25, 2026. [Online]. Available: https://www.cyberdefensemagazine.com/amid-cyberthreats-telecom-companies-must-balance-security-with-innovation/

[5] I. Balodis, “Cybersecurity in the Digital Age: Threats, Challenges, and Strategic Responses,” Feb. 19, 2025. doi: 10.2139/ssrn.5144431.

[6] S. Garai and Z. Taskeen, “Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers,” Blockchain in Healthcare Today, vol. 7, no. 1, 2024, doi: 10.30953/bhty.v7.302.

[7] K. Jaggi, “Advancing Cybersecurity Strategies: Balancing Threat Detection, Compliance, and Resilient Architectures,” Feb. 04, 2025, SSRN. doi: 10.2139/ssrn.5124287..

[8] K. Khadka, “Forecasting Risks, Challenges, and Innovations: A Cybersecurity Perspective,” Dec. 21, 2024, Social Science

Research Network, Rochester, NY: 5187659. doi: 10.2139/ssrn.5187659.

[9] S. AlDaajeh and S. Alrabaee, "Strategic cybersecurity," Computers & Security, vol. 141, p. 103845, Jun. 2024, doi: 10.1016/j.cose.2024.103845.

[10] F. Heiding, A. O'Neill, and L. Price, "Cybersecurity Strategy Scorecard | The Belfer Center for Science and International Affairs." Mar. 27, 2025. Accessed: Jul. 18, 2025. [Online]. Available: https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard

[11] T. Johansmeyer, G. Mott, and J. R. C. Nurse, "Cyber Strategy in Practice: The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experience of War," The RUSI Journal, vol. 169, no. 3, pp. 40–51, Apr. 2024, doi: 10.1080/03071847.2024.2377544.

[12] M. Clarke and K. Martin, "Managing cybersecurity risk in healthcare settings," Healthcare Management Forum, vol. 37, no. 1, pp. 17–20, 2024, doi: 10.1177/08404704231195804.

[13] I. Thornton-Trump, "State of Cybersecurity 2025: Trends, Insights and Strategies for Resilience," 2025. [Online]. Available: https://whitepapers.theregister.com/paper/view/40177/state-of-cybersecurity-2025-trends-insights-and-strategies-for-resilience

[14] The Institute of Value Management, "Value Management Standards, applying best practice," The Standard BS EN12973:2020 represents a consensus of views and provides a benchmark of best practice. Accessed: Jul. 20, 2025. [Online]. Available: https://ivm.org.uk/value-management/standards/

[15] M. Law, "EY Study: How Cybersecurity Adds $36m Value per Initiative," Cloud & Cybersecurity. Accessed: Feb. 25, 2026. [Online]. Available: https://technologymagazine.com/articles/ey-study-how-cybersecurity-adds-36m-value-per-initiative

[16] K. Maes, S. De Haes, and W. Van Grembergen, "Developing a Value Management Capability: A Literature Study and Exploratory Case Study," Information Systems Management, vol. 32, no. 2, pp. 82–104, Apr. 2015, doi: 10.1080/10580530.2015.1018767.

[17] R. H. Ashton, "Value-Creation Models for Value-Based Management: Review, Analysis, and Research Directions," in Advances in Management Accounting, vol. 16, Bingley: Emerald (MCB UP), 2007, pp. 1–62. doi: 10.1016/S1474-7871(07)16001-9.

[18] G. Barbieri, A. M. Benavides, L. A. Esteves, C. Olaya, and F. Zapata, "Organizational Value Framework for Asset Management Decision-Making," IFAC-PapersOnLine, vol. 58, no. 8, pp. 395–400, 2024, doi: 10.1016/j.ifacol.2024.08.153.

[19] X. Li, B. Deng, Y. Yin, and Y. Jia, "Critical Obstacles in the Implementation of Value Management of Construction Projects," Buildings, vol. 12, no. 5, p. 680, May 2022, doi: 10.3390/buildings12050680.

[20] F. Rowe, "What literature review is not: diversity, boundaries and recommendations," European Journal of Information Systems, vol. 23, no. 3, pp. 241–255, May 2014, doi: 10.1057/ejis.2014.7.

[21] M. Genero Bocco, Métodos de investigación en ingeniería del software. Madrid: RA-MA Editorial, 2014.

[22] B. Kitchenham and S. Charters, "Guidelines for Performing Systematic Literature Reviews in Software Engineering," Technical report, EBSE Technical Report EBSE-2007-01, 2007..

