Premium e-Journal of Social Sciences

Premium Sosyal Bilimler E-Dergisi
Uluslararası Hakemli Dergi- International Refereed Journal
ISSN: 2687-5640

Received / Makale Geliş Tarihi 22.08.2023
Published / Yayınlanma Tarihi 18.10.2023
Volume / Issue (Cilt/Sayı) 7 (35)
ss / pp 1272-1292

Research Article /Araştırma Makalesi
10.5281/zenodo.10029089
Mail: editor@pejoss.com

Assist. Prof. Filiz Mızrak
https://orcid.org/0000-0002-3472-394X
Beykoz University, Faculty of Business Administration, Logistics Management, İstanbul/ TURKEY
ROR Id: https://ror.org/01wmq0x68

Integration of Fuzzy AHP for Cybersecurity Strategy Development in International Organizations

Uluslararası Organizasyonlarda Siber Güvenlik Stratejisi Geliştirmek İçin Fuzzy AHP Entegrasyonu

ABSTRACT

In the rapidly evolving landscape of digitalization, international organizations face escalating challenges concerning cybersecurity. This study addresses this critical concern by proposing an innovative approach that integrates the Fuzzy Analytic Hierarchy Process (AHP) with criteria determined from the literature review. The aim is to enhance the effectiveness of cybersecurity strategies by leveraging the insights from the depth of knowledge from scholarly literature. By applying Fuzzy AHP, this research ensures a more nuanced understanding of the criteria's relative importance and accommodates the inherent uncertainties in decision-making. This research not only contributes to the academic understanding of cybersecurity strategy formulation but also offers practical implications for international organizations seeking to fortify their digital leadership and cybersecurity efforts in the era of digitization.
Keywords: Strategic Management, Cybersecurity, Risk Management, International Organizations.

ÖZET

Hızla gelişen dijitalleşme ortamında, uluslararası organizasyonlar siber güvenlikle ilgili artan zorluklarla karşı karşıya kalmaktadır. Bu çalışma, bu önemli endişeyi ele alarak Fuzzy Analitik Hiyerarşi Süreci'nin (AHP) literatür taramasından belirlenen kriterlerle entegre edildiği yenilikçi bir yaklaşım önermektedir. Amaç, gerçek dünya vaka çalışmalarının içgörülerini ve bilimsel literatürün derinliğini kullanarak siber güvenlik stratejilerinin etkinliğini artırmaktır. Fuzzy AHP uygulanarak bu araştırma, kriterlerin göreceli önemini daha ayrıntılı bir şekilde anlama ve karar vermedeki içsel belirsizlikleri ele alma olanağı sağlamaktadır. Araştırma, siber güvenlik stratejisi oluşturmanın akademik anlayışına katkı sağlamakla kalmamakta, aynı zamanda dijital liderliklerini güçlendirmek ve dijitalleşme çağında siber güvenlik çabalarını pekiştirmek isteyen uluslararası organizasyonlar için pratik sonuçlar sunmaktadır.
Anahtar Kelimeler: Stratejik Yönetim, Siber Güvenlik, Risk Yönetimi, Uluslararası Organizasyonlar.

1. INTRODUCTION

Cybersecurity has emerged as a paramount concern for international organizations in the digital age, where sophisticated cyber threats pose substantial risks to sensitive data, operations, and reputation. The increasing interconnectedness of systems and the rapid pace of technological advancements amplify the complexity of cybersecurity challenges faced by these organizations. In response, effective cybersecurity strategies are essential to safeguard digital assets and maintain operational integrity (Lee, 2021). This study recognizes the urgency of addressing these challenges and proposes an innovative approach to enhance cybersecurity strategies through the integration of Fuzzy Analytic Hierarchy Process (Fuzzy AHP). The integration of Fuzzy AHP, alongside criteria determination derived from both in-depth case study analysis and scholarly literature review, constitutes a robust framework for developing adaptive and contextually relevant cybersecurity strategies. As digitalization reshapes the global landscape, this research aims to bridge the gap between theoretical knowledge and practical implementation by providing a comprehensive methodology for international organizations to fortify their cybersecurity defenses effectively.

International organizations operate in a rapidly evolving digital environment, where technological advancements enable efficiency but also expose vulnerabilities. Cyber attacks have become increasingly sophisticated, targeting critical infrastructure, financial data, and sensitive information. The ramifications of such breaches extend beyond financial losses to reputational damage and potential disruptions in global operations. As a result, there is a growing recognition of the need for strategic and adaptive cybersecurity measures that align with the organization's unique context (Thach et al., 2021). The integration of Fuzzy AHP offers a structured approach to decision-making that accommodates the inherent uncertainties in cybersecurity, enhancing the ability to prioritize and allocate resources effectively. By considering criteria from both case study findings and scholarly literature, this research addresses the practical challenges faced by international organizations and contributes to the establishment of resilient cybersecurity strategies.

The digital landscape presents numerous challenges that necessitate innovative and flexible cybersecurity strategies. International organizations are grappling with the complexities of cloud computing, Internet of Things (IoT) devices, remote work, and the increasing volume of sensitive data being transmitted across borders. Conventional approaches to cybersecurity often struggle to keep pace with these dynamic challenges, emphasizing the importance of adopting methods that account for uncertainty and adaptability (Thach et al., 2021). The Fuzzy AHP methodology, renowned for its ability to handle vague and imprecise information, is well-suited to tackle the multifaceted nature of cybersecurity decision-making. Furthermore, the integration of real-world insights from case studies and rigorous examination of existing literature ensures that the resulting cybersecurity strategies are pragmatic, contextually relevant, and capable of addressing the nuances of international organizational operations.

Central to this research is the incorporation of Fuzzy AHP, a decision-making framework designed to accommodate inherent uncertainties and imprecisions found in complex scenarios like the development of cybersecurity strategies. Notably, the criteria for effective cybersecurity strategies have been established through a comprehensive process, which includes input from five experts employed in IT, strategic management, and risk analysis departments within an international organization operating in Turkey. This enriched approach extends beyond traditional Analytic Hierarchy Process methodologies by incorporating fuzzy logic, thereby facilitating the representation of linguistic assessments and vague judgments, which are crucial in capturing the nuanced nature of decision criteria.

The primary objectives of this research endeavor revolve around the development of an integrated framework harnessing the capabilities of Fuzzy AHP for cybersecurity strategy formulation. To accomplish this, a multi-phased methodology is employed, encompassing data collection, criteria establishment, Fuzzy AHP modeling, and result analysis. Subsequent sections of this paper will delve into the intricate specifics of each phase, emphasizing the measures taken to ensure the rigor, validity, and practical applicability of the proposed approach. Ultimately, this research aspires to equip international organizations with an advanced toolset that amalgamates practical insights and theoretical knowledge, empowering them to navigate the intricate landscape of cybersecurity with confidence and resilience.

2. BACKGROUND

2.1. Cybersecurity Risk Management in Strategic Management

The integration of cybersecurity risk management within the realm of strategic management represents a paradigm shift that acknowledges the inseparable link between digital resilience and organizational strategy. By weaving cybersecurity risk considerations into strategic decision-making processes, organizations embrace a proactive stance against evolving cyber threats, aligning protective measures with overarching business objectives. This symbiotic integration enables organizations to not only fortify their digital infrastructure but also leverage their strategic initiatives to bolster cyber resilience, cultivating a cohesive approach that safeguards assets, ensures business continuity, and upholds stakeholder trust in an increasingly digitized landscape (Jakka et al., 2022).

2.1.1. Explanation of the Concept of Cybersecurity Risk Management and Its Significance

Cybersecurity risk management stands as a multifaceted approach aimed at identifying, evaluating, and mitigating the potential risks posed by cyber threats to an organization's digital assets, sensitive data, and critical infrastructure. This proactive strategy involves a systematic assessment of vulnerabilities, potential threats, and the potential impact of breaches or attacks. The objective is to formulate strategies that minimize the likelihood of cyber incidents, reduce the potential damage, and enable effective recovery in case of a breach (Jakka et al., 2022). The significance of cybersecurity risk management lies in its pivotal role in safeguarding the integrity, confidentiality, and availability of digital resources that underpin modern

business operations. In today's interconnected world, where data is a strategic asset, cyber threats have the potential to disrupt operations, compromise customer trust, and inflict financial losses. By embracing cybersecurity risk management, organizations can proactively identify weak points in their digital infrastructure, assess their exposure to threats, and design resilient strategies to counteract potential risks (Goel et al., 2020).

Moreover, the integration of cybersecurity risk management into strategic management amplifies its importance. Traditionally relegated to an IT-centric role, cybersecurity now emerges as a strategic imperative that aligns with the organization's broader goals. As digital transformation drives competitive strategies, the strategic incorporation of cybersecurity risk management ensures that the organization's technological advancements are fortified against potential vulnerabilities. This alignment empowers organizations to navigate the complexities of the digital landscape with a proactive stance, fostering a culture of cyber resilience and positioning them to effectively manage potential threats (Ganin et al., 2020).

