Intelligent Information Management, 2025, 17(3), 58-77
https://www.scirp.org/journal/iim
ISSN Online: 2160-5920
ISSN Print: 2160-5912

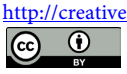
Developing a Comprehensive Cyber Risk Assessment Framework for Supply Chains: Insights into Third-Party Vulnerabilities and Security Gaps

Muhannad Almohaimeed[1*], Faisal Albalwy[2], Rawan Alharbi[1], Aisha Alqarni[1], Abrar Aljohani[1]

[1]Department of Information Systems, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia
[2]Department of Cybersecurity, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia
Email: *mmohimeed@taibahu.edu.sa, TU4570396@taibahu.edu.sa, TU4570421@taibahu.edu.sa, TU4570415@taibahu.edu.sa, fbalwy@taibahu.edu.sa

How to cite this paper: Almohaimeed, M., Albalwy, F., Alharbi, R., Alqarni, A. and Aljohani, A. (2025) Developing a Comprehensive Cyber Risk Assessment Framework for Supply Chains: Insights into Third-Party Vulnerabilities and Security Gaps. *Intelligent Information Management*, **17**, 58-77.
https://doi.org/10.4236/iim.2025.173004

Received: March 14, 2025
Accepted: May 18, 2025
Published: May 21, 2025



Abstract

This research developed an all-rounded cyber risk assessment framework for supply chains, which focused on third-party vulnerabilities and security gaps that arise due to increasing digitalization. The objectives were to identify key cybersecurity vulnerabilities, profile third-party risks, and formulate actionable strategies to enhance resilience. Informed by research questions on principal vulnerabilities, managing third-party risk, and cybersecurity strategies that scale, this methodology combined data analytics and a literature review against aligned frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001. Critical risks included noncompliance standards, ineffective sharing of data, malware threats, and disruption to operations because of system downtime. These would encompass proactive steps such as blockchain-based traceability, improved encryption protocols, and periodic third-party audits. Periodic risk assessments were recommended; IoT and blockchain were used for real-time supply chain visibility; cybersecurity training was provided to stakeholders; and sustainability was integrated within the risk management framework. The contribution resulted in the development of a safe and resilient digital ecosystem with practical solutions to protect organizations from cyber threats while business continuity was assured. Future research should go on to validate the framework in real-world contexts and address the implications of emerging technologies such as quantum computing and AI on supply chain cybersecurity.

Keywords

Supply Chain Cybersecurity, Data Analytics, Risk Assessment, Vulnerability Identification, Third-Party Risk, Risk Management

1. Introduction

Unprecedented digitalization at an unbelievable rate has overpowered the nature of modern supply chains, furthering efficiency and transparency in interconnected networks. Indeed, new technologies such as IoT, cloud computing, and blockchain have further created visibility of real-time data, improving decision-making across supply chains. However, all these developments have brought about overwhelming cybersecurity vulnerabilities, increased the attack surface, and exposed the networks to potential threats at one or many points. While the supply chains become more integrated, they also become more vulnerable to the threats of cyber-attacks that can exploit the weak links across the network. Other vulnerabilities include data breaches, malware attacks, and denial of service attacks, all of which pose a critical disruption to operations, compromise sensitive information, and damage an organization's reputation.

While the supply chains are increasingly embracing digital technologies, the complexity and scale of possible cyber threats grow exponentially. Linton *et al.* note that the interrelatedness of such networks implies that one weak point in a single node can lead to a cascade in the overall system. This is usually interrelated through third-party suppliers, logistics providers, and sometimes even customers, each potentially bringing new vulnerabilities [1]. Manuj and Mentzer emphasize that strategies for supply chain risk management on a global scale need to consider such dynamic and, at times, unpredictable threats. Without proactive steps, organizations run the risk of severe disruptions to operations, customer trust, and regulatory compliance [2].

Besides, even though cybersecurity strategies have improved over time to safeguard critical infrastructure, Luiijf *et al.* state that the national security framework lacks speed to adapt to the cross-border nature of contemporary supply chains [3]. Cybercriminals leverage such jurisdictional gaps to attack via ransomware and phishing against the weak links in the chain. For instance, a supply chain partner with poor cybersecurity could introduce malware into the system that may then spread to larger, more secure organizations. Reade stresses that these kinds of disruptions can have very serious consequences for business continuity, from disrupting production schedules to product delivery [4].

Also, the increasing usage of IoT in supply chains contributes to an increased attack surface. IoT sensors are used to track shipments, manage inventory, and monitor equipment performance, creating and sharing data across the network continuously. However, such devices are usually deployed with limited security

features, making them an easy target for attacks. According to Rongping and Yonggang, securing these endpoints is necessary for preventing data breaches and keeping the integrity of supply chain operations intact [5].