[23] W. Mengist, T. Soromessa, and G. Legese, "Method for conducting systematic literature review and meta-analysis for environmental science research," MethodsX, vol. 7, p. 100777, 2020, doi: 10.1016/j.mex.2019.100777.

[24] G. Lindemulder and M. Kosinski, "¿Qué es la ciberseguridad? | IBM," ¿Qué es la ciberseguridad? | IBM. Accessed: Jul. 20, 2025. [Online]. Available: https://www.ibm.com/es-es/topics/cybersecurity

[25] F. Schiliro, "Towards a Contemporary Definition of Cybersecurity," 2023, arXiv. doi: 10.48550/ARXIV.2302.02274.

[26] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," JCSANDM, vol. 4, no. 1, pp. 65–88, May 2015, doi: 10.13052/jcsm2245-1439.414.

[27] DHS, "A Glossary of Common Cybersecurity Terminology," A Glossary of Common Cybersecurity Terminology. Accessed: Jul. 20, 2025. [Online]. Available: https://niccs.cisa.gov/resources/glossary

[28] ISO/IEC 27032:2023(en), Cybersecurity — Guidelines for Internet security, 2023. Accessed: Apr. 24, 2020. [Online]. Available: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27005:ed-3:v1:en

[29] A. Dengkeng, A. Halid, G. Pratiwi, A. I. Rachman, S. B, and L. F. Mz, "Cyber Security Challenges and Solutions in Critical Infrastructure: A Systematic Review of Threat Spectrum, Systemic Vulnerabilities, and Multi-Level Protection Strategies," JLMA, vol. 6, no. 5, pp. 1183–1193, Sep. 2025, doi: 10.37899/journallamultiapp.v6i5.2469.

[30] Y. N. Bravo Delgado and D. F. Zambrano Montenegro, "Seguridad y privacidad en las redes 5g: una revisión sistemática de la literatura: Security and privacy in 5g networks: a systematic literature review," Rev. Cient. Multi. G-nerando, vol. 5, no. 2, Jul. 2024, doi: 10.60100/rcmg.v5i2.259.

[31] Y. Khourdifi, A. El Alami, M. Zaydi, Y. Maleh, and M. Bahaj, "Navigating the cybersecurity maze," in Agile Security in the Digital Era, 1st ed., Boca Raton: CRC Press, 2024, pp. 1–18. doi: 10.1201/9781003478676-1.

[32] RAE, "valor | Diccionario de la lengua española," «Diccionario de la lengua española» - Edición del Tricentenario. 2025. Accessed: Mar. 03, 2026. [Online]. Available: https://dle.rae.es/valor

[33] H. C. C. D. Silva, D. S. D. Silveira, J. S. Dornelas, and H. S. Ferreira, "Information Technology Governance in Small and Medium Enterprises - a Systematic Mapping," JISTEM USP, vol. 17, Dec. 2019, doi: 10.4301/S1807-1775202017001.

[34] A. Levstek, T. Hovelja, and A. Pucihar, "IT Governance Mechanisms and Contingency Factors: Towards an Adaptive IT Governance Model," Organizacija, vol. 51, no. 4, pp. 286–310, Dec. 2018, doi: 10.2478/orga-2018-0024.

[35] B. H. Díaz Pinzón, J. S. Gómez Medina, J. D. García González, H. A. Melo Román, and F. E. Sanabria Villamizar, "Contribución de las iniciativas de tecnologías de la información en las organizaciones: una revisión de la literatura," Innovar, vol. 27, no. 66, pp. 41–55, Oct. 2017, doi: 10.15446/innovar.v27n66.66710.

[36] M. Thiry, A framework for value management practice, Second edition. Newtown Square, Pennsylvania: Project Management Institute, Inc, 2013.

[37] E. De Bono, Lateral Thinking: Creativity step by step. New York: Harper & Row, 1973.

[38] Institute Value Management, "Value Management," IVM. Accessed: Mar. 03, 2026. [Online]. Available: https://ivm.org.uk/value-management/

[39] British Standards Institution, BS EN 1325:2014 Value Management. Vocabulary. Terms and definitions, BS EN 1325:2014, London., 2014. Accessed: Aug. 15, 2025. [Online]. Available: https://knowledge.bsigroup.com/products/value-management-vocabulary-terms-and-definitions

[40] British Standards Institution, BS EN 12973:2020 Value Management, BS EN 12973:2020, London., 2020. Accessed: Sep. 28, 2020. [Online]. Available: https://shop.bsigroup.com/ProductDetail/?pid=000000000030314082

[41] L. Alevizos, L. Bhakuni, and S. Jäschke, "A value driven framework for cybersecurity innovation in transportation and infrastructure," International Journal of Information Technology, vol. 17, no. 1, pp. 321–331, Jan. 2025, doi: 10.1007/s41870-024-02288-w.