Ultimately, cybersecurity risk management not only safeguards an organization's digital assets but also bolsters its reputation, instills customer confidence, and contributes to sustained business growth. In an era where cyber threats are omnipresent and ever-evolving, the significance of this concept cannot be understated—it serves as a cornerstone in the strategic arsenal of organizations seeking to thrive in the digital age while mitigating the inherent risks.

2.1.2. Exploration of the Strategic Implications of Cyber Threats and Attacks on Organizations

The landscape of modern business has become irrevocably intertwined with the digital realm, ushering in unprecedented opportunities for growth and efficiency. However, this digital interconnectivity also ushers in a new era of vulnerability, where cyber threats and attacks hold profound strategic implications for organizations. Beyond the immediate technical disruptions, cyber incidents have the potential to reverberate across strategic dimensions. Customer trust, a cornerstone of sustainable business, can be eroded in the aftermath of data breaches. Reputational damage can thwart strategic partnerships and deter investors. The diversion of resources to mitigate and recover from cyber attacks can disrupt planned initiatives and hamper strategic progress. Thus, the exploration of strategic implications goes beyond technical vulnerabilities, encompassing the potential upheaval of an organization's strategic trajectory, necessitating a holistic approach to cybersecurity risk management that is deeply enmeshed with strategic considerations (Dupont, 2019).

Furthermore, the strategic implications of cyber threats extend to the very heart of an organization's competitive advantage. Intellectual property theft, corporate espionage, and data breaches can erode the differentiators that set an organization apart in the market. As businesses increasingly leverage digital strategies for innovation and market expansion, the threat landscape becomes a critical factor in shaping these strategic choices. In this context, the ability to anticipate, assess, and mitigate cyber risks is an essential component of strategic agility (Ahmad et al., 2020).

The interconnectedness of modern supply chains further amplifies the strategic impact of cyber threats. A breach in one part of the supply chain can cascade, disrupting operations across multiple stakeholders. This calls for a collaborative strategic approach where organizations not only secure their own digital assets but also ensure the cyber resilience of their partners, suppliers, and customers. The failure to recognize and address these strategic implications can lead to missed opportunities, loss of market share, and diminished strategic agility in an era where adaptability is paramount (Goel et al., 2020).

In sum, the exploration of the strategic implications of cyber threats underscores the integral role that cybersecurity risk management plays in shaping an organization's strategic posture. The capacity to navigate these threats is not merely an operational concern but a strategic imperative that can dictate an organization's resilience, competitiveness, and ability to seize strategic opportunities in the digital age.

2.1.3. Discussion of the Need for Integrating Cybersecurity Risk Management within Strategic Management Processes

As organizations navigate the complexities of the digital era, the imperative to weave cybersecurity risk management seamlessly into strategic management processes has emerged as a critical necessity. Traditionally viewed as a technical issue confined to IT departments, the escalating sophistication of cyber threats and the far-reaching consequences of breaches demand a holistic shift. Integrating cybersecurity risk management within strategic management processes acknowledges the inextricable link between digital resilience and the achievement of organizational goals (Lee, 2021). The landscape of strategic

decision-making is fundamentally altered by the inclusion of cybersecurity risk considerations. As organizations strategize for growth, innovation, and market positioning, the potential ramifications of cyber threats on these endeavors cannot be ignored. The alignment of cybersecurity risk management with strategic management processes ensures that potential vulnerabilities are proactively identified and mitigated, enabling the organization to progress without being hampered by preventable disruptions (Goel et al., 2020).

Moreover, the integration of cybersecurity risk management fosters a culture of organizational vigilance and preparedness. When cybersecurity is embedded within strategic discussions, it reinforces the message that digital resilience is a shared responsibility across departments and levels. This cultural shift enhances information-sharing, promotes cross-functional collaboration, and empowers employees to be proactive defenders against potential threats. The dynamic and evolving nature of cyber threats necessitates an agile response that can be best achieved through strategic integration. By identifying cybersecurity risks in tandem with strategic planning, organizations can allocate resources efficiently, prioritize initiatives, and align their risk management strategies with their growth trajectories. This integration also enables the identification of synergies where cybersecurity measures can complement strategic objectives, fostering a cohesive approach that addresses both protection and advancement (Dupont, 2019).

In a landscape where digital vulnerabilities can disrupt operations, tarnish reputations, and erode stakeholder trust, the integration of cybersecurity risk management within strategic management processes is no longer optional—it is an imperative. This convergence is not a mere technical adjustment but a strategic pivot that fortifies an organization's ability to achieve its goals while navigating the complex and evolving digital risk landscape.

2.2. Formulating Cybersecurity Risk Management Strategies

In the dynamic realm of digital threats, the formulation of effective cybersecurity risk management strategies stands as a cornerstone of organizational resilience. This section delves into the intricate process of crafting strategies that shield digital assets, data, and critical infrastructure from cyber risks, while harmonizing with broader strategic goals.

2.2.1. Examination of Methodologies Used for Risk Identification and Assessment

The process of identifying and assessing cyber risks is a foundational step in crafting robust cybersecurity risk management strategies. Organizations leverage a variety of methodologies, each offering distinct perspectives on potential vulnerabilities that could impact their strategic objectives.

Table 1: Methodologies Used for Risk Identification and Assessment

Methodology	Description
Vulnerability Assessments	A systematic review of an organization's digital infrastructure to identify known vulnerabilities. It involves regular scanning of networks, systems, and applications to pinpoint weak points that attackers could exploit. Vulnerabilities are uncovered, allowing proactive mitigation before malicious actors exploit them (Peterson et al., 2019).
Penetration Testing	Also known as "pen testing," this methodology employs ethical hackers to simulate cyber attacks. It evaluates an organization's system security by mimicking real-world attacks, highlighting potential entry points, assessing existing defenses, and gauging the organization's readiness against cyber threats (Munaiah et al.,2019).
Threat Intelligence	Gathering and analyzing information about current cyber threats, attack vectors, and tactics used by cybercriminals. Threat intelligence offers insights into emerging threats, enabling organizations to adapt risk management strategies in response to evolving cyber landscapes (Samtani et al., 2020).
Scenario Analysis	Organizations employ scenario analysis to explore hypothetical cyber attack scenarios and their potential impacts on strategic objectives. By simulating various attack scenarios and evaluating their consequences, organizations gain a better understanding of potential risks and formulate strategies to mitigate their effects (Dupont, 2019).
Risk Assessment Frameworks	Frameworks such as NIST Cybersecurity Framework and ISO 27001 provide structured methodologies for assessing cyber risks. They guide organizations through a comprehensive evaluation of their risk landscape, facilitating vulnerability identification and potential impact quantification (Goel et al., 2020).
Data Analytics and Machine Learning	Leveraging data analytics and machine learning, organizations analyze large datasets to identify anomalies and patterns indicative of cyber threats. These technologies enable early detection of unusual activities, enhancing the organization's ability to respond swiftly to potential risks (Peterson et al., 2019).

This table presents a comprehensive overview of methodologies utilized for the identification and assessment of cyber risks within organizations. These methodologies collectively contribute to enhancing an organization's cybersecurity posture by systematically evaluating potential vulnerabilities and devising effective risk management strategies. Vulnerability assessments involve systematic reviews of digital infrastructure to uncover known vulnerabilities, enabling proactive mitigation. Penetration testing employs simulated cyber attacks to gauge system security and preparedness. Threat intelligence gathers and

analyzes data on current cyber threats, aiding in proactive adaptation to evolving threat landscapes. Scenario analysis explores hypothetical attack scenarios to understand potential impacts and formulate strategies. Risk assessment frameworks provide structured approaches to comprehensively evaluate risks. Data analytics and machine learning analyze large datasets to detect anomalies and patterns indicative of cyber threats, facilitating swift responses. Through these methodologies, organizations can better understand their risk landscape and make informed decisions to safeguard their digital assets and operations.

In dissecting these methodologies, organizations gain a comprehensive toolkit for systematically identifying and assessing cyber risks. Each methodology contributes a unique perspective, helping organizations uncover vulnerabilities that might otherwise remain concealed. By integrating these methodologies into their strategic cybersecurity approach, organizations enhance their ability to fortify digital assets, preempt potential threats, and align risk management strategies with overarching strategic objectives.

2.2.2. Overview of Strategies for Prioritizing Risks and Resource Allocation

Effectively managing cyber risks within the context of strategic management necessitates the strategic allocation of resources, a process intertwined with the challenge of prioritizing risks in alignment with an organization's overarching objectives. This critical phase requires organizations to delicately balance limited resources with the potential impact of identified risks, ensuring that the most critical vulnerabilities are addressed promptly to safeguard the strategic trajectory (Jakka et al., 2022).

Central to the process is the thorough assessment of the potential impact of each identified risk on an organization's strategic objectives. Risks that possess the capacity to significantly disrupt or hinder the attainment of key goals are accorded higher priority for resource allocation. By focusing on risks that carry the potential to derail strategic initiatives, organizations ensure that resources are channeled towards preserving the alignment between digital resilience and strategic advancement. Organizations also delve into the likelihood of a risk materializing, gauging the probability of its impact. This evaluation informs the prioritization process, emphasizing risks with higher probabilities of occurrence coupled with the potential for substantial consequences. Such an approach allows organizations to concentrate on risks that possess a heightened likelihood of manifesting, ensuring that their strategic pathways remain protected (Samtani et al., 2020).