The second critical vulnerability involves information sharing between partners. While transparency and real-time data exchanges enhance decision-making, Manzouri *et al.* warn that data transfers not properly secured will result in unauthorized access or leakage of data [6]. For mitigation of these risks, encryption, authentication protocols, and access control will be necessary. Tran *et al.* have commented that organizations should establish standardized protocols for information sharing in order to protect sensitive data along the value chain [7].

In this regard, comprehensive cyber risk assessment frameworks should be developed to pinpoint third-party vulnerabilities and security gaps. According to Linkov *et al.*, such a framework can include resilience metrics that enable an organization to predict future threats, respond quickly to incidents, and bounce back from disruptions with minimum business loss [8]. Companies should use these frameworks to develop and enhance their supply chain security, ensuring operational continuity and reputation in the modern digitized world.

The proposed research introduces the framework that integrates the cybersecurity risk of the digital supply chains using data analytics. The following are the objectives for which data from multiple touchpoints of the supply chain shall be analyzed in this study:

- **Identify the vulnerabilities:** Find weaknesses in the digital infrastructure that could be used to their advantage by any malicious actor.
- **Third-Party Risk Profiling:** Evaluate suppliers' and partners' cybersecurity postures to determine where threats could happen.
- **Development of Risk Management Strategies:** Recommend efficient measures to be taken for avoiding identified risks which, in turn, would further enhance the supply chain security at large.

In this respect, the research will be focused on those objectives which would help to enhance the cybersecurity resilience of digital supply chains by:

- Data breaches and disruptions are less likely to happen by protecting sensitive information and ensuring business continuity.
- Better supply chain visibility can thereby provide a company with a far greater understanding of the security landscape and possible sources of threats.
- Better decision-making through better-informed cybersecurity investments, armed with data and insights provided to the organizations.
- Promoting a safer, more resilient digital ecosystem.

Though recent literature has highlighted that end-to-end supply chain visibility is important in securing the information flow among network participants, cybersecurity measures so far have focused on the organization in view alone and do not consider the greater supply chain for protection. The modern supply chain is complex, relying on both IoT and real-time data exchange, which multiply these challenges. Hence, considering the said vulnerabilities, there is an immediate need

to develop an organized and all-encompassing risk assessment framework specific to digital supply chains.

In this regard, the framework that this study proposes provides a structured mechanism for monitoring and assessing third-party risks from the digital supply chains. It focuses on the visibility of the risks and their assessment along the continuous chain. Unlike most security models, which have been focused on atomized entities, this framework encompasses the entire value chain for resilience.

The paper proceeds with related works that first cover some foundational theories in cybersecurity in supply chains, determining the gaps in the current frameworks. This is followed by a methodology section that outlines in detail the methods employed in data collection and analysis to develop the proposed framework. The results are then outlined to identify vulnerabilities and third-party risk exposures, followed by recommended strategies to mitigate such risks. The discussion of the findings and their comparison with earlier studies is done next, followed by the conclusion, which highlights the major contributions and pinpoints areas where further research may be conducted.

2. Related Works

Accordingly, modern supply chains are highly digitalized, and with this development, cyber threats have come to be considered one of the most important risks due to the use of third-party data exchange and IoT-driven logistics. Several works presented frameworks and methods for enhancing cybersecurity and risk management within connected supply chain networks.

2.1. Cybersecurity Frameworks for Supply Chains

These risks in supply chains often involve interconnected systems that provide several nodes in a network where vulnerabilities may exist. Syed *et al.* present an important role of traceability in ensuring cybersecurity in supply chains. They started with an asset-centric threat modeling approach by using the STRIDE model and identified as well as mitigated threats about specific assets and their common vulnerabilities. This framework also embeds a scalable and adaptive layered architecture using the GS1 traceability standards. The fact that such a study has been validated shows that threat modeling can reduce cyber threats considerably to ensure data integrity within the supply chain if it is conducted systematically [9].

On this base, Alzahrani and Asghar continue, narrowing their scope to IoT-based logistics systems. They study how logistics-driven IoT systems increase transparency but, at the same time, increase the attack surface hence making the systems vulnerable to unauthorized data access. Their framework proposes a hybrid deep learning model, LSTM combined with CNN, to detect vulnerabilities based on the IoT and reach high accuracy in threat identification. They report an accuracy of detection of 95.73% with this model applied to the BoT-IoT dataset-assurance of AI in managing logistics-based cyber vulnerabilities but at the same

time, a feature selection challenge in threat detection [10].