[42] C. Aksoy, "Are critical success factors for cybersecurity just technical issues Cybersecurity management and the human factor," Pressacademia, p. 2, Jun. 2023, doi: 10.17261/Pressacademia.2023.1735.

[43] I. Jebril, R. Almaslmani, B. A. F. Jarah, M. I. Mugableh, and N. Zaqeeba, "The impact of strategic intelligence and asset management on enhancing competitive advantage: The mediating role of cybersecurity," 10.5267/j.uscm, vol. 11, no. 3, pp. 1041–1046, 2023, doi: 10.5267/j.uscm.2023.4.018.

[44] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," Sustainability, vol. 15, no. 7, p. 5828, Mar. 2023, doi: 10.3390/su15075828.

[45] H. M. Melaku, "A Dynamic and Adaptive Cybersecurity Governance Framework," Journal of Cybersecurity and Privacy, vol. 3, no. 3, pp. 327–350, Jun. 2023, doi: 10.3390/jcp3030017.

[46] W. Okori and S. Buteraba, "Cyber Security Exploits and Management in Telecommunication Companies: The Case of Uganda," Journal of Computer Science and Technology Studies, vol. 6, no. 4, pp. 67–76, Oct. 2024, doi: 10.32996/jcsts.2024.6.4.10.

[47] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," Sustainability, vol. 15, no. 18, p. 13369, Sep. 2023, doi: 10.3390/su151813369.

[48] W. Tan, B. Guo, and Q. Zhang, "Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust," Pacific-Basin Finance Journal, vol. 90, p. 102646, Apr. 2025, doi: 10.1016/j.pacfin.2024.102646.

[49] W. Yeoh, S. Wang, A. Popovič, and N. H. Chowdhury, "A systematic synthesis of critical success factors for cybersecurity," Computers & Security, vol. 118, p. 102724, Jul. 2022, doi: 10.1016/j.cose.2022.102724.

[50] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework," Computers & Security, vol. 133, p. 103412, Oct. 2023, doi: 10.1016/j.cose.2023.103412.

[51] M. Petticrew and H. Roberts, Systematic Reviews in the Social Sciences: A Practical Guide, 1st ed. Wiley, 2006. doi: 10.1002/9780470754887.

[52] M. J. Page et al., "PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews," BMJ, p. n160, Mar. 2021, doi: 10.1136/bmj.n160.

[53] 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, Nov. 2021, doi: 10.1016/j.future.2021.05.033.

[54] J. Hillmann and E. Guenther, "Organizational Resilience: A Valuable Construct for Management Research?," Int J Management Reviews, vol. 23, no. 1, pp. 7–44, Jan. 2021, doi: 10.1111/ijmr.12239.

[55] C. B. Silaule, L. M. Makhubele, and S. P. Mamorobela, "A model to reduce insider cybersecurity threats in a South African telecommunications company," SA Journal of Information Management, vol. 24, no. 1, Oct. 2022, doi: 10.4102/sajim.v24i1.1573.

[56] A. Onumo, I. Ullah-Awan, and A. Cullen, "Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures," ACM Transactions on Management Information Systems, vol. 12, no. 2, pp. 1–29, Jun. 2021, doi: 10.1145/3424282.

[57] I. Bongiovanni, D. Goyeneche, E. Tsen, E. C. James, P. Singh, and R. Ko, "Cyber-attackers as a social force: conceptualizing value sabotage in cybersecurity services," Journal of Service Management, vol. ahead-of-print, no. ahead-of-print, pp. 1–32, Dec. 2025, doi: 10.1108/JOSM-12-2024-0537.

[58] Manuel De Nicola and Christo Delightson David Raja, "Cybersecurity and Blockchain Impacts on Value Creation Process: Empirical Evidences From Non-financial Disclosure," Journal of Modern Accounting and Auditing, vol. 18, no. 6, Jun. 2022, doi: 10.17265/1548-6583/2022.06.001.

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

[60] M. F. Arroyabe, C. F. A. Arranz, I. Fernandez De Arroyabe, and J. C. Fernandez De Arroyabe, "Exploring the economic role of cybersecurity in SMEs: A case study of the UK," Technology in Society, vol. 78, p. 102670, Sep. 2024, doi: 10.1016/j.techsoc.2024.102670.

[61] A. Creazza, C. Colicchia, S. Spiezia, and F. Dallari, "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era," Supply Chain Management: An International Journal, vol. 27, no. 1, pp. 30–53, Jan. 2022, doi: 10.1108/SCM-02-2020-0073.

[62] T. Sawik, "Balancing cybersecurity in a supply chain under direct and indirect cyber risks," International Journal of Production Research, vol. 60, no. 2, pp. 766–782, Jan. 2022, doi: 10.1080/00207543.2021.1914356.

[63] P. R. J. Trim and Y.-I. Lee, "Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience," Big Data and Cognitive Computing, vol. 6, no. 4, p. 110, Oct. 2022, doi: 10.3390/bdcc6040110.

[64] T. Bailetti and D. Craigen, "Examining the Relationship between Cybersecurity and Scaling Value for New Companies," Technology Innovation Management Review, vol. 10, no. 2, pp. 62–69, Feb. 2020, doi: 10.22215/timreview/1329.

[65] P. S. Aithal, "How to Create Business Value Through Technological Innovations Using ICCT Underlying Technologies," International Journal of Applied Engineering and Management Letters (IJAEML), vol. 7, no. 2, pp. 232–292, Jun. 2023, doi: 10.47992/IJAEML.2581.7000.0184.

[66] M. Lezzi, A. Corallo, M. Lazoi, and A. Nimis, "Measuring cyber resilience in industrial IoT: a systematic literature review," Management Review Quarterly, 2025, doi: 10.1007/s11301-025-00495-8.

[67] D. Botha-Badenhorst, "Navigating the Intersection of Innovation and Cybersecurity: A Framework," European Conference on Research Methodology for Business and Management Studies, vol. 22, no. 1, pp. 18–25, Aug. 2023, doi: 10.34190/ecrm.22.1.1490.

[68] M. F. Franco, F. Künzler, J. von der Assen, C. Feng, and B. Stiller, "RCVaR: an Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports," 2023, arXiv. doi: 10.48550/ARXIV.2307.11140.

[69] G. P. Platunina, T. Y. Salutina, and I. A. Frank, "Risk Management of Data Transmission Within the Framework of the Digital Transformation of the Telecommunications

Industry," in 2024 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria: IEEE, Oct. 2024, pp. 1–5. doi: 10.1109/EMCTECH63049.2024.10741645.
[70] C.-N. Wang, F.-C. Yang, N. T. M. Vo, and V. T. T. Nguyen, "Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry—A Promising Application for UAVs," Drones, vol. 6, no. 11, p. 363, 2022, doi: 10.3390/drones6110363.
[71] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," Neural Computing and Applications, vol. 34, no. 18, pp. 15241–15271, Sep. 2022, doi: 10.1007/s00521-022-06959-2.
[72] M. Tsiodra, S. Panda, M. Chronopoulos, and E. Panaousis, "Cyber Risk Assessment and Optimization: A Small Business Case Study," IEEE Access, vol. 11, pp. 44467–44481, 2023, doi: 10.1109/ACCESS.2023.3272670.
[73] D. Kosutic and F. Pigni, "Cybersecurity: investing for competitive outcomes," Journal of Business Strategy, vol. 43, no. 1, pp. 28–36, Jan. 2022, doi: 10.1108/JBS-06-2020-0116.
[74] K. Kostelić, "Dynamic Awareness and Strategic Adaptation in Cybersecurity: A Game-Theory Approach," Games, vol. 15, no. 2, p. 13, Apr. 2024, doi: 10.3390/g15020013.
[75] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance," Applied Sciences, vol. 11, no. 8, p. 3383, Apr. 2021, doi: 10.3390/app11083383.
[76] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," Journal of Cybersecurity, vol. 6, no. 1, p. tyaa005, Jan. 2020, doi: 10.1093/cybsec/tyaa005.
[77] S. Islam, N. Basheer, S. Papastergiou, M. Ciampi, and S. Silvestri, "Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure," Journal of Reliable Intelligent Environments, vol. 11, no. 3, p. 12, Sep. 2025, doi: 10.1007/s40860-025-00253-3.
[78] Z. Bederna and T. Szádeczky, "Managing the financial impact of cybersecurity incidents," Security and Defence Quarterly, vol. 41, no. 1, pp. 15–35, 2023, doi: 10.35467/sdq/159625.
[79] A. A. Ganin et al., "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," Risk Analysis, vol. 40, no. 1, pp. 183–199, Jan. 2020, doi: 10.1111/risa.12891.
[80] M. A. Hajar et al., "The Effect of Value Innovation in the Superior Performance and Sustainable Growth of Telecommunications Sector: Mediation Effect of Customer Satisfaction and Loyalty," Sustainability, vol. 14, no. 10, p. 6342, May 2022, doi: 10.3390/su14106342.
[81] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," Sensors, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273.
[82] A. Orlando, "Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk," Risks, vol. 9, no. 10, p. 184, 2021, doi: 10.3390/risks9100184.
[83] Philip Olaseni Shoetan, Olukunle Oladipupo Amoo, Enyinaya Stefano Okafor, and Oluwabukunmi Latifat Olorunfemi, "Synthesizing AI'S Impact on Cybersecurity in Telecommunications: A Conceptual Framework," Comput. sci. IT res. j., vol. 5, no. 3, pp. 594–605, Mar. 2024, doi: 10.51594/csitrj.v5i3.908.
[84] P. Żebrowski, A. Couce-Vieira, and A. Mancuso, "A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems," Risk Analysis, vol. 42, no. 10, pp. 2275–2290, Oct. 2022, doi: 10.1111/risa.13900.
[85] T. Sawik, "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains," International Journal of Production Research, vol. 60, no. 4, pp. 1368–1385, Feb. 2022, doi: 10.1080/00207543.2020.1856442.
[86] W. J. Triplett, "Addressing Human Factors in Cybersecurity Leadership," Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 573–586, Jul. 2022, doi: 10.3390/jcp2030029.
[87] H. El Amin, A. E. Samhat, M. Chamoun, L. Oueidat, and A. Feghali, "An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure," Journal of Cybersecurity and Privacy, vol. 4, no. 2, pp. 357–381, Jun. 2024, doi: 10.3390/jcp4020018.
[88] I. Krawczyk-Sokołowska and W. Caputa, "Awareness of network security and customer value – The company and customer perspective," Technological Forecasting and Social Change, vol. 190, p. 122430, May 2023, doi: 10.1016/j.techfore.2023.122430.
[89] M. N. Y. Marican, S. A. Razak, A. Selamat, and S. H. Othman, "Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review," IEEE Access, vol. 11, pp. 5442–5452, 2023, doi: 10.1109/ACCESS.2022.3229766.
[90] A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," Journal of Economic Surveys, vol. 36, no. 1, pp. 157–187, Feb. 2022, doi: 10.1111/joes.12456.
[91] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," Sensors, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/s23156666.
[92] M. Kianpour, S. J. Kowalski, and H. Øverby, "Systematically Understanding Cybersecurity Economics: A Survey," Sustainability, vol. 13, no. 24, p. 13677, Dec. 2021, doi: 10.3390/su132413677.
[93] X. Mu and M. F. Antwi-Afari, "The applications of Internet of Things (IoT) in industrial management: a science mapping review," International Journal of Production Research, vol. 62, no. 5, pp. 1928–1952, Mar. 2024, doi: 10.1080/00207543.2023.2290229.
[94] N.-A. Perifanis and F. Kitsios, "Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review," Information, vol. 14, no. 2, Feb. 2023, doi: 10.3390/info14020085.
[95] N. S. Sewpersadh, "Disruptive business value models in the digital era," Journal of Innovation and Entrepreneurship, vol. 12, no. 1, p. 2, Jan. 2023, doi: 10.1186/s13731-022-00252-1.



Vicente Merchán-Rodriguez (b. 1970) received his Engineering degree in Systems Engineering from Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador, in 1996, the Master's in Telecommunication Strategic Management from the Universidad San Francisco de Quito (USFQ), Quito, Ecuador, in 2010, and the Ph.D in Informatics Science from the University of La Plata, La Plata, Argentina, in 2017. He joined the Department of Computer Science at ESPE to work as a part-time professor. His current research interests focus

on Cybersecurity, eGovernment, IT Government, Information Systems, Artificial Intelligence, and Telecommunications Process.



Danny Zambrano-Vera (b. 1976) received his Engineering degree in Commercial Engineering from Army Polytechnical School ESPE, Sangolquí, Ecuador, in 2001, the MBA from Army Polytechnical School ESPE, Sangolquí, Ecuador, in 2005, and the Ph.D. in Economics and Business from Santiago of Compostela University, Spain, in 2017. He joined the Department of Economics and Business at ESPE to work as a full-time professor. His current research interests focus on rural, community, and agribusiness economic development, analytics, and business administration.