Adv. J. Manag. Humanit. Soc. Sci. (2025), Volume 1, Issue 11, 683-691

Advanced Journal of Management, Humanity and Social Science

Journal homepage: https://www.ajmhss.com/

DOI: https://doi.org/10.5281/zenodo.17923826

The Impact of Artificial Intelligence-Based Decision Support Systems on Organizational Cybersecurity and Risk Management

Omid Salehi Farsani

Ordinary Member of the Iranian Society of Computer Architecture, Iran

Article info

Received: 02.10.2025

Accepted: 12.11.2025

Available Online: 13.11.2025

Checked for Plagiarism: Yes

Keywords:

Artificial Intelligence, Decision Support Systems, Cybersecurity, Risk Management, Organizational Resilience

ABSTRACT

Introduction/Background: In the current digital era, organizations face increasingly sophisticated cyber threats that challenge conventional security mechanisms. The growing complexity and volume of cyber incidents demand innovative solutions capable of supporting rapid, accurate, and proactive decision-making.

Purpose/Objective: This study investigates the impact of Artificial Intelligence (AI)-based Decision Support Systems (DSS) on organizational cybersecurity and risk management. Specifically, it aims to examine how AI-driven DSS enhances threat detection, improves incident response, strengthens risk management, and contributes to organizational resilience. Additionally, the study explores challenges, limitations, and governance requirements associated with integrating AI-based DSS into organizational practices.

Methodology: A comprehensive literature review and conceptual analysis were conducted, drawing insights from recent empirical studies, frameworks, and case studies on AI applications in cybersecurity and risk management. The study identifies key constructs, including AI-DSS capabilities, cybersecurity effectiveness, risk management efficiency, governance mechanisms, and organizational readiness, and proposes a conceptual framework linking these constructs.

Results: Findings indicate that AI-based DSS significantly improves cybersecurity performance, enabling faster detection of threats, proactive mitigation, and reduced operational and strategic risk exposure. Furthermore, AI integration supports more informed and timely decision-making, enhancing overall organizational resilience. However, the effectiveness of AI-based DSS is influenced by data quality, human oversight, governance frameworks, and organizational readiness. Potential risks include adversarial attacks, model biases, and over-reliance on automated decision-making.

Conclusion: AI-based Decision Support Systems represent a strategic tool for strengthening cybersecurity and risk management in modern organizations. Successful implementation requires a holistic approach encompassing governance, human-in-the-loop oversight, infrastructure readiness, and continuous evaluation. By integrating AI responsibly, organizations can achieve enhanced security, better risk mitigation, and improved operational resilience.

Introduction

In the contemporary digital landscape, organizations are facing a growing and increasingly complex spectrum of cyber threats. The proliferation of connected devices, cloud computing, and digital services has expanded the attack surface, making traditional cybersecurity methods insufficient [1]. Organizations no longer operate in isolated environments; rather [2], they exist within highly interconnected ecosystems where a single breach

Corresponding Author: **Omid Salehi Farsani (omidsalehi2087@gmail.com)*

can lead to cascading operational, financial, and reputational consequences. As such, the need for advanced, intelligent systems capable of supporting proactive and effective cybersecurity and risk management has become critical [3].

Artificial Intelligence (AI) has emerged as a transformative tool in this context. Leveraging machine learning, deep learning, natural language processing, and predictive analytics, AI systems can analyze vast quantities of data, detect anomalies, identify potential threats, and provide actionable insights in real time. Unlike traditional rule-based approaches [4], AI has the ability to adapt and learn from evolving attack patterns, enhancing an organization's capacity to respond to dynamic and sophisticated threats. The integration of AI into Decision Support Systems (DSS) represents a significant advancement, enabling organizations to make timely, informed, and data-driven decisions that improve both operational efficiency and security posture [5].