2.2. Cyber Supply Chain Risk Management (CSCRM)

According to Gani *et al.*, "visibility is the crucial feature of CSCRM to achieve resilience." In this work, the empirical approach was adopted to analyze CSCRM practices in electrical and electronic manufacturing firms. According to the findings, while at the supply chain levels, visibility results in cybersecurity, it also leads to improved decision-making and resilience capabilities against disruptions. It provides evidence of the direct link between the practices of CSCRM, supply chain visibility, and performance; it confirms that visibility aids in achieving business outcomes in a sustainable and competitive manner through interconnected supply chains [11].

Supportive of the findings of Gani *et al.*, and Layode *et al.*, investigate the challenges and future directions toward the issues of cybersecurity within supply chains for sustainability [12]. Their review resolves visibility as a core component in efficient CSCRM; it is mere in coordination and secure information sharing amongst the supply chain participants. This paper emphasizes the importance of holistic CSCRM practices that include not only technical security measures but also the broader organizational and inter-organizational practices needed for resilience in digital networks.

2.3. Risks in Digital Supply Chain 5.0

With the integration of digital twins, AI, and other advanced technologies, new cyber risks have emerged with the recent rise of Supply Chain 5.0 technologies. Zekhnini *et al.* propose an integrated risk assessment model using AHP and DEMATEL to underline the prioritization and analysis of the risks in Supply Chain 5.0. This model identifies key risks that are unique to the environment of Supply Chain 5.0: technological dependence and system complexity. The given study presents practical insights into risk mitigation and resource prioritization by showing the cause-and-effect relationship between such risks, thus enabling supply chain managers to take steps toward proactive identification of vulnerabilities and enhancement of resilience overall [13].

2.4. Supply Chain Characteristics as Predictors of Cyber Risk

Hua *et al.* add to this corpus of literature through a data-driven approach, testing various supply chain characteristics as predictors of cyber risk using machine learning. This article therefore develops a new risk assessment model that can bring in third-party features and draw on concepts rooted in network science in order to extend detection capability. On analyzing the complete dataset comprising more than 30,000 companies, the study shows that including supply chain network features in risk models improves the prediction of cyber risk incidents, adding an out-of-sample AUC increase of 2.3% compared to models leveraging only internal enterprise features [14]. The approach would therefore indicate that

third-party risks bear greater significance in cybersecurity assessment; such models integrating external factors in a comprehensive management of cyber vulnerabilities are hence welcome.

2.5. Smart Supply Chain Risk Assessment Frameworks

Khan has identified such challenges with the digital transformation, such as system complexity, web application failures, and a shortage of talent, and provided a smart supply chain risk assessment framework. Exploratory factor analysis done in Khan's work identifies these as major risk factors in smart supply chains and prioritizes them in order of their impact and probability. This framework identifies unique digital supply chain risks; it gives reason for the fact that proactive risk management is needed for operational continuity and resilience. Khan also established the dire need for adaptable frameworks that can overcome dynamic threats within smart supply chains [15].

2.6. Data-Driven Technologies and Sustainability Risks

Ozkan-Ozen *et al.*, with the increasingly important contribution of data-driven technologies in sustainable supply chains, direct the axe to the risks related to data privacy, information sharing, and traceability, which is prioritized by the authors, taking into consideration their impact on economic, social, and environmental sustainability by using a Multi-Criteria Decision-Making model. The findings showed that data privacy risks and IT system weaknesses have developed as the most critical challenges in the field of sustainable supply chain management; thus, it requires a framework which equally deals with cybersecurity and sustainability issues. This research has underlined the interdependence of digital and sustainable supply chains and the need for a completely integrated risk management strategy for both areas [16].

2.7. Current Research Gap and Contributions of This Study

While existing frameworks provided essential insights into specific aspects of supply chain cybersecurity and risk management, most of these frameworks had a limited focus holistically on third-party vulnerabilities across the network. Consequently, this study tries to fill this gap by developing an integrative framework that fits the identification and securing of third-party risks to assure secure data exchanges along the whole value-added chain. This, unlike other models, gives prominence to end-to-end visibility that will help the organization have an in-depth understanding of the possible cyber threats and make the supply chain resilient.

Though previous models have developed certain cybersecurity practices for supply chains, it is believed that this research study proposes a comprehensive model better suited to third-party vulnerabilities. This framework integrates cybersecurity and risk management strategies related to the interdependent nature of digital supply chains; therefore, extending methods by which improved resili-

ence for global supply networks can be attained.