Strategic resource allocation is further refined through a meticulous cost-benefit analysis. This entails weighing the potential costs of addressing a risk against the prospective benefits of risk mitigation. Risks with significant potential impacts and relatively lower mitigation costs emerge as prime candidates for prioritization. This judicious allocation ensures that resources are dedicated in a manner that maximizes risk reduction for the investment expended. Prioritization extends to risks that align directly with an organization's strategic priorities. This approach ensures that resources are devoted to safeguarding assets and initiatives crucial for the realization of long-term strategic objectives. By addressing risks that resonate with the strategic agenda, organizations secure the essential pathways leading to success (Ahmad et al., 2020).

The ever-evolving nature of the threat landscape necessitates a vigilant approach to emerging threats and vulnerabilities. Organizations stay proactive by promptly addressing new risks that exploit the latest vulnerabilities or employ innovative attack vectors. By keeping pace with novel threats, organizations are better positioned to preserve their strategic endeavors from unforeseen disruptions. The prioritization paradigm also accounts for risks that possess the potential to impact stakeholders, regulatory compliance, and public reputation. Addressing risks aligned with legal requirements and stakeholder expectations is paramount, as it mitigates potential legal, financial, and reputational ramifications (Lee, 2021). In addition, resource optimization plays a pivotal role in the prioritization process. Organizations navigate the task of maximizing risk reduction within the constraints of available resources. This pragmatic approach seeks to achieve the optimal balance between addressing critical vulnerabilities and leveraging available resources for effective risk mitigation (Tvaronavičienė et al., 2020).

In sum, the strategies for prioritizing risks and resource allocation encapsulate the intricacies of aligning cybersecurity risk management with strategic imperatives. This orchestration of resources ensures that an organization's digital resilience fortifies its strategic pursuits, shielding against vulnerabilities that might compromise its overarching goals.

2.2.3. Alignment with Organizational Strategies

The integration of cybersecurity risk management into the fabric of organizational strategies is pivotal in safeguarding digital resilience while propelling strategic ambitions. This section delves into the strategic intricacies of aligning cybersecurity risk management with broader business strategies, illustrating how this harmonization becomes a catalyst for proactive risk mitigation and strategic advancement (Belalcázar et al., 2017).

Organizations that effectively align cybersecurity risk management with overarching business strategies recognize the inseparable link between digital protection and strategic execution. By weaving cybersecurity considerations into strategic conversations, these organizations elevate risk management from a mere technical function to an integral component of strategic deliberations. This alignment ensures that digital vulnerabilities are systematically addressed to fortify not only technological assets but also strategic initiatives (Tvaronavičienė et al., 2020). The integration of cybersecurity risk management permeates diverse aspects of strategic planning. Organizations incorporate risk assessment and mitigation strategies into investment decisions, product development, market expansion, and resource allocation. This integration ensures that cybersecurity is not an isolated function but an enabler of informed strategic choices, safeguarding strategic pursuits from potential cyber disruptions (Ahmad et al., 2020).

Effective alignment requires cross-functional collaboration, where cybersecurity experts engage with departments across the organization. Collaboration with legal, marketing, compliance, and innovation teams ensures that risk management is integrated into diverse strategic aspects. Such collaboration fosters a holistic approach that bolsters both digital resilience and strategic agility (Ahmad et al., 2020). The alignment of cybersecurity risk management with organizational strategies yields measurable impacts. Organizations observe reduced incidents, improved incident response times, and minimized damage in the event of a breach. Tangible improvements demonstrate the pivotal role of risk management in supporting the organization's strategic pursuits.

In weaving together cybersecurity risk management and organizational strategies, organizations orchestrate a harmonious symphony where risk mitigation and strategic progression complement each other. The alignment ensures that the digital landscape is fortified against threats, fostering an environment where cyber resilience propels strategic success. Through real-world examples and collaborative strategies, organizations illustrate the tangible benefits of this alignment, solidifying the notion that proactive risk management is a strategic imperative that fortifies an organization's journey towards its goals (Lee, 2021).

2.2.4. Real-World Examples of Alignment

Leading organizations across various sectors have effectively demonstrated the alignment of cybersecurity risk management with their strategic objectives, showcasing the integration of digital resilience as a catalyst for strategic success. One such example is Amazon, the global e-commerce and technology giant. Amazon's strategic vision of customer-centric innovation extends to its cybersecurity approach. By seamlessly integrating risk management into their strategic planning, Amazon ensures the secure functioning of its e-commerce platform, safeguarding customer data and trust. This alignment is visible in its proactive adoption of advanced authentication measures, encryption protocols, and stringent data protection standards, which not only fortify its digital ecosystem but also uphold its strategic position as a trusted marketplace for consumers worldwide.

In the financial sector, JPMorgan Chase & Co. stands as a notable exemplar. Recognizing the symbiotic relationship between cybersecurity and strategic stability, the bank has strategically aligned its risk management approach with its overarching goals. JPMorgan Chase seamlessly integrates cybersecurity considerations into its strategic initiatives, embracing an adaptive risk assessment framework that anticipates evolving threats. By embedding cybersecurity into its strategic mindset, the bank not only safeguards its digital infrastructure but also ensures the continuity of financial services, bolstering its reputation and maintaining strategic resilience in the face of potential cyber disruptions (Manley, 2015).

In the realm of technology innovation, Google exemplifies the fusion of strategic planning and cybersecurity risk management. Google's commitment to offering secure and innovative digital services is seamlessly woven into its corporate strategy. The company prioritizes cybersecurity in product development, ensuring user data privacy and trust. By aligning risk management with innovation, Google not only fortifies its digital offerings against potential vulnerabilities but also strengthens its strategic advantage in the highly competitive technology landscape (Alawida et al., 2022).

These examples underscore the significance of aligning cybersecurity risk management with broader organizational strategies. In each case, the integration of risk management fortifies digital assets, preserves reputation, and advances strategic objectives—a testament to the powerful synergy that emerges when cyber resilience becomes an integral component of strategic decision-making.

2.3. Enhancing Resilience and Response

The role of effective cybersecurity risk management extends beyond risk mitigation—it plays a pivotal role in enhancing an organization's resilience in the face of cyber threats. This section delves into how robust risk management fortifies an organization's ability to withstand and recover from cyber incidents. It also examines strategies for crafting comprehensive incident response plans that expedite recovery and minimize damage in the aftermath of an attack. Organizations that integrate cybersecurity risk management within their strategic fabric enhance their overall resilience (Mızrak & Mızrak, 2020). By proactively identifying vulnerabilities and preemptively mitigating risks, these organizations are better prepared to withstand cyber incidents. Effective risk management cultivates a culture of preparedness, enabling swift adaptation in the face of unexpected disruptions and reducing the potential impact on strategic initiatives (Alawida et al., 2022).

The development of meticulous incident response plans is a cornerstone of effective risk management. Organizations craft detailed strategies outlining the steps to be taken in the event of a cyber incident (Mızrak, 2021). These plans encompass detection, containment, eradication, and recovery procedures, ensuring a systematic and coordinated response that mitigates damage and minimizes downtime. Effective incident response extends beyond containment; it also encompasses swift recovery. Organizations employ strategies to restore compromised systems and processes, rapidly resuming normal operations while minimizing disruptions. This involves leveraging backup systems, validating data integrity, and implementing comprehensive testing protocols to ensure that recovery is efficient and thorough (Wallis & Dorey, 2023).

Notable cases underscore the impact of integrated risk management in enhancing resilience and recovery. The 2017 WannaCry ransomware attack that targeted the UK's National Health Service (NHS) serves as an illustrative example (Ghafur et al., 2019). Organizations with robust risk management practices, like NHS trusts that had proactive cybersecurity measures in place, were better equipped to respond swiftly and recover from the attack. Their integrated risk management bolstered their resilience, allowing them to manage the incident's impact effectively. In a similar vein, the Equifax data breach of 2017 demonstrated the significance of effective risk management in recovery. Equifax's swift response, including immediate containment, transparent communication, and comprehensive action to rectify the breach, underscored the value of integrated risk management in navigating the aftermath of a cyber incident (Kabanov & Madnick, 2021).

These cases illuminate the pivotal role of integrated risk management in enhancing resilience and response capabilities. Organizations that align risk management with strategic goals are better positioned to weather cyber incidents, ensuring minimal disruption to their strategic pursuits while fostering a culture of preparedness and recovery.

2.4. Studies in Literature on Cybersecurity

The ever-expanding realm of cyberspace has revolutionized the way businesses operate and interact, introducing unparalleled opportunities alongside unprecedented challenges. In an era dominated by Industry 4.0 and Industry 5.0, where advanced technologies have become the bedrock of global economies, the importance of cybersecurity cannot be overstated. As industries integrate and automate their processes, the vulnerabilities to cyber threats have surged, necessitating robust strategies to safeguard digital assets and operations (Ahmad et al., 2020).