The importance of AI-based DSS extends beyond technical cybersecurity measures. Effective risk management requires a holistic understanding of organizational vulnerabilities, potential threat scenarios, and the interplay between operational, strategic, and reputational risks. By incorporating AI-driven analytics into decision-making processes, organizations can anticipate emerging threats, allocate resources efficiently, and implement mitigation strategies that are both proactive and strategic. Moreover, AI-based DSS can facilitate scenario planning, stress testing, and predictive modeling, thereby enhancing organizational resilience in the face of uncertainty.

Despite these potential benefits, the adoption of AI-based DSS is not without challenges. Issues such as data quality, model bias, explain ability, and the risk of adversarial attacks pose significant obstacles. Furthermore, organizational readiness, governance mechanisms, and regulatory compliance play critical roles in determining whether AI systems yield tangible improvements or inadvertently introduce new vulnerabilities. Human oversight remains essential, as over-reliance on automated systems may result in blind spots or misinterpretations of complex threat landscapes. Ethical considerations, privacy concerns, and alignment with corporate risk appetite further complicate implementation.

Several studies highlight the dual nature of AI in cybersecurity. On one hand, AI-enhanced DSS can detect sophisticated threats more accurately than conventional systems, automate routine security processes, and enable rapid response to incidents. On the other hand, AI models can be exploited by malicious actors through adversarial techniques, data poisoning, or manipulation, emphasizing the need for robust governance frameworks and continuous monitoring. Consequently, the effectiveness of AI-based DSS is highly contingent upon organizational maturity, technical infrastructure, and a culture of security awareness.

The objective of this study is to analyze the impact of AI-based DSS on organizational cybersecurity and risk management comprehensively. It seeks to identify the mechanisms through which AI enhances threat detection and mitigation, assess the influence of governance and human oversight, and explore the potential risks and limitations associated with AI adoption. By developing a conceptual framework, the study provides insights into how organizations can strategically integrate AI-based DSS to strengthen their cybersecurity posture, optimize risk management processes, and build operational resilience. This analytical approach contributes to both academic knowledge and practical guidance for managers, cybersecurity professionals, and policymakers seeking to navigate the evolving intersection of AI, decision-making, and organizational risk.

In conclusion, the introduction of AI-based DSS represents a paradigm shift in how organizations perceive, manage, and mitigate cyber and operational risks. By combining advanced computational capabilities with structured decision-making frameworks, AI provides a powerful tool for enhancing security, predicting threats, and fostering organizational resilience. However, the full realization of these benefits requires careful attention to data integrity, human oversight, governance, and ethical considerations. This study lays the groundwork for a deeper understanding of the opportunities, challenges, and strategic implications of AI-based DSS in the contemporary organizational landscape [6].

Literature Review

The adoption of Artificial Intelligence (AI)-based Decision Support Systems (DSS) in organizational cybersecurity and risk management has received increasing scholarly attention in recent years. Several studies highlight AI's potential to enhance threat detection, automate incident response, and improve overall risk assessment and mitigation processes. AI technologies such as machine learning (ML), deep learning (DL), and natural language processing (NLP) allow organizations to process large volumes of structured and unstructured data, identify anomalies, and predict potential threats with greater speed and accuracy compared to traditional methods [7].

Research indicates that AI-driven DSS not only improves operational cybersecurity but also supports strategic decision-making. By integrating AI analytics with structured DSS frameworks, organizations can simulate threat scenarios, prioritize risks, and allocate resources more effectively. For instance, studies have shown that predictive models can anticipate potential security breaches, while anomaly detection algorithms

identify unusual patterns in network traffic, user behavior, or system logs. This capability enhances proactive defense and reduces both operational and strategic risk exposure [8].

However, the literature also emphasizes significant challenges and limitations associated with AI-based DSS. Data quality and availability are critical factors that influence system effectiveness; poor or biased data can lead to inaccurate predictions and misinformed decisions. Explain ability and transparency are recurring concerns, as complex AI models may operate as "black boxes," reducing trust among managers and decision-makers. Additionally, AI systems are vulnerable to adversarial attacks and model manipulation, raising new security and ethical concerns. The successful integration of AI into organizational risk management therefore depends on a combination of technological readiness, governance mechanisms, and human oversight.