Table 1 provides a concise summary of the discussed studies, highlighting their focus areas, methodologies, and key findings to clearly outline the current research landscape and demonstrate the contributions of this study.

Table 1. Summary of reviewed studies on cybersecurity and risk management in supply chains.

Reference	Study	Focus Area	Methodology	Key Findings
[12]	Layode *et al.* (2024)	Holistic CSCRM practices for sustainability	Review of visibility and information-sharing challenges	Visibility is essential for secure information sharing and coordination
[10]	Alzahrani and Asghar (2024)	IoT-based logistics systems and AI-driven threat detection	Hybrid deep learning model (LSTM + CNN) with BoT-IoT dataset	95.73% accuracy in detecting vulnerabilities; feature selection challenges
[11]	Gani *et al.* (2023)	Visibility in Cyber Supply Chain Risk Management (CSCRM)	Empirical analysis of CSCRM practices in manufacturing firms	Visibility enhances decision-making and resilience against disruptions
[13]	Zekhnini *et al.* (2023)	Risk assessment in Supply Chain 5.0	Integrated risk assessment using AHP and DEMATEL	Technological dependence and system complexity are key risks
[16]	Ozkan-Ozen *et al.* (2023)	Data-driven technologies and sustainability risks	Multi-Criteria Decision-Making model for sustainability risks	Data privacy and IT system weaknesses are critical for sustainability
[9]	Syed *et al.* (2022)	Traceability and threat modeling in supply chains	Asset-centric threat modeling using STRIDE and GS1 standards	Systematic threat modeling reduces cyber threats and ensures data integrity
[14]	Hua *et al.* (2022)	Supply chain characteristics as predictors of cyber risk	Machine learning model with network science features	Third-party features improve cyber risk prediction (2.3% AUC increase)
[15]	Khan (2021)	Smart supply chain risk assessment framework	Exploratory factor analysis of digital transformation risks	System complexity and talent shortages are major risks

3. Conceptual Framework Description

The conceptual framework is made up of three key components: threat identification, risk assessment, and risk mitigation strategies. Under threat identification, cyber threats are categorized into technical threats such as malware infections and unauthorized access, and operational threats such as system crashes and data compromises. Each of these threats is assessed in terms of its source and its applicability to the supply chain. The Risk Assessment targets third-party risk, which assesses and monitors the performance of its suppliers or partners in terms of compliance, e.g., ISO/IEC 27001-performance, e.g., security audits, and communication practices. It classifies partners as either critical or peripheral, assigning a risk score based on the probability of breaches and their potential consequences. Lastly, Risk Mitigation Strategies will fall under two categories: preventive measures in the form of blockchain traceability, encryption among others, and responsive measures, such as incident response plans. The scalability, cost-effectiveness, and applicability across different supply chain configurations of these

strategies are tested for practical implementation.

3.1. Components of the Framework

It consists of three fundamental elements: threat identification, risk assessment, and strategies to mitigate. Each component is specifically designed to deal with cybersecurity aspects within supply chains clearly and practically.

3.1.1. Threat Identification

It consists of three fundamental elements: threat identification, risk assessment, and risk mitigation strategies. Each component is specifically designed to address a critical aspect of cybersecurity within digitally interconnected supply chains, helping organizations to identify vulnerabilities, evaluate risks, and proactively apply suitable security measures. Figure 1 visually summarizes the proposed cybersecurity risk assessment framework and clearly illustrates the interactions among the main components: threat identification, risk assessment, and risk mitigation strategies.