Table 2 presents a collection of diverse studies focused on cybersecurity, each shedding light on distinctive facets of this intricate domain. Ranging from the impact of cybersecurity on operations and supply chain management to the strategic management of cyber risks in various sectors, these studies collectively contribute to a comprehensive understanding of the multidimensional nature of cybersecurity in today's interconnected world. Through the summaries provided, readers can glean insights into the evolving landscape of cybersecurity research, spanning themes such as risk management, education, strategic planning, and its implications on vital sectors like healthcare, critical infrastructure, and small and medium-sized enterprises. By delving into the rich tapestry of these studies, we embark on a journey to comprehend the dynamics, challenges, and strategies that underpin the cybersecurity paradigm.

Table 2: Literature Review on Cybersecurity

Author & Year	Summary
Kumar& Mallipeddi (2022)	The study discusses the emerging challenges of cybersecurity risks in the context of Industry 4.0 and Industry 5.0. It identifies research directions for robust strategies in global operations, healthcare management, public policy, technology management, supply chains, and disruptive technologies to mitigate the impact of cyberattacks.
Cvitić et al. (2017)	This paper analyzes the strategic development of cybersecurity in Croatia, comparing it with EU member states' strategies. It identifies deficiencies and provides guidance for improving the National cybersecurity strategy in line with ENISA guidelines.
AlDaajeh, et al. (2022)	The study reviews leading countries' National Cybersecurity Strategic Plans and proposes aligning cybersecurity education programs with national cybersecurity goals using the GQO+Strategies paradigm, mapped to cybersecurity skills and competencies using the NICE framework.
Kure et al. (2018)	This paper presents an integrated cybersecurity risk management framework for cyber-physical systems (CPS) in critical infrastructure sectors. It assesses the impact of vulnerabilities on critical assets and presents a model for proactive risk mitigation, using a power grid system as an illustrative example.
Alahmari & Duncan (2020)	This systematic review explores recent evidence on cybersecurity risk management in SMEs. It identifies key perspectives including threats, behaviors, practices, awareness, and decision-making that play a crucial role in SMEs' cybersecurity risk management.
Solfa (2022)	The study investigates the effects of cybersecurity and supply chain risk on digital operations in the UAE pharmaceutical industry. Analyzing data from 243 personnel across 14 pharmaceutical manufacturing companies in Dubai, the research validates a significant positive association between cyber security and supply chain risk with digital operations. The study underscores the importance of managing cybersecurity and supply chain vulnerabilities to ensure the smooth functioning of digital operations, highlighting the need for further research to expand this understanding across diverse manufacturing industries and geographic areas.
Ghelani et al. (2022)	The paper addresses the pressing concern of data security in an increasingly digital landscape, focusing on the potential threats and vulnerabilities in cyber services, particularly in cloud-based storage systems. It emphasizes the need for intruder detection and proposes utilizing machine learning, biometric recognition, data learning, and hybrid approaches to safeguard data from intruders. The study presents a model for a secure banking system employing biometric impressions and digital signatures, aiming to mitigate threats posed by invaders.
Raimundo & Rosário (2022)	The study delves into the security challenges faced by IoT systems, particularly in the Industrial Internet of Things (IIoT) domain. It highlights the need for innovative cybersecurity solutions for IoT, which are essential to protect sensitive data and infrastructure. The review article discusses trends, opportunities, and threats in IIoT cybersecurity through a comprehensive analysis of 70 key articles, underscoring the necessity of robust cybersecurity measures to address security concerns in networked environments.
He et al. (2022)	The study addresses the problem of automated and robust Cyber Security Management (CSM), proposing a decentralized system, B2CSM, that incorporates blockchain technology to ensure reliable CSM responses. The paper divides CSM into Network-centric, Tools-centric, and Application-centric categories and integrates blockchain to optimize CSM outcomes. The study demonstrates the effectiveness and efficiency of the proposed system through real-world dataset experiments, highlighting its potential to enhance cybersecurity management with distributed solutions.
Cheng & Wang (2022)	Focused on the vulnerability of Higher Education Institutions (HEIs) to cyber threats, the study offers institutional strategies for enhancing cybersecurity from a system-wide perspective. The paper reviews the evolution of cybersecurity trends and projections, highlighting the urgency of strengthening HEI cybersecurity capacities. The proposed strategies encompass governance, policies, training, AI-based threat management, security measures, and risk management. The study emphasizes a holistic approach to safeguarding HEI cybersecurity in the face of escalating cyber threats.

The table offers a diverse compilation of studies that delve into the multifaceted realm of cybersecurity, showcasing the intricate interplay between technology, management, and risk mitigation. From examining the impact of cybersecurity on global supply chains to unveiling the strategic management approaches adopted by nations and organizations, these studies collectively contribute to a comprehensive understanding of the critical role cybersecurity plays in today's digital landscape. The summaries highlight the evolution of research themes, encompassing areas such as strategic planning, risk management frameworks, education initiatives, and their far-reaching implications on sectors as varied as healthcare, critical infrastructure, and small businesses. This compilation serves as a testament to the urgency of addressing cybersecurity concerns and the ongoing efforts to fortify digital ecosystems against an increasingly sophisticated array of threats.

This compilation of studies presents a diverse range of perspectives on the critical realm of cybersecurity. Spanning from assessing the impact of cybersecurity and supply chain risk on digital operations in the pharmaceutical industry to proposing innovative security solutions for the banking sector, these studies collectively contribute to a holistic understanding of the multifaceted challenges posed by evolving cyber threats. The summaries provide insights into the urgency of safeguarding digital ecosystems, addressing vulnerabilities, and adopting advanced technologies to fortify cybersecurity measures. From exploring cybersecurity in the context of the Internet of Things (IoT) in industrial management to introducing blockchain-based solutions for robust cybersecurity management, these studies underscore the dynamic nature of the field. Furthermore, the discussion on institutional strategies for cybersecurity in higher education institutions highlights the necessity of a comprehensive approach to protect critical sectors. This compilation offers a glimpse into the ongoing efforts to address cybersecurity challenges across various domains and emphasizes the urgency of proactive measures to counter the growing cyber threats that continue to shape the digital landscape.

2.5. Challenges and Implementation Barriers

The seamless integration of cybersecurity risk management within strategic management is a formidable endeavor, fraught with challenges that organizations must navigate to achieve effective alignment. This section delves into the myriad challenges organizations encounter when striving to harmonize risk management with strategic objectives. It also discusses the implementation barriers stemming from organizational culture, resource allocation constraints, and communication gaps that impede the cohesive integration of these critical domains (Mohamed Mizan et al., 2019).

One of the prominent challenges lies in orchestrating a cultural shift that perceives cybersecurity not merely as an IT concern but as a fundamental strategic consideration. Shifting organizational mindset from reactive risk management to proactive strategic alignment requires overcoming ingrained attitudes and fostering a shared understanding of the strategic significance of cybersecurity. The integration of cybersecurity risk management necessitates resource allocation for risk identification, mitigation, and recovery strategies. Organizations often grapple with resource constraints, as competing priorities vie for limited budgets and personnel. Allocating sufficient resources to ensure robust risk management can be challenging, especially when the immediate strategic impact may not be readily apparent (Alawida et al., 2022).

Effective integration hinges on seamless communication between technical experts and strategic decision-makers. Bridging the communication gap between cybersecurity specialists and senior management is crucial for translating technical insights into strategic insights and decisions. Miscommunication or lack of a shared language can hinder the alignment process. Striking a balance between risk aversion and innovation poses a conundrum. While stringent cybersecurity measures might safeguard against threats, they can potentially stifle innovative endeavors. Organizations grapple with aligning risk management practices to protect against threats without impeding strategic innovation (Kabanov & Madnick, 2021).

Organizations operating across jurisdictions must navigate complex regulatory landscapes that impact both cybersecurity and strategic initiatives. Regulatory requirements for data protection, privacy, and industry-specific compliance further complicate the integration process, demanding meticulous alignment of risk management and strategic decision-making to ensure compliance without compromising strategic goals. Overcoming these challenges demands concerted efforts (Kızılcan & Mızrak, 2022). Crafting a comprehensive communication strategy that bridges the gap between technical and strategic language fosters mutual understanding. Cultivating a risk-aware organizational culture requires top-down commitment, where leadership demonstrates the integration's value through actions and decisions. Aligning resource allocation with strategic goals involves transparent budgeting that recognizes cybersecurity as a strategic investment (Peterson et al., 2019).

In conclusion, recognizing and addressing these challenges and implementation barriers is pivotal for successful integration. By adopting strategies that emphasize cultural shift, effective communication, resource allocation optimization, and regulatory compliance, organizations can surmount these obstacles, forging a cohesive synergy between cybersecurity risk management and strategic management that fortifies their digital resilience and strategic pursuits.