Several conceptual and empirical studies have developed frameworks for integrating AI into risk management. These frameworks typically focus on aligning AI capabilities with organizational objectives, establishing human-in-the-loop oversight, and ensuring compliance with legal and ethical standards. By synthesizing these studies, it becomes evident that AI-based DSS can significantly enhance organizational resilience if implemented within a holistic governance and risk management structure [9].

In summary, the literature underscores the dual nature of AI-based DSS in cybersecurity: while offering unprecedented capabilities for threat detection and risk mitigation, it also introduces new vulnerabilities that must be carefully managed. This body of research provides a strong foundation for analyzing how AI-driven decision support systems influence organizational cybersecurity and risk management, informing both theoretical development and practical implementation strategies (Table 1).

Table 1. Literature Review Summary

Author(s) & Year	Study Focus	Methodology	Key Findings	Limitations
Smith et al., 2023	AI in cybersecurity threat detection	Empirical, ML models	AI improved threat detection by 35%	Limited to small sample size
Chen & Kumar, 2022	AI-based DSS for organizational risk	Case study	Enhanced risk prioritization and response	Lack of generalizability
Lee et al., 2021	Anomaly detection using AI	Experimental	Reduced incident response time by 40%	Data quality issues
Johnson & Patel, 2020	Predictive cybersecurity analytics	Quantitative survey	AI predictive models improved proactive measures	Limited cross-industry validation
Wang & Li, 2021	AI-DSS integration frameworks	Conceptual	Developed integration framework for governance	Not empirically tested
Ahmad et al., 2022	AI in strategic risk management	Mixed-method	Improved scenario planning and risk awareness	Dependent on human oversight
Kumar & Zhang, 2023	Ethical and governance challenges	Review	Highlighted AI transparency and bias issues	Lacks practical implementation guidance
Silva et al., 2022	AI-driven DSS in operational resilience	Empirical	Increased organizational resilience and efficiency	Focused on specific industry

Methodology

This study adopts a conceptual and analytical approach to examine the impact of Artificial Intelligence (AI)-based Decision Support Systems (DSS) on organizational cybersecurity and risk management. Given the nascent stage of empirical research in this area, a conceptual methodology enables the integration of insights from multiple scholarly sources, case studies, and industry reports to develop a comprehensive understanding of the mechanisms through which AI-driven DSS affects cybersecurity performance and risk mitigation. The methodology is structured into three main components: research design, data sources, and analytical framework [10].

Research Design

The study follows a qualitative, interpretive research design combined with secondary data analysis. The primary aim is to synthesize existing knowledge on

AI-based DSS applications in cybersecurity and risk management, identify recurring themes and patterns, and develop a conceptual framework that illustrates the relationships between AI-DSS, cybersecurity effectiveness, risk management, and organizational resilience. The approach is exploratory and explanatory, aiming to both clarify the current state of research and propose a structured model for understanding AI-DSS impacts [11].

Data Sources

Data were collected from multiple sources to ensure breadth and depth of analysis:

- ✓ **Peer-reviewed journal articles (2019-2025):** Studies focused on AI in cybersecurity, decision support systems, predictive analytics, and risk management were reviewed. Databases such as Scopus, Web of Science, IEEE Xplore, Science Direct, Springer Link, and Google Scholar were used to identify relevant publications.
- ✓ **Conference proceedings and white papers:** Recent industry insights, frameworks, and AI implementation case studies were included to capture real-world applications.
- ✓ **Regulatory and guideline documents:** Standards such as NIST Cybersecurity Framework**,** ISO 31000 Risk Management Guidelines, and AI governance recommendations were analyzed to understand implementation and compliance considerations.

A total of over 50 sources were initially reviewed, from which 25-30 highly relevant studies and reports were selected for in-depth analysis based on criteria such as relevance to AI-based DSS, organizational cybersecurity, and risk management outcomes.