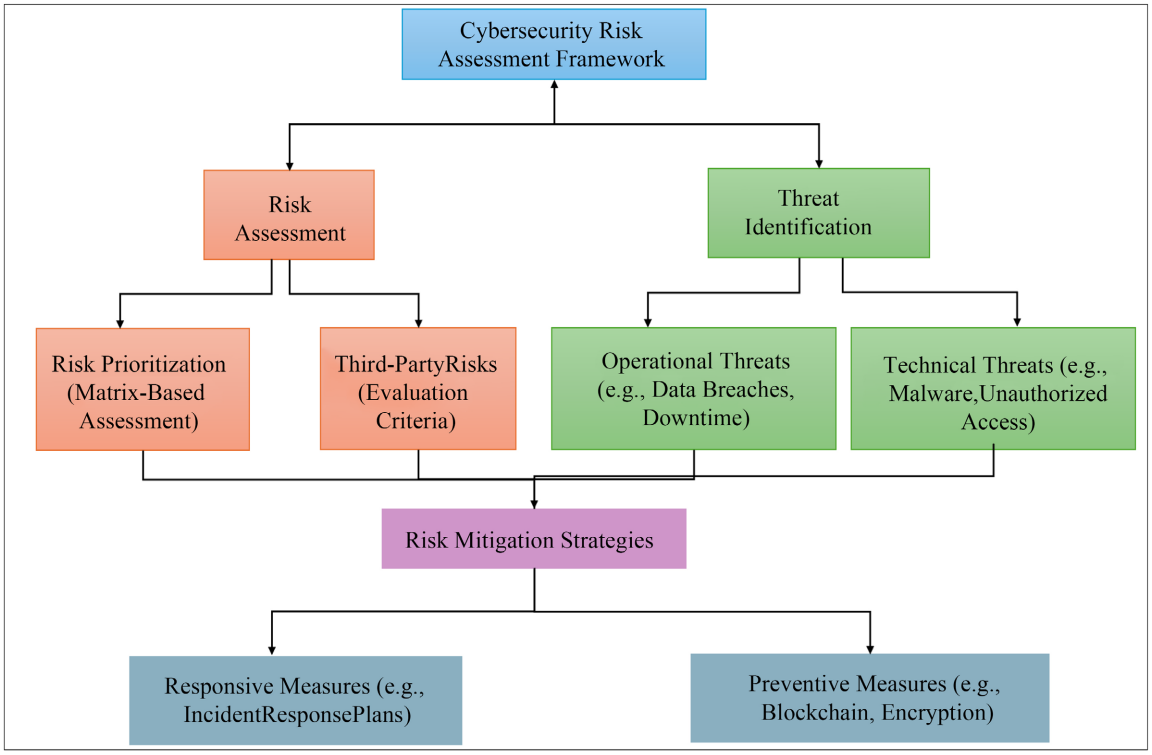


Figure 1. Flowchart of the cybersecurity risk assessment framework for supply chains.

- Technical Threats: These involve vulnerabilities inherent to IT infrastructure, such as malware and ransomware attacks, unauthorized system access, denial-of-service (DoS) attacks, and exploitation of unsecured IoT devices or unpatched systems. These threats primarily exploit digital vulnerabilities to disrupt supply chain operations or compromise sensitive data.

- Operational Threats: These threats relate to disruptions arising from processes and workflow inefficiencies. Examples include system downtime due to third-party software or cloud service disruptions, data breaches resulting from poor encryption practices or inadequate data-sharing protocols, and third-party vendor non-compliance with cybersecurity standards. Operational threats may not necessarily originate from deliberate cyber-attacks but can significantly affect the continuity and reliability of supply chains.

Each threat is assessed clearly regarding its origin (internal or external) and its potential impact (relevance) to the supply chain.

3.1.2. Third-Party Risk Assessment

Third-party partners are reviewed and categorized based on clear criteria:

- **Compliance:** Adherence to recognized security standards, such as ISO/IEC 27001.
- **Performance:** Security audit results, penetration testing outcomes, and vulnerability assessment findings.
- **Communication:** Transparency and effectiveness in reporting security incidents and maintaining security practices.

Partners are classified as either:

- **Critical Partners:** Integral suppliers whose disruption could severely impact supply chain continuity.
- **Peripheral Partners:** Partners with less direct operational impact but who may still pose cybersecurity risks as attack vectors.

Each third party is assigned a risk score clearly based on:

- Likelihood that the partner's cybersecurity posture could lead to a breach.
- Potential severity of impact on supply chain operations.

3.1.3. Risk Mitigation Strategies

The proposed mitigation strategies fall clearly into two practical categories:

- **Preventive Measures: Blockchain-based traceability**, improved encryption standards (**AES-256 for data at rest, TLS 1.3 for data in transit**), and secure data-sharing protocols (**SFTP, HTTPS, and multi-factor authentication (MFA)**).
- **Responsive Measures:** Clear and practical **incident response plans** detailing roles, steps for containment, eradication, recovery, and internal/external communications, supported by continuous monitoring tools such as **Security Information and Event Management (SIEM) systems (e.g., Splunk, IBM QRadar)**.

Strategies align with specific identified risks, ensuring that recommendations are practical, feasible, and directly address existing vulnerabilities.

3.2. Evaluation and Categorization Criteria

The framework clearly defines and structures risk evaluation using the following criteria.

3.2.1. Likelihood of Occurrence

Clearly assessed based on historical cybersecurity data, industry reports, and known vulnerability trends. Likelihood scores range from Low (1) to High (5), representing rare to frequent events, respectively.