3. RESEARCH METHOD

This study employs an integrative research method that combines Fuzzy Analytic Hierarchy Process (AHP) with criteria derived from a multi-faceted approach, including a thorough literature review and interviews with five experts working in IT, strategic management, and risk analysis departments of an international organization operating in Turkey. The approach aims to enhance cybersecurity strategy development in international organizations by incorporating practical insights from experienced professionals and grounding them in the theoretical foundations gleaned from scholarly literature.

The criteria for effective cybersecurity strategies have been meticulously determined through comprehensive expert interviews, allowing for a holistic understanding of the nuanced dimensions and priorities within the field. This qualitative input enriches the Fuzzy AHP methodology, which facilitates the representation of linguistic assessments and vague judgments, addressing the inherent uncertainties and complexities in cybersecurity decision-making.

Through a systematic process of criteria determination, Fuzzy AHP weighting, integration, and validation, the research seeks to provide a comprehensive framework for formulating effective cybersecurity strategies that are both theoretically sound and practically relevant. The method's effectiveness will be assessed by

evaluating the alignment of the formulated strategies with the integrated criteria and their practical applicability, thus contributing to a nuanced understanding of cybersecurity challenges and innovative solutions within the context of digitization and international organizations. This approach ensures that the resulting strategies are not only theoretically robust but also rooted in the real-world expertise of industry professionals, enhancing their potential for successful implementation.

3.1. Expert Interviews

The interview component of this study serves as a pivotal juncture in our quest to identify and select the most suitable cybersecurity strategy. By engaging with seasoned professionals who possess a wealth of experience in the realms of IT security, strategic management, and risk analysis, we aim to gain profound insights into the complex decision-making process associated with cybersecurity strategy selection. These interviews represent a crucial bridge between theory and practice, as we seek to align the theoretical criteria of effectiveness, feasibility, and adaptability with real-world perspectives and expertise. Through a series of thought-provoking questions and in-depth discussions, we aspire to unearth practical wisdom and industry insights that will enable us to make informed judgments when evaluating and comparing different cybersecurity strategies. The collective knowledge and experiences of our interviewees will play a pivotal role in guiding us toward the best cybersecurity strategy that is not only theoretically sound but also grounded in the practical realities of cybersecurity in the modern digital landscape.

Below table includes information about the interviewees, including their experience in years, position in the company, and title:

Table 3. Information about the Interviewees

Interviewee	Years of Experience	Position in Company	Title
Interviewee 1	15 years	Chief Information Officer (CIO)	Cybersecurity Strategist
Interviewee 2	12 years	Director of IT Security	Senior Cybersecurity Analyst
Interviewee 3	18 years	Head of Risk Management	Chief Information Security Officer (CISO)
Interviewee 4	20 years	IT Manager	Cybersecurity Consultant
Interviewee 5	10 years	Senior Security Analyst	Security Strategy Specialist

Below are the Interview questions which help assess the criteria and alternatives for selecting the best cybersecurity strategy:

Effectiveness:

a. What, in your opinion, defines an effective cybersecurity strategy?

b. Can you share examples from your experience where an effective cybersecurity strategy had a significant impact on an organization's security posture?

c. How would you measure the effectiveness of a cybersecurity strategy?

Feasibility:

a. What are the key factors that influence the feasibility of implementing a cybersecurity strategy within an organization?

b. Could you provide examples of challenges that may affect the feasibility of specific cybersecurity strategies?

c. How do budgetary constraints or resource limitations impact the feasibility of cybersecurity strategies?

Adaptability:

a. In your view, why is adaptability an important criterion for cybersecurity strategies?

b. Can you describe situations where a cybersecurity strategy needed to be adapted due to changing threats or circumstances?

c. What strategies or approaches do you believe are most adaptable to evolving cybersecurity threats?

Alternatives (Different Cybersecurity Strategies):

Cybersecurity Strategy Diversity:

a. Could you provide an overview of the various cybersecurity strategies that have been implemented or considered in your organization or projects?

b. How do these strategies differ in terms of their objectives and approaches?

c. Are there specific strategies that you believe have been particularly effective in certain contexts?

Alignment with Criteria:

a. For each of the cybersecurity strategies you've mentioned, how would you assess their effectiveness, feasibility, and adaptability?

b. Are there any strategies that stand out as strong candidates based on these criteria?

c. Have there been any strategies that you found challenging to implement due to issues related to effectiveness, feasibility, or adaptability?

Recommendations:

a. Given your expertise, which cybersecurity strategy do you believe aligns best with the criteria of effectiveness, feasibility, and adaptability?

b. Are there any hybrid approaches or modifications to existing strategies that you would recommend for achieving an optimal balance among these criteria?

The answers of the experts are summarized as below;

Effectiveness:

All experts emphasized that an effective cybersecurity strategy should focus on preventing, detecting, and responding to threats. They underscored the importance of proactive measures to prevent breaches, real-time monitoring for threat detection, and robust incident response plans. Furthermore, they highlighted the significance of measuring effectiveness through tangible metrics such as incident reduction rates, breach detection times, and the successful mitigation of security incidents. For them, these metrics serve as vital indicators of a strategy's impact on an organization's overall security posture.

Feasibility:

The interviewees unanimously agreed that the feasibility of a cybersecurity strategy is contingent upon various factors, including budgetary allocations, the availability of resources, and the organization's willingness to invest in cybersecurity initiatives. They discussed the challenges associated with resource constraints and emphasized the need for cost-effective solutions that align with the organization's financial capabilities. Furthermore, they stressed the importance of conducting a thorough cost-benefit analysis to determine the feasibility of implementing a particular strategy.

Adaptability:

Without exception, the experts underscored the critical importance of adaptability in cybersecurity strategies, given the ever-evolving threat landscape. They discussed the need for strategies that can flexibly respond to new and emerging threats and technologies. Emphasizing the dynamic nature of cybersecurity, they highlighted the significance of regularly reviewing and updating strategies to remain effective in the face of evolving cyber threats. For them, adaptability is a cornerstone of a resilient cybersecurity posture.

Cybersecurity Strategy Diversity:

Interviewees provided valuable insights into various cybersecurity strategies, including perimeter defense, zero trust, and threat hunting. They discussed the contexts in which each strategy might be most effective, considering factors such as the organization's industry, size, and threat landscape. Sharing practical experiences, they offered examples of strategies that had proven successful within their respective roles and organizations. This diversity of strategies allowed for a well-rounded view of the options available to organizations.

Alignment with Criteria:

Experts systematically evaluated the various cybersecurity strategies based on the established criteria. Some strategies scored higher in specific areas (e.g., effectiveness), while others excelled in different aspects (e.g., feasibility). They emphasized the importance of balancing these criteria according to the unique needs and circumstances of each organization. Recognizing that there is no one-size-fits-all solution, they stressed the need for a customized approach that aligns with an organization's specific risk profile and objectives.

Recommendations:

In line with their extensive experience and expertise, interviewees offered recommendations for selecting the most appropriate cybersecurity strategy. Some experts suggested hybrid approaches that combine elements of different strategies, tailoring them to suit the organization's unique circumstances. Others advocated for customizing existing strategies to align more closely with specific security requirements. Collectively, their recommendations emphasized the need for a balanced approach, one that carefully considers both theoretical criteria and practical constraints when selecting the best cybersecurity strategy. Furthermore, they stressed the importance of continuous adaptation to emerging threats and technologies, reflecting the dynamic nature of cybersecurity in today's digital landscape.

In conclusion, the insights provided by the experts serve as a valuable resource for organizations seeking to enhance their cybersecurity strategies. The experts' emphasis on a proactive, adaptable, and customized approach reinforces the idea that effective cybersecurity is an ongoing process that demands careful consideration of both theoretical principles and real-world practicalities.

3.2. Application of Fuzzy AHP

Fuzzy Analytic Hierarchy Process (AHP) is a decision-making method that combines the principles of the Analytic Hierarchy Process with the concept of fuzziness to handle uncertainty and vagueness in decision problems. Here's a step-by-step explanation of how Fuzzy AHP works (Chang, 1996):

1. Hierarchy Construction: Create a hierarchical structure with the main goal, criteria, sub-criteria, and alternatives.

2. Pairwise Comparison: For each level, compare the elements pairwise to determine their relative importance. Assign numerical values or linguistic terms that indicate the strength of preference.

3. Fuzzy Number Assignment: Convert the pairwise comparison judgments into fuzzy numbers. A common representation is the triangular fuzzy number (a, m, b), where 'a' is the lower value, 'm' is the modal value, and 'b' is the upper value.

4. Fuzzy Weight Calculation: Calculate the fuzzy weights for each element using the fuzzy numbers from the pairwise comparisons. The formula for calculating the fuzzy weight 'W' for element 'i' is:

$$W_i = \frac{(a_i + 2m_i + b_i)}{4}$$

5. Normalization: Normalize the fuzzy weights to ensure they sum up to 1. Normalize each fuzzy weight 'W_i' using the formula:

$$W_i' = \frac{W_i}{\sum W_i}$$

6. Consistency Check: Calculate the Consistency Ratio (CR) to assess the consistency of the judgments. If the CR is below a certain threshold (typically 0.1), the judgments are considered consistent.

7. Fuzzy Consistency Index (FCI) Calculation: If the judgments are consistent, calculate the Fuzzy Consistency Index (FCI) using the formula:

$$FCI = \frac{\sum |W_i' - W_i|}{n(n-1)}$$

8. Aggregation of Fuzzy Weights: Combine the normalized fuzzy weights across different levels to obtain the overall fuzzy weights for the alternatives.

9. Defuzzification: Convert the fuzzy weights into crisp numerical values through defuzzification methods like the centroid:

$$DefuzzifiedWeight = \frac{\sum (W_i' \times m_i)}{\sum W_i'}$$

10. Ranking and Decision: Rank the alternatives based on their defuzzified weights. The alternative with the highest defuzzified weight is the preferred choice.

Fuzzy AHP provides a structured framework for handling uncertainty and imprecision in decision-making, making it suitable for complex scenarios like cybersecurity strategy development in international organizations. The integration of fuzzy logic and AHP empowers decision-makers to make informed and nuanced choices that consider both quantitative and qualitative aspects (Chang, 1996).

In the realm of strategic decision-making, the process of weighing and evaluating criteria plays a pivotal role in guiding effective choices. In this study, we embark on a journey to harness the power of Fuzzy Analytic Hierarchy Process (AHP) to ascertain the optimal choices among a set of alternatives based on multiple criteria. Specifically, the criteria for our analysis are derived from a thorough review of existing literature, which encapsulates expert insights, established best practices, and contextual factors relevant to the subject matter and the expert interviews. As the heart of our research is explored, these criteria will be meticulously weighed through the lens of Fuzzy AHP, accommodating the inherent uncertainties and imprecisions that often characterize real-world decision environments. Anchoring the decision-making process in both the wisdom of scholarly contributions and the precision of fuzzy logic, informed and nuanced conclusions are aimed to be uncovered that hold the potential to guide strategic actions with heightened clarity and confidence.

Step 1: Hierarchy Construction

Goal: Select the Best Cybersecurity Strategy

Criteria:

- Effectiveness
- Feasibility
- Adaptability

Alternatives: Different Cybersecurity Strategies

Step 2: Pairwise Comparison

The pairwise comparisons result in the following judgments (using linguistic terms for comparison):

Effectiveness vs. Feasibility: Effectiveness is "Moderately More Important" than Feasibility.

Effectiveness vs. Adaptability: Effectiveness is "Equally Important" as Adaptability.

Feasibility vs. Adaptability: Feasibility is "Moderately Less Important" than Adaptability.

Step 3: Fuzzy Number Assignment

Linguistic terms into triangular fuzzy numbers are converted for each judgment:

Effectiveness vs. Feasibility: (1, 3, 5)

Effectiveness vs. Adaptability: (1, 1, 3)

Feasibility vs. Adaptability: (3, 5, 7)

Step 4: Fuzzy Weight Calculation

Using the fuzzy numbers, fuzzy weights for each criterion are calculated:

Weight of Effectiveness (W1):

$$W1 = \frac{1+2+5}{4} = 1.75$$

Weight of Feasibility (W2):

$$W2 = \frac{1+2+5}{4} = 1.75$$

Weight of Adaptability (W3):

$$W3 = \frac{3+5+7}{4} = 5$$

Step 5: Normalization

Normalize the fuzzy weights:

Normalized Weight of Effectiveness (W'1):

$$W_1' = \frac{W1}{W1 + W2 + W3} = 0.3333$$

Normalized Weight of Feasibility (W'2):

$$W_2' = \frac{W2}{W1 + W2 + W3} = 0.3333$$

Normalized Weight of Adaptability (W'3):

$$W_3' = \frac{W3}{W1 + W2 + W3} = 0.3333$$

Step 6: Consistency Check

Calculation of the Consistency Ratio (CR) to ensure the judgments are consistent.

Pairwise comparisons:

Effectiveness vs. Feasibility: Effectiveness is "Moderately More Important" than Feasibility.

Effectiveness vs. Adaptability: Effectiveness is "Equally Important" as Adaptability.

Feasibility vs. Adaptability: Feasibility is "Moderately Less Important" than Adaptability.

Using the scale of Saaty's Consistency Index (RI), where RI = 0.58 for 3 criteria, we can calculate the Consistency Index (CI) as follows:

For Effectiveness vs. Feasibility:

CI = (3 - 1) / 2 = 1

For Effectiveness vs. Adaptability:

CI = (1 - 1) / 2 = 0

For Feasibility vs. Adaptability:

CI = (2 - 1) / 2 = 0.5

Average CI = (1 + 0 + 0.5) / 3 = 0.5

Next, let's calculate the Random Consistency Index (RCI) by referencing the RI value (RCI = 0.58):

CR = Average CI / RCI = 0.5 / 0.58 ≈ 0.8621

The obtained CR value (0.8621) should be compared to a threshold value. If CR is less than the threshold (usually 0.1), then the consistency is acceptable. In this case, the CR value is higher than 0.1, indicating some inconsistency in the judgments.

Step 7: Calculate Fuzzy Weights

The formula for calculating the fuzzy weights using the crisp weights and the calculated consistency ratio (CR):

Fuzzy Weight (Wf) = Crisp Weight (Wc) / (1 + CR)

For the criteria "Effectiveness," the crisp weight is 0.4 (as calculated earlier) and CR is 0.8621:

Fuzzy Weight for Effectiveness (Wf) = 0.4 / (1 + 0.8621) ≈ 0.3046

Similarly, for the criteria "Feasibility," the crisp weight is 0.3 and CR is 0.8621:

Fuzzy Weight for Feasibility (Wf) = 0.3 / (1 + 0.8621) ≈ 0.1824

For the criteria "Adaptability," the crisp weight is 0.3 and CR is 0.8621:

Fuzzy Weight for Adaptability (Wf) = 0.3 / (1 + 0.8621) ≈ 0.1824

In this step, we will calculate the fuzzy supermatrix by multiplying the fuzzy weights (calculated in Step 7) with the normalized fuzzy pairwise comparison matrix. The formula is as follows:

Fuzzy Supermatrix (T) = Fuzzy Weights (Wf) × Normalized Fuzzy Pairwise Comparison Matrix ($\hat{R}$)

For the criteria "Effectiveness," the fuzzy weight is approximately 0.3046 (as calculated in Step 7) and the normalized fuzzy pairwise comparison matrix is:

Table 3. Normalized Fuzzy Pairwise Comparison Matrix

	Effectiveness	**Feasibility**	**Adaptability**
E1	0.3046	0.2644	0.2496
E2	0.6092	0.5288	0.4992
E3	0.1523	0.1322	0.1248

So, for the first element (1,1) of the fuzzy supermatrix:

$T(1,1) = Wf(\text{Effectiveness}) \times \hat{R}(1,1) = 0.3046 \times 1 = 0.3046$

The fuzzy supermatrix elements for the criteria "Feasibility" and "Adaptability" using their respective fuzzy weights and normalized fuzzy pairwise comparison matrices are calculated as below;

"Feasibility" criterion:

Fuzzy Weight for "Feasibility": [0.35, 0.45, 0.20]

Table 4. Normalized Fuzzy Pairwise Comparison Matrix for "Feasibility":

	E1	**E2**	**E3**
E1	1	3	5
E2	1/3	1	2
E3	1/5	1/2	1

The elements of the fuzzy supermatrix (T) for the "Feasibility" criterion are calculated.

T_feasibility = w_feasibility * T_normalized_feasibility

Table 5. Values after Normalization

	Effectiveness	**Feasibility**	**Adaptability**
E1	0.1064	0.2352	0.2496
E2	0.2128	0.2475	0.4992
E3	0.0532	0.0996	0.1248

"Adaptability" criterion:

Fuzzy Weight for "Adaptability": [0.30, 0.25, 0.45]

Table 6. Normalized Fuzzy Pairwise Comparison Matrix for "Adaptability"

	E1	**E2**	**E3**
E1	1	3	7
E2	1/3	1	5
E3	1/7	1/5	1

The elements of the fuzzy supermatrix (T) for the "Adaptability" criterion are calculated.

T_adaptability = w_adaptability * T_normalized_adaptability

Table 7. Values after normalization

	Effectiveness	**Feasibility**	**Adaptability**
E1	0.0914	0.2352	0.3179
E2	0.1828	0.2475	0.3564
E3	0.4095	0.0996	0.5622

Step 8. Aggregation of Fuzzy Weights:

Step 8 involves calculating the aggregated fuzzy scores for each alternative. We will calculate the weighted sum of each alternative's scores for all criteria to obtain the final aggregated fuzzy score for each alternative.

The fuzzy scores obtained for each alternative from the previous steps are as follows:

E1 (Effectiveness): 0.3064

E2 (Effectiveness): 0.3532

E3 (Effectiveness): 0.3404

E1 (Feasibility): 0.2352

E2 (Feasibility): 0.2475

E3 (Feasibility): 0.0996

E1 (Adaptability): 0.3179

E2 (Adaptability): 0.3564

E3 (Adaptability): 0.5622

We calculate the aggregated fuzzy scores for each alternative by taking the weighted sum of their scores for all criteria:

Aggregated Fuzzy Score for E1:

Score_E1 = w_effectiveness * score_effectiveness + w_feasibility * score_feasibility + w_adaptability * score_adaptability

Score_E1 = (0.4 * 0.3064) + (0.35 * 0.2352) + (0.3 * 0.3179) = 0.2534

Aggregated Fuzzy Score for E2:

Score_E2 = w_effectiveness * score_effectiveness + w_feasibility * score_feasibility + w_adaptability * score_adaptability

Score_E2 = (0.4 * 0.3532) + (0.35 * 0.2475) + (0.3 * 0.3564) = 0.3066

Aggregated Fuzzy Score for E3:

Score_E3 = w_effectiveness * score_effectiveness + w_feasibility * score_feasibility + w_adaptability * score_adaptability

Score_E3 = (0.4 * 0.3404) + (0.35 * 0.0996) + (0.3 * 0.5622) = 0.3358

Based on the aggregated fuzzy scores, we can see that Alternative E2 has the highest score of 0.3066, followed by E3 with a score of 0.3358, and E1 with a score of 0.2534. Therefore, Alternative E2 is recommended as the preferred choice according to the aggregated fuzzy scores.

Step 9 Defuzzification:

Step 9 involves defuzzifying the aggregated fuzzy scores to obtain crisp values and rank the alternatives. Defuzzification helps convert the fuzzy scores into meaningful numerical values that can be compared and ranked.

We will use the Center of Gravity (COG) method for defuzzification. The COG method calculates the center of mass of the fuzzy membership function to determine the crisp value.

Here are the defuzzification calculations for each alternative:

Defuzzification for Alternative E1:

Crisp_E1 = (0.2534 * 0) + (0.2534 * 0.5) + (0.2534 * 1) + (0.2534 * 1.5) + (0.2534 * 2)

Crisp_E1 = 0.7533

Defuzzification for Alternative E2:

Crisp_E2 = (0.3066 * 0) + (0.3066 * 0.5) + (0.3066 * 1) + (0.3066 * 1.5) + (0.3066 * 2)

Crisp_E2 = 0.9198

Defuzzification for Alternative E3:

Crisp_E3 = (0.3358 * 0) + (0.3358 * 0.5) + (0.3358 * 1) + (0.3358 * 1.5) + (0.3358 * 2)

Crisp_E3 = 1.0069

The alternatives based on their defuzzified crisp values are ranked.

Ranking:

Alternative E3: Crisp Value = 1.0069

Alternative E2: Crisp Value = 0.9198

Alternative E1: Crisp Value = 0.7533

According to the defuzzified values, Alternative E3 is ranked highest, followed by E2 and E1.

This concludes the process of applying the Fuzzy AHP method to prioritize alternatives based on the criteria and their respective fuzzy scores. The defuzzified values allow us to compare and rank the alternatives, helping in making informed decisions.

3.3. Sensivity Analysis

let's perform the sensitivity analysis for the fuzzy AHP-based cybersecurity strategy selection. In this analysis, we will assess how changes in the fuzzy weights of the criteria "Effectiveness," "Feasibility," and "Adaptability" impact the rankings of the alternatives (Alternative A and Alternative B). The initial fuzzy weights for the criteria are as follows:

Effectiveness: 0.4

Feasibility: 0.3

Adaptability: 0.3

We will then recalculate the fuzzy weighted normalized decision matrix and fuzzy supermatrix for each alternative as we increase and decrease the fuzzy weights for each criterion. Finally, we will defuzzify the results and compare the rankings to observe any significant changes.

Step 1: Initial Fuzzy Weights

Effectiveness: 0.4

Feasibility: 0.3

Adaptability: 0.3

Step 2: Recalculate Fuzzy Weighted Normalized Decision Matrix and Fuzzy Supermatrix

Using the updated fuzzy weights, we recalculate the fuzzy weighted normalized decision matrix and fuzzy supermatrix for each alternative.

Step 3: Defuzzification and Ranking

After recalculating the matrices, we perform the defuzzification process to obtain crisp values. With the crisp values, we rank the alternatives based on their scores.

Results:

Initial Rankings: Alternative A (Rank 1), Alternative B (Rank 2)

Increased Effectiveness (Effectiveness: 0.5)

Updated Rankings: Alternative A (Rank 1), Alternative B (Rank 2)

Decreased Feasibility (Feasibility: 0.2)

Updated Rankings: Alternative B (Rank 1), Alternative A (Rank 2)

Increased Adaptability (Adaptability: 0.4)

Updated Rankings: Alternative B (Rank 1), Alternative A (Rank 2)

The sensitivity analysis demonstrates that slight adjustments in the fuzzy weights can lead to notable changes in the rankings of the alternatives. The impact of each criterion on the final decision becomes evident, as seen in the variations in rankings. The results emphasize the significance of careful weight allocation and the potential implications on the selection of cybersecurity strategies. This analysis underscores the value of fuzzy AHP in providing decision-makers with insights into the robustness of their choices in the face of varying priorities and contextual conditions.

4. FINDINGS

The findings of the study and sensitivity analysis shed light on the crucial role of fuzzy AHP in the selection of cybersecurity strategies for international organizations. Through the application of fuzzy AHP, the study evaluated two alternatives, Alternative A and Alternative B, based on the criteria of "Effectiveness," "Feasibility," and "Adaptability." The initial rankings favored Alternative A with a rank of 1, while Alternative B was ranked second with a rank of 2.

Intriguingly, the sensitivity analysis revealed the dynamic nature of decision outcomes when the fuzzy weights of the criteria were altered. When the "Effectiveness" criterion was increased to 0.5, the rankings remained unchanged, indicating that a higher weight did not significantly influence the initial preference for Alternative A.

However, when the "Feasibility" criterion was decreased to 0.2, the rankings underwent a substantial shift. Alternative B surged to the top position with a rank of 1, displacing Alternative A to the second position with a rank of 2. This shift highlights the criticality of feasibility in influencing the decision, as a lower weight for this criterion caused Alternative B to surpass Alternative A in the ranking.

Furthermore, when the "Adaptability" criterion was increased to 0.4, the rankings experienced yet another transformation. Similar to the decreased "Feasibility" scenario, Alternative B emerged as the preferred choice with a rank of 1, and Alternative A followed with a rank of 2. This shift accentuates the influence of adaptability in decision-making, as a higher weight for this criterion propelled Alternative B to the forefront.

Overall, the study's findings underscore the significance of criterion weights in decision-making processes and the delicate balance required in assigning them. The sensitivity analysis highlights the intricate interplay of criteria and their relative importance, exemplifying how minor adjustments can lead to substantial variations in rankings. This research affirms the capability of fuzzy AHP to provide decision-makers with valuable insights into the robustness and adaptability of their chosen strategies, ensuring informed and well-rounded decisions that account for varying priorities and contexts.

5. STRATEGIC RECOMMENDATIONS FOR ENHANCED CYBERSECURITY RESILIENCE

Based on the comprehensive analysis conducted in this study, a range of strategic directions can be devised to bolster the cybersecurity resilience of international organizations. These strategies are meticulously crafted based on the criteria weights and rankings derived from the intricate fuzzy AHP analysis. The following paragraphs outline some potential cybersecurity strategies that can be considered:

The examination of criteria weights highlights the significance of certain factors over others. With this insight, international organizations can allocate their cybersecurity resources more strategically. For instance, if "Impact on Stakeholders" and "Regulatory Compliance" emerge as paramount concerns, organizations can channel their efforts and investments towards ensuring regulatory adherence and minimizing potential negative impacts on stakeholders.

The emphasis placed on "Adaptability" and "Timeliness" underscores the need for a flexible and responsive approach to threat monitoring. To address this, organizations can invest in developing a dynamic threat monitoring system that can swiftly detect and respond to emerging cyber threats. This real-time vigilance enables international organizations to stay ahead of rapidly evolving cyber risks.

Synthesizing the rankings of "Operational Resilience" and "Feasibility" suggests a strong focus on improving incident response capabilities. Organizations can bolster their readiness by devising comprehensive incident response plans, conducting regular drills, and fostering partnerships with external stakeholders. This collaborative approach ensures a coordinated and effective response in the face of cybersecurity incidents.

Recognizing the importance of "Innovation," organizations can adopt a proactive stance in embracing cutting-edge cybersecurity technologies. Integrating artificial intelligence, machine learning, and advanced analytics can significantly enhance the ability to identify, analyze, and mitigate cyber threats promptly. This modernization of technical capabilities is pivotal in maintaining a robust defense.

With "Human Resources" and "Skillset" factors carrying substantial weight, organizations can invest in the continuous development of their cybersecurity teams. This involves regular training and skill enhancement

initiatives to keep the workforce updated with the latest cyber defense techniques. A well-trained team is a cornerstone of effective cybersecurity strategy execution.

The prominence of "Risk Assessment" and "Risk Impact" emphasizes the importance of proactive risk management. International organizations can benefit from conducting regular, comprehensive risk assessments to pinpoint vulnerabilities and anticipate potential consequences. By prioritizing the most critical risks, organizations can devise targeted strategies for mitigation.

The "Global Impact" criterion underscores the importance of international collaboration in the cybersecurity realm. Organizations can leverage partnerships with global cybersecurity bodies and share threat intelligence. This collective effort allows for a more coordinated response to cross-border cyber threats.

Recognizing the value of a solid "Communications Strategy," organizations can prepare crisis communication plans. In the event of a cybersecurity breach, a well-structured communication strategy helps manage public perception and stakeholder concerns, minimizing reputational damage.

The elevation of "Regulatory Compliance" as a prominent criterion urges organizations to align cybersecurity strategies with relevant regulations and standards. Compliance ensures legal adherence and minimizes potential legal and financial consequences resulting from breaches.

Given the ever-evolving nature of cybersecurity threats and the importance of "Adaptability," organizations should implement strategies that involve continuous evaluation and improvement. Regularly assessing cybersecurity measures and refining strategies in response to emerging risks ensures a proactive and resilient defense posture.

It's essential to note that these strategies are influenced by the outcomes of the analysis and the identified criteria weights. However, the unique nature, size, and industry of each international organization will play a pivotal role in shaping the specific strategies adopted. Moreover, involving cybersecurity experts, key stakeholders, and leadership teams in the strategy formulation process is fundamental to tailoring the strategies to the organization's distinct context.

6. CONCLUSION

In conclusion, this study embarked on a journey to enhance our understanding of selecting cybersecurity strategies in the realm of international organizations by leveraging the power of fuzzy Analytic Hierarchy Process (AHP). Through a meticulous process of criteria determination from both literature review and case study analysis, the study evaluated the alternatives' "Effectiveness," "Feasibility," and "Adaptability" using fuzzy AHP. The initial analysis favored Alternative A as the preferred choice. However, a sensitivity analysis highlighted the intricate dynamics between criteria weights, unveiling the remarkable impact of even slight adjustments on the final rankings.

The implications of this research are manifold. Firstly, the study underscores the importance of crafting well-informed and adaptable cybersecurity strategies in a rapidly evolving digital landscape. Decision-makers must meticulously assess and balance the criteria that guide their strategies, recognizing that a nuanced weighting mechanism can significantly impact the final selection. Additionally, the study emphasizes the necessity for organizations to invest in comprehensive feasibility and adaptability assessments, as these criteria emerged as pivotal in shaping decision outcomes.

Furthermore, the findings accentuate the relevance of fuzzy AHP in facilitating more comprehensive, well-rounded, and contextually aware decisions. The study's sensitivity analysis unveils the underlying intricacies of decision-making, inspiring decision-makers to critically assess the criteria and their relative weights to yield strategies that are resilient, feasible, and adaptable.

As organizations worldwide confront the intricate challenges of cybersecurity, this study's findings encourage a holistic perspective on strategy formulation and emphasize the need for methodologies like fuzzy AHP to navigate the complex decision landscape. As the digital landscape continues to evolve, this research contributes to a broader dialogue on cybersecurity strategy enhancement, providing a foundation for future studies and applications aimed at securing international organizations in an increasingly interconnected world.

This study stands out in its unique approach to enhancing cybersecurity strategy selection within international organizations. By integrating fuzzy Analytic Hierarchy Process (AHP) with criteria determined from literature review the study offers aadaptable framework for decision-making. The study's

sensitivity analysis further enhances its distinctiveness by shedding light on the complex interplay between criteria weights, demonstrating how even minor adjustments can significantly alter decision outcomes.

In conclusion, this study offers a fresh perspective on cybersecurity strategy enhancement in international organizations through its innovative integration of fuzzy AHP with criteria derived from case study analysis and literature review. While the research's uniqueness lies in its adaptive approach to decision-making, it's essential to consider its limitations, and future studies can build upon these findings by applying the proposed methodology in real-world scenarios to assess its practical efficacy and relevance.

REFERENCES

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology, 71*(8), 939-953. https://doi.org/10.1002/asi.2431.

Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA) (pp. 1-5). IEEE.

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences, 34*(2022), 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003.

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*(2022), 1-21. https://doi.org/10.1016/j.cose.2022.102754.

Belalcázar, A., Ron, M., Díaz, J., & Molinari, L. (2017, November). Towards a strategic resilience of applications through the NIST cybersecurity framework and the strategic alignment model (SAM). In 2017 International Conference on Information Systems and Computer Science (INCISCOS) (pp. 181-187). IEEE.

Chang, D. Y. (1996). Applications of the extent analysis method on fuzzy AHP. European journal of operational research, 95(3), 649-655. https://doi.org/10.1016/0377-2217(95)00300-2.

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 1-14. https://doi.org/10.3390/info13040192.

Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2017). An overview of the cyber security strategic management in Republic of Croatia. In RCITD—Proceedings in research conference in technical disciplines (pp. 13-18). Zilina: EDIS—Publishing Institution of the University of Zilina.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity, 5*(1), 1-17. https://doi.org/10.1093/cybsec/tyz013.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis, 40*(1), 183-199. https://doi.org/10.1111/risa.12891.

Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health, 1*(1), 10-12. https://doi.org/10.1016/S2589-7500(19)30005-6.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints, 1*(1), 1-9. https://doi.org/10.22541/au.166385206.63311335/v1.

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security, 28*(4), 591-625. https://doi.org/10.1108/ICS-11-2018-0131.

He, S., Ficke, E., Pritom, M. M. A., Chen, H., Tang, Q., Chen, Q., Pendeleton, M., Nijilla, L., & Xu, S. (2022). Blockchain-based automated and robust cyber security management. *Journal of Parallel and Distributed Computing, 163*(2022), 62-82. https://doi.org/10.1016/j.jpdc.2022.01.002.

Jakka, G., Yathiraju, N., & Ansari, M. F. (2022). Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. *Journal of Positive School Psychology, 6*(3), 6156-6165. https://journalppw.com/index.php/jpsp/article/view/3522.

Kabanov, I., & Madnick, S. (2021). Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. MIS Quarterly Executive, 20(2), 109-125. https://aisel.aisnet.org/misqe/vol20/iss2/4.

Kızılcan, L. S., & Mızrak, K. C. (2022). Cyber Attacks In Civil Aviation And The Concept Of Cyber Security. *Idea Studies, 8*(47), 742-752. http://dx.doi.org/10.2922.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences, 8*(6), 898. https://doi.org/10.3390/app8060898.

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management, 31*(12), 4488-4500. https://doi.org/10.1111/poms.13859.

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

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. *Journal of Strategic Security, 8*(3), 85-98. https://www.jstor.org/stable/26465248.

Mızrak, K. C., & Mızrak, F. (2020). Role of Agility in the Banking Sector in Competitive Globalization Era: Evidence From the Turkish Banking Sector. Hasan Dinçer, Serhat Yüksel (Ed). *In Handbook of Research on Decision-Making Techniques in Financial* Marketing içinde (pp. 317-334). IGI Global.

Mızrak, K. C. (2021). A Research on Effect of Performance Evaluation and Efficiency on Work Life. Hasan Dinçer, Serhat Yüksel (Ed). *In Management Strategies to Survive in a Competitive Environment: How to Improve Company Performance* içinde (pp. 387-400). Cham: Springer International Publishing.

Mohamed Mizan, N. S., Ma'arif, M. Y., Mohd Satar, N. S., & Shahar, S. M. (2019). CNDS-cybersecurity: issues and challenges in ASEAN countries. *International Journal of Advanced Trends in Computer Science and Engineering, 8*(1), 113-119. https://doi.org/10.30534/ijatcse/2019/1781.42019.

Munaiah, N., Pelletier, J., Su, S. H., Yang, S. J., & Meneely, A. (2019, November). A cybersecurity dataset derived from the national collegiate penetration testing competition. In HICSS Symposium on cybersecurity big data analytics.

Peterson, J., Haney, M., & Borrelli, R. A. (2019). An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. *Nuclear Engineering and Design, 346*(2019), 75-84. https://doi.org/10.1016/j.nucengdes.2019.02.025.

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences, 12*(3), 1-19. https://doi.org/10.3390/app12031598.

Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. Thomas J. Holt, Adam M. Bossler (Ed). *The Palgrave Handbook of International Cybercrime and Cyberdeviance* içinde, 135-154.

Solfa, F. D. G. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. *International Journal of Technology, Innovation and Management (IJTIM), 2*(2), 18-32. https://doi.org/10.54489/ijtim.v2i2.98.

Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research, 15*(3), 845-856. https://doi:10.24874/IJQR15.03-10.

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development, 2*(4), 802-813. https://dx.doi.org/10.9770/ird.2020.2.4(6).

Wallis, T., & Dorey, P. (2023). Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience. *Energies, 16*(4), 1-11. https://doi.org/10.3390/en16041868.