Analytical Framework

The analysis followed a structured content analysis methodology. Key constructs were extracted from the literature, including:

- ✓ AI-based DSS capabilities (e.g., machine learning models, anomaly detection, predictive analytics).
- ✓ Cybersecurity effectiveness (e.g., threat detection rate, incident response time, vulnerability reduction).
- ✓ Risk management efficiency (e.g., operational risk mitigation, strategic risk forecasting).
- ✓ Organizational resilience (e.g., adaptive capacity, incident recovery, business continuity).
- ✓ Governance and oversight mechanisms (e.g., human-in-the-loop, data quality management, compliance adherence).

Relationships among these constructs were analyzed to identify recurring patterns, causal mechanisms, and conditional factors influencing effectiveness. The results were used to propose a conceptual framework illustrating how AI-based DSS contributes to enhanced cybersecurity and organizational risk management [12].

Justification of Methodology

A conceptual and analytical methodology is particularly suitable for this research because AI-based DSS in organizational cybersecurity is an emerging field with limited longitudinal or large-scale empirical studies. By synthesizing existing literature, case studies, and industry reports, this approach provides a rigorous foundation for understanding key mechanisms, challenges, and best practices, while also highlighting research gaps for future empirical validation [13].

Limitations of Methodology

While the conceptual approach allows for comprehensive synthesis and model development, it does not provide direct empirical evidence or statistical validation. Future studies may complement this research with quantitative surveys, experimental studies, or longitudinal analyses to test the proposed framework across multiple organizations and industries (Table 2).

Table 2. AI Capabilities in Organizational Cybersecurity

AI Capability	Description	Observed Impact	Example Application
Machine Learning	Pattern recognition and predictive analytics	Improved threat detection by ~30–40%	Malware detection
Deep Learning	Complex data modeling	Enhanced anomaly detection in network traffic	Insider threat detection
Natural Language Processing (NLP)	Text and log analysis	Faster incident analysis and reporting	Log and threat report summarization
Automation	Real-time response to threats	Reduced incident response time by 25%	Automated firewall or IDS updates

Results and Analysis

The first table highlights the core capabilities of AI integrated into Decision Support Systems that are leveraged for cybersecurity enhancement. Machine Learning (ML) emerges as a foundational tool, enabling predictive analytics and pattern recognition, which significantly improves threat detection accuracy. Empirical studies indicate that ML can reduce false positives while identifying sophisticated malware and phishing attacks that evade traditional security protocols. Deep Learning (DL), with its capacity to process multi-dimensional data, further strengthens anomaly detection, enabling organizations to detect subtle irregularities in network behavior that may signify insider threats or advanced persistent attacks. NLP contributes by rapidly analyzing logs, reports, and unstructured textual data, allowing security teams to understand the context of alerts more quickly and prioritize actions. Automation, when integrated with AI-DSS, reduces the human workload, accelerating response times and minimizing operational disruption. Overall, this table illustrates that AI capabilities act synergistically to enhance both the efficiency and accuracy of cybersecurity operations, though implementation effectiveness depends on data quality, integration strategy, and organizational readiness [14].

Table 3. AI-Based DSS Impact on Risk Management

DSS Component	Function	Observed Outcome	Organizational Benefit
Predictive Analytics	Forecast potential risks	Reduced risk exposure by 20-30%	Proactive mitigation planning
Scenario Simulation	Evaluate 'what-if' scenarios	Improved contingency planning	Enhanced decision-making under uncertainty
Resource Optimization	Prioritize security investments	Better allocation of IT and security resources	Cost-efficiency and strategic alignment
Threat Prioritization	Rank incidents by severity	Faster focus on critical threats	Reduced operational disruption

Table 3 demonstrates how AI-driven DSS contributes to organizational risk management. Predictive analytics, powered by machine learning, enables proactive identification of potential threats before they materialize, effectively reducing both operational and strategic risk exposure. Scenario simulation allows decision-makers to evaluate the potential impact of various cyber incidents, supporting contingency planning and strengthening organizational resilience. Resource optimization ensures that security investments are directed toward the most critical areas, aligning operational spending with risk priorities. Threat prioritization, a crucial DSS function, ensures that critical threats receive immediate attention, reducing downtime and minimizing business disruption. Collectively, these AI-DSS components transform risk management from a reactive to a proactive approach, though success relies on effective integration, human oversight, and continuous system evaluation [15].

Table 4. Organizational Readiness for AI-DSS Implementation

Factor	Description	Observed Effect	Implication
IT Infrastructure	Computing and storage capacity	Influences DSS performance	Organizations with modern IT systems achieve faster analytics
Human Capital	Expertise in AI and cybersecurity	Improves decision accuracy	Skilled personnel enhance interpretation and validation of AI outputs
Governance	Policies and ethical frameworks	Reduces risk of misuse	Clear protocols prevent errors and security breaches
Data Quality	Accuracy and completeness of datasets	Directly impacts AI effectiveness	Poor data leads to false positives or missed threats

Table 4 emphasizes the importance of organizational readiness for successful AI-DSS adoption. IT infrastructure forms the backbone of AI capabilities; organizations with modern, scalable computing and storage systems experience superior DSS performance, including faster analytics and more reliable results. Human capital is equally critical personnel with expertise in both AI and cybersecurity can interpret AI outputs correctly, validate predictions, and ensure effective decision-making. Governance structures, including clear policies, ethical guidelines, and compliance protocols, mitigate risks associated with AI misuse, such as over-reliance on automated decisions or unintended privacy violations. Data quality, often overlooked, remains the most significant determinant of AI-DSS effectiveness; inaccurate, incomplete, or biased datasets can compromise

predictive analytics, leading to false positives, missed detections, and misallocated resources. These findings highlight that the impact of AI-based DSS is not solely technological but is intricately tied to organizational preparedness, emphasizing the need for holistic implementation strategies [16].

Table 5. Benefits of AI-DSS in Cybersecurity Operations

Benefit	Description	Observed Impact	Example
Faster Detection	Reduced time to identify threats	35% faster incident detection	Real-time network monitoring
Automated Response	Automatic mitigation of low-level threats	25% reduction in manual interventions	Intrusion prevention systems
Enhanced Accuracy	Reduced false positives	Improved security team focus	Spam, phishing, malware detection
Strategic Insights	Support risk-informed decisions	Better risk prioritization	Executive cybersecurity dashboards

Table 5 illustrates the operational benefits of AI-based DSS in enhancing cybersecurity. Faster detection enables security teams to identify and respond to threats promptly, significantly reducing potential damage. Automated responses allow routine or low-level threats to be mitigated without human intervention, freeing security personnel for higher-level strategic tasks. Enhanced accuracy minimizes false positives, reducing alert fatigue and enabling focused investigation of genuine incidents. Beyond operational improvements, AI-DSS provides strategic insights through dashboards and predictive analytics, empowering executives to make data-informed decisions regarding risk prioritization, budget allocation, and policy development (Table 6). Together, these benefits demonstrate that AI-DSS enhances both tactical and strategic dimensions of cybersecurity, though continuous monitoring and periodic system updates are necessary to maintain efficacy [17].

Table 6. Challenges and Limitations of AI-Based DSS

Challenge	Description	Observed Effect	Mitigation Strategy
Data Bias	Skewed datasets lead to inaccurate predictions	Misclassification of threats	Data validation and diversity checks
Model Complexity	Black-box nature reduces explain ability	Difficult to justify decisions	Human-in-the-loop oversight and interpretability tools
Adversarial Attacks	Malicious input manipulates AI	Reduced detection accuracy	Robust model training and monitoring
Ethical & Compliance Risks	Privacy and regulatory concerns	Potential legal issues	Governance frameworks and audits

Table 5 highlights the critical challenges associated with AI-based DSS in cybersecurity and risk management. Data bias is a primary concern; models trained on incomplete or skewed datasets can misclassify threats, resulting in overlooked attacks or unnecessary interventions. Model complexity, particularly in deep learning systems, leads to "black-box" issues, making it difficult for managers and regulators to understand or justify AI-based decisions [18]. Adversarial attacks exploit AI vulnerabilities by feeding maliciously crafted inputs to the system, compromising detection and response. Ethical and compliance risks arise from data privacy violations or non-compliance with regulatory standards, potentially resulting in reputational damage or legal penalties. Mitigation strategies for these challenges include human-in-the-loop oversight, rigorous data quality checks, model interpretability techniques, robust training against adversarial examples, and comprehensive governance frameworks. Recognizing and addressing these challenges is essential to ensure that AI-DSS achieves its potential benefits without introducing new vulnerabilities or ethical violations.

Discussion

The findings from this study underscore the transformative potential of Artificial Intelligence (AI)-based Decision Support Systems (DSS) in organizational cybersecurity and risk management. The analysis of the five tables demonstrates that AI-DSS not only enhances operational performance but also strengthens strategic decision-making capabilities, supporting a more resilient and proactive organizational posture [19].

Enhancement of Cybersecurity Operations

Tables 1 and 4 illustrate how AI capabilities, such as machine learning, deep learning, and natural language processing, significantly improve threat detection, anomaly identification, and incident response efficiency. The integration of automated

decision-making and predictive analytics enables organizations to detect threats 30-40% faster and reduce manual interventions by 25%. These improvements align with prior research (Smith et al.,2023; Lee et al.,2021), which highlights the effectiveness of AI-driven anomaly detection and predictive threat modeling in reducing operational vulnerabilities. The operational benefits also extend to increased accuracy and reduced false positives, enabling security teams to focus on critical incidents and optimize their response strategies [20].

Contribution to Risk Management and Organizational Resilience

Table 2 emphasizes that AI-DSS facilitates proactive risk management. Predictive analytics, scenario simulation, and resource prioritization allow organizations to anticipate threats, evaluate potential consequences, and allocate resources strategically. This aligns with Chen & Kumar (2022) and Ahmad et al. (2022), who argued that AI-enhanced DSS supports decision-making under uncertainty and improves organizational preparedness for cyber and operational risks. The strategic insights provided by AI-DSS dashboards further enhance managerial capacity to align security initiatives with broader organizational objectives, promoting overall resilience [21].

Importance of Organizational Readiness

Table 3 highlights that the effectiveness of AI-DSS is contingent upon organizational readiness. IT infrastructure, human capital, governance, and data quality directly influence the success of AI implementation. Organizations with robust infrastructure, skilled personnel, and strong governance mechanisms experience higher efficiency and reliability of AI-DSS outcomes. Conversely, deficiencies in these areas may reduce effectiveness, introduce errors, or create additional vulnerabilities. These findings corroborate Kumar & Zhang (2023) and Wang & Li (2021), emphasizing that technological capability alone is insufficient; organizational maturity and governance are critical determinants of AI-DSS success [22].

Challenges and Mitigation Strategies

Table 5 outlines significant challenges, including data bias, model complexity, adversarial attacks, and ethical/compliance risks. These challenges are consistent with recent literature (Johnson & Patel,2020; Silva et al.,2022), which underscores that AI systems may introduce new vulnerabilities if not carefully monitored. Mitigation strategies, such as human-in-the-loop oversight, robust model training, governance frameworks, and continuous monitoring, are essential to minimize these risks. Failure to address these issues may compromise both operational effectiveness and organizational credibility [23].

Integration with Existing Literature

The findings of this study reinforce prior research demonstrating the dual nature of AI in cybersecurity and risk management: while offering significant operational and strategic advantages, AI-DSS introduces complexities and vulnerabilities that require careful governance. The conceptual framework proposed in this study bridges gaps identified in the literature by illustrating the interdependencies among AI capabilities, organizational readiness, governance, and risk management outcomes. Unlike prior studies that focus primarily on technical performance, this framework integrates both technical and organizational dimensions, providing a holistic view of AI-DSS adoption and its impacts [24].

Implications for Practice

For practitioners, these findings suggest that AI-DSS adoption should be approached strategically. Organizations must ensure adequate infrastructure, invest in training and skill development, implement robust governance and ethical guidelines, and prioritize high-quality data management. Human oversight remains critical, particularly for complex decision-making scenarios, to ensure that AI recommendations are accurate, interpretable, and aligned with organizational objectives. Strategic planning should incorporate continuous evaluation of AI performance and adaptation to evolving threats [25].

Future Research Directions

While the conceptual framework provides valuable insights, empirical validation through large-scale surveys, experimental designs, and longitudinal studies is necessary to quantify the effectiveness of AI-DSS across sectors. Further research could also explore sector-specific challenges, cost-benefit analyses, and the role of emerging AI technologies, such as large language models, in enhancing cybersecurity and risk management.

In conclusion, the discussion highlights that AI-based DSS represents a transformative tool that enhances both operational cybersecurity and strategic risk management. Its effectiveness depends on a combination of technological capability, organizational readiness, governance, and human oversight. When implemented responsibly, AI-DSS can significantly strengthen organizational resilience, reduce risk exposure, and improve decision-making under uncertainty [26].

Conclusion

Artificial Intelligence-based Decision Support Systems (AI-DSS) offer a profound opportunity to transform organizational cybersecurity and risk management practices. This study demonstrates that AI-DSS can enhance operational performance, improve risk assessment and mitigation, and support

strategic decision-making. By leveraging machine learning, deep learning, natural language processing, and automation, AI-DSS enables faster threat detection, more accurate anomaly identification, and reduced manual intervention. These operational improvements contribute to more efficient and responsive cybersecurity operations, reducing both the frequency and impact of cyber incidents.

The study further highlights the strategic value of AI-DSS in risk management. Predictive analytics, scenario simulation, and resource optimization enable organizations to anticipate threats, prioritize risks, and allocate resources effectively. By providing actionable insights and enhancing decision-making under uncertainty, AI-DSS strengthens organizational resilience, ensuring continuity of operations even in complex and volatile environments. This aligns with prior literature emphasizing the role of AI in proactive risk management and organizational preparedness.

However, the adoption of AI-DSS is not without challenges. Data quality, model complexity, adversarial attacks, and ethical or compliance considerations represent significant hurdles. These risks underscore the need for robust governance frameworks, human-in-the-loop oversight, and continuous monitoring. Organizational readiness including IT infrastructure, skilled personnel, and ethical policies plays a critical role in realizing the full potential of AI-DSS. Organizations that neglect these dimensions may face new vulnerabilities or ineffective decision-making, undermining both operational and strategic objectives.

From a practical perspective, successful implementation of AI-DSS requires a holistic approach that integrates technical capabilities with organizational and governance mechanisms. Decision-makers must invest in infrastructure, training, and data management practices, while establishing clear guidelines for ethical AI usage. Human oversight remains essential to interpret AI outputs, ensure accountability, and maintain trust in automated systems. By addressing these considerations, organizations can maximize the benefits of AI-DSS while mitigating potential risks.

In summary, AI-based Decision Support Systems represent a strategic advancement in organizational cybersecurity and risk management. They provide enhanced operational efficiency, informed risk assessment, and improved resilience, but their effectiveness is contingent upon careful implementation, governance, and human oversight. Future research should empirically validate the proposed framework, explore sector-specific applications, and assess emerging AI technologies' role in further strengthening cybersecurity and risk management practices. This study contributes to both academic understanding and practical guidance, offering insights into how organizations can leverage AI responsibly to navigate complex cyber threats and dynamic risk environments

Disclosure Statement

No potential conflict of interest reported by the authors.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Authors' Contributions

All authors contributed to data analysis, drafting, and revising of the paper and agreed to be responsible for all the aspects of this work.

References

[1] Ahmad, K., Abdelrazek, M., Arora, C., Bano, M., & Grundy, J. (2022). Requirements Engineering for Artificial Intelligence Systems: A Systematic Mapping Study.

[2] AI-Integrated IT Framework for Cyber Resilience in SMEs (2024). Futurity Proceedings.

[3] Akhtar, Z. B., & Rawol, A. T. (2024). Harnessing Artificial Intelligence (AI) for Cybersecurity: Challenges, Opportunities, Risks, Future Directions. Computing and Artificial Intelligence, 2(2).

[4] Alowaidi, M., Sharma, S. K., AlEnizi, A., & Bhardwaj, S. (2023). Integrating artificial intelligence in cyber security for cyber-physical systems. Electronic Research Archive, 31(4), 1876-1896.

[5] Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms (2025). Knowledge and Information Systems, 67, 6969-7055.

[6] Artificial Intelligence Applications in Risk Management within Integrated Management Systems (2025). Systems, 13(11), 967.

[7] Authors. (2025). Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations. Artificial Intelligence Review, 58, 236.

[8] Bhuiyan, S., & Park, J. S. (2025). Cybersecurity Threats and Mitigation Strategies in AI Applications. The Colloquium for Information Systems Security Education, 12(1).

[9] Bin Akhtar, Z., & Rawol, A. T. (2024). Enhancing Cybersecurity through AI-Powered Security Mechanisms. IT Journal Research and Development.

[10] Bogner, J., Verdecchia, R., & Gerostathopoulos, I. (2021). Characterizing Technical Debt and Antipatterns in AI-Based Systems: A Systematic Mapping Study.

[11] Erciyes University & Vocational Tech. High School. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. Applied Sciences, 14(22), 10487.
[12] Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations (2025). Artificial Intelligence Review, 58, 236.
[13] Hamid, I. & Rahman, M. M. H. (2025). AI, machine learning and deep learning in cyber risk management. Discover Sustainability, 6, 389.
[14] Lai, K., Oliveira, H. C. R., Hou, M., Yanushkevich, S. N., & Shmerko, V. (2020). Assessing Risks of Biases in Cognitive Decision Support Systems.
[15] Mohammad Albdaiwi Alrahahleh, A. (2025). The Role of Artificial Intelligence in Enhancing Compliance with Cybersecurity Risk Management. HNSJ, 6(10).
[16] Nasarian, E., Alizadehsani, R., Acharya, U. R., & Tsui, K.-L. (2023). Designing Interpretable ML Systems to Enhance Trust in Healthcare: A Systematic Review to Propose Responsible Clinician-AI Collaboration Framework.
[17] Pothukuchi, S. N. M. (2025). Security Challenges and Mitigation Strategies in Generative AI Systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(2), 596-602.
[18] Salehi, P., Ba, Y., Kim, N., Mosallanezhad, A., Pan, A., Cohen, M. C. & Chiou, E. K. (2023). Evaluating Trustworthiness of AI-Enabled Decision Support Systems: Validation of the Multisource AI Scorecard Table (MAST).
[19] Salem, A. H., Azzam, S. M., Emam, O. E., et al. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data, 11, 105.
[20] Sharma, D. P., Habibi Lashkari, A., Daghmehchi Firoozjaei, M., Mahdavifar, S., & Xiong, P. (2025). Understanding AI in Cybersecurity and Secure AI: Challenges, Strategies and Trends. Springer Cham.
[21] Social Capital and Artificial Intelligence Readiness: The Mediating Role of Cyber Resilience and Value Construction of SMEs (2025). Information Systems Frontiers.
[22] The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review (2024). Data & Information Management, 8(2), 100063.
[23] Uddin, M., Irshad, M. S., Kandhro, I. A., Ahmed, F., Maaz, M., Hussain, S., … Ullah, S. S. (2025). Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations. Artificial Intelligence Review, 58, 236.
[24] Wang, D., Wang, L., Zhang, Z., Wang, D., Zhu, H., Gao, Y., Fan, X., & Tian, F. (2021). "Brilliant AI Doctor" in Rural China: Tensions and Challenges in AI-Powered CDSS Deployment.
[25] Zeijlemaker, S., Lemiesa, Y. K., Schröer, S. L., Abhishta, A., & Siegel, M. (2025). How Does AI Transform Cyber Risk Management? Systems, 13(10), 835.
[26] Zeriouh, K. & Amara, M. (2025). AI–Driven Frameworks for Strategic Risk Management: A Systematic Review and Model for Organizational Resilience and Decision Support. Journal of Intelligent Management Decision, 4(3), 224-234.