3.2.2. Impact on Supply Chain

Clearly evaluated by the severity of disruption, potential financial and reputational damages, and operational downtime. Scores range from Minimal (1) to Critical (5), indicating negligible to severe impacts, respectively.

3.2.3. Third-Party Risk Scoring

The scoring method has been clarified and structured transparently as follows:

- **Compliance:**
  - **Score 1 (Low Risk):** Partners with full ISO/IEC 27001 certification or equivalent adherence to recognized cybersecurity standards.
  - **Score 2:** Partners with strong compliance but minor documented gaps in cybersecurity standards.
  - **Score 3 (Moderate Risk):** Partners actively working toward certification or demonstrating partial adherence to cybersecurity standards.
  - **Score 4:** Partners showing significant gaps in cybersecurity compliance or lacking formal certification processes.
  - **Score 5 (High Risk):** Partners with no recognized certification and minimal or no adherence to cybersecurity compliance standards.
- **Performance:**
  - Score 1 (Low Risk): Partners consistently achieving strong security audit results with no critical vulnerabilities identified.
  - Score 2: Partners demonstrating generally strong performance, with infrequent minor vulnerabilities promptly resolved.
  - Score 3 (Moderate Risk): Partners occasionally show moderate vulnerabilities, typically addressed within a reasonable timeframe.
  - Score 4: Partners regularly encountering notable security issues, with delayed remediation or inadequate response procedures.
  - Score 5 (High Risk): Partners frequently exhibiting critical, unresolved vulnerabilities or failing to complete satisfactory security audits.
- **Communication:**
  - Score 1 (Low Risk): Partners maintaining clearly documented and effective cybersecurity incident reporting processes, with proactive and timely communication.
  - Score 2: Partners generally communicate cybersecurity incidents clearly, with occasional minor delays.
  - Score 3 (Moderate Risk): Partners are occasionally unclear or delayed in communicating cybersecurity incidents or updates.
  - Score 4: Partners frequently exhibiting poor or delayed incident communication practices.

- Score 5 (High Risk): Partners lacking effective cybersecurity communication processes, demonstrating consistently poor, delayed, or nonexistent reporting protocols.

Final third-party risk scores are derived by clearly averaging these sub-scores (Compliance, Performance, and Communication), thus reducing subjectivity and enabling practical, consistent, and transparent risk prioritization. Table 2 below visually summarizes this structured scoring matrix to enhance clarity for practical use.

Table 2. Third-party risk scoring matrix.

Criteria	Score = 1 (Low Risk)	Score = 3 (Moderate Risk)	Score = 5 (High Risk)
Compliance	Full ISO/IEC 27001 certification or equivalent adherence	Partial adherence or actively pursuing certification	No recognized certification or minimal compliance
Performance	Consistently strong audit results, no critical vulnerabilities	Moderate vulnerabilities, resolved within reasonable timeframe	Frequent unresolved critical vulnerabilities
Communication	Clear, effective, and proactive incident communication	Occasional unclear or delayed incident communication	Poor or absent cybersecurity incident reporting

Overall Risk Score = Average of Compliance, Performance, and Communication scores. Low Risk: 1 - 2. Moderate Risk: > 2 - 4. High Risk: > 4 – 5.

3.2.4. Emerging Technology Considerations

The framework explicitly addresses emerging cybersecurity threats related to quantum computing and AI technologies:

- Quantum Computing:

Quantum technologies threaten traditional encryption methods. Future compliance assessments should evaluate partner readiness to adopt quantum-resistant encryption standards.

- Artificial Intelligence (AI):

AI amplifies risks by automating cyber-attacks and complicating detection. Future performance evaluations should include assessments of AI-driven threat detection and response capabilities.

3.2.5. Risk Prioritization

Risks are visually and practically plotted onto a risk matrix as follows:

- **Low Priority:** Risks scoring low (1 - 2) on likelihood and impact.
- **Moderate Priority:** Risks scoring medium (3) on either likelihood or impact.
- **High Priority:** Risks scoring high (4 - 5) on likelihood, impact, or third-party risk.

This structured prioritization ensures clear and practical guidance for risk mitigation priorities.

4. Methodology

The development of the cyber risk assessment framework in regard to digitally interconnected supply chains reliant on third-party vendors will be detailed step

by step. A sound framework identifying the vulnerabilities, studying the potential risks, and offering effective ways of mitigating these for improved supply chain resilience against cyber threats will be developed. This methodology therefore encompasses several elements including framework design, data sources, data analysis techniques, validation procedures, and ethical considerations. The design process incorporates established cybersecurity standards and best practices to keep the framework relevant to real-world applications.

4.1. Framework Design

The framework is designed to address challenges posed by the modern, interconnected supply chain, particularly for those dependent upon third-party vendors. It contains three essential elements: threat identification, risk assessment, and strategies to mitigate those risks.

It provides the evaluation of vulnerabilities from both internal operational perspectives and those of external third-party dependencies within a threat identification phase. Threats might be technical-impacting, like malware infections, unauthorized access, or insecure IoT devices; or operational, like data breaches, system crashes, or lousy data-sharing practices. This will help identify and classify all the possible vulnerabilities for comprehensiveness and multiangulation in potential quick vulnerabilities.

The risk assessment module leverages industry standards, including the NIST Cybersecurity Framework and ISO/IEC 27001, to create the evaluation criteria. Every identified threat is rated on the probability of occurrence and potential impact to supply chain operations. Quantification of these risks through metrics enables organizations to focus on threats and resource allocation in an effective manner to address key vulnerabilities.

For the risk mitigation strategies, the framework goes on to describe in detail action plans aimed at reducing vulnerability and improving resilience. These strategies are directed at increasing supply chain visibility and secure data sharing. The measures have been divided into two groups: preventive actions, which include encryption and blockchain-based traceability; and responsive actions, such as incident response plans and rapid remediation of identified vulnerabilities.

4.2. Data Sources

Secondary data collected from various renowned sources forms the basis of this research to ensure that it is reliable as well as valid in establishing this framework.

Academic articles are core data material, where critical reviews have been carried out based on relevant, peer-reviewed papers comprising case studies and research findings on cybersecurity and supply chain risk management. These give an insight into the present vulnerabilities, factors of risk, and mitigation strategies adopted across various industries.

Besides academic literature, the research will be supported by industry standards including the NIST Cybersecurity Framework and ISO/IEC 27001. These standards give best practices and guidelines on how to manage cybersecurity risks,

hence ensuring the framework is in line with established principles and methodologies.

Further, published reports from cybersecurity organizations and industry bodies are reviewed for practical challenges and real-world solutions. These reports provide an opportunity to learn from past cybersecurity incidents and showcase strategies that have been successfully applied to mitigate supply chain risks.

4.3. Data Analysis Techniques

Several data analysis techniques are developed for constructing a comprehensive framework.

Content analysis is an approach that shall be used to identify the key findings from the literature review by determining recurring vulnerabilities, criteria of effective risk assessment, and proven mitigation strategies. The research systematically analyzes the content such that no critical insight is missed.

A comparative analysis is done to assess the different cybersecurity frameworks that are in place, finding their gaps or weaknesses. Comparing the proposed framework with established models like NIST and ISO/IEC 27001 provides a basis for identifying areas of improvement and innovation, making the framework both comprehensive and adaptable.

It is at this stage that framework synthesis integrates the findings into a cohesive and practical structure. This synthesis process merges threat identification, risk assessment, and mitigation strategies into a single and unified framework applicable to various contexts of supply chains with flexibility and scalability.

4.4. Framework Validation

The proposed framework is subjected to clear validation processes to assess robustness and practical applicability:

- **Theoretical Benchmarking:** Framework alignment with established standards such as the NIST Cybersecurity Framework and ISO/IEC 27001 ensures theoretical soundness.
- **Literature-Based Validation:** Framework components are supported explicitly by reviewed literature examples, strengthening theoretical credibility and applicability.
- **Future Empirical Validation:** Explicit future research direction includes empirical validation through industry collaborations, implementing the framework in real-world supply chain scenarios. Such practical applications and pilot studies will test effectiveness, refine components, and ensure realistic applicability.

4.5. Ethical Considerations

It only relies on publicly available data and literature, which ensures that the research is ethical. No proprietary or confidential information is utilized, and all sources are duly acknowledged. This approach has been undertaken to ensure

transparency and adherence to ethical research practices, thus making the framework as inclusive as possible for various organizations.

5. Results

The specific implications derived from this study have generated knowledge on threats, risk assessment criteria, and mitigation strategies through digitally interconnected supply chains. Each section of the findings has been synthesized to ensure applicability in the framework, deriving solutions to the challenges posed uniquely by cybersecurity risks.

A review of the existing literature highlighted some of the major cybersecurity threats impacting digital supply chains. These were categorized into two major types: technical threats and operational threats. The critical risks from technical threats were malware and ransomware attacks, which destroyed IT systems across supply chains and led to the theft of data and operational shutdowns. **For example, malware attacks exploiting unpatched software vulnerabilities could compromise the inventory management systems across multiple interconnected organizations, causing extended operational downtime and significant data losses.** IoT device vulnerabilities were another major concern, as most IoT devices are designed without robust security measures, thus allowing unauthorized access to and manipulation of sensitive supply chain information. **For instance, attackers could gain entry through insecure IoT sensors, manipulate tracking systems, or alter critical logistical information, causing disruptions across the entire digital supply chain.** Poor authentication systems were also highlighted as major vulnerabilities facilitating unauthorized access, as attackers exploit weak authentication protocols to infiltrate sensitive systems.

Operational threats were among the significant risks to supply chains. Insufficient encryption of data or inefficient practices of data sharing led to leaks of sensitive information, jeopardizing operations and eroding trust among partners. **For instance, third-party vendors transmitting sensitive order or client data without appropriate encryption methods could inadvertently expose critical business information to unauthorized entities, severely damaging trust and resulting in financial and reputational losses.** System downtime, mostly because of reliance on third-party software or cloud platforms, caused operational disruptions in the case of cyberattacks. **For example, reliance on third-party cloud providers without adequate redundancy or backup solutions could result in prolonged disruptions across the supply chain, especially if these providers experience cyber incidents like DDoS attacks or ransomware infections.** Lastly, third-party non-conformity was identified as a critical threat, whereby suppliers and partners failed to meet cybersecurity standards, thus exposing the entire supply chain to increased vulnerabilities. **For instance, a third-party logistics provider with inadequate cybersecurity audits or non-compliant practices could introduce vulnerabilities into the primary organization's infrastructure, leading to a wider breach or system compromise.**

To mitigate these identified threats, the framework proposed a mix of preventive and responsive strategies alongside enhanced vendor management practices. Preventive strategies included proactive measures such as blockchain for secure data exchange and better supply chain traceability, security protocols of IoT devices (hardened authentication and regular firmware updating), and strong encryption standards to prevent unauthorized access to data. Responsive strategies were designed for handling breaches and disruptions effectively, such as incident response plans to quickly remediate breaches and continuous monitoring tools like SIEM systems for real-time detection of threats. Enhanced vendor management practices included periodic security audits of third-party vendors and clearly defined data-sharing agreements specifying encryption requirements and secure access procedures.

The framework was validated using two primary approaches: theoretical comparison and hypothetical scenario application. The framework was theoretically benchmarked against established frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001. While NIST focuses primarily on organizational cybersecurity, this framework extends to encompass third-party risks across interconnected supply chain environments. ISO/IEC 27001 was strong in compliance but lacked realistic strategies for managing interconnected systems.

Furthermore, hypothetical scenarios were presented to demonstrate the practical applicability of the framework. For instance, in one hypothetical scenario, the framework identified the risks posed by a third-party logistics supplier using outdated software, which became a target for cyberattacks, causing severe disruptions to multiple stakeholders. The framework clearly assessed this risk as high, recommending immediate preventive measures such as updating the software, improving data encryption, and strengthening access controls. Additionally, a clear incident response plan was recommended for immediate action if the threat materialized.

Another illustrative scenario highlighted third-party IoT vulnerabilities. A logistics provider relying heavily on IoT devices without robust security measures was vulnerable to unauthorized external access. The framework explicitly evaluated this scenario as high-risk, recommending improved authentication procedures, regular firmware updates, and continuous security monitoring to mitigate such vulnerabilities proactively.

These practical examples clearly illustrated how the framework can systematically identify risks, assess their impacts and likelihoods, and suggest effective mitigation strategies. This approach enhanced the cybersecurity resilience of digital supply chains by ensuring data integrity, reducing disruptions, and protecting sensitive information from potential threats.

6. Discussion

While increased digitalization of supply chains has no doubt improved their efficiency and transparency, it has also created many serious challenges in cyberse-

curity. Specifically, prior studies have discussed the fact that these challenges may result from interrelated systems and third-party dependencies, which further reinforce vulnerabilities. Syed *et al.*, indeed provide a sound basis for the application of traceability as a cyber threat mitigant within supply chains. Their solution utilizes the STRIDE model and asset-centric threats to demonstrate how systematic threat identification adds value. However, though their proposed framework deals with internal vulnerabilities, it has not gone further in focusing on the greater supply chain network, particularly on third-party risk, which this research seeks to achieve.

Equally, Alzahrani and Asghar focused on IoT-based logistics systems that unveiled the two-edged sword of technological advancements. While IoT devices increase the transparency of a supply chain, they also widen the attack surface and open systems to unauthorized data access. Their hybrid deep learning model showcases extremely high accuracy in the detection of vulnerabilities. However, due to the embedding of advanced machine learning techniques, it may be hard for organizations that lack technical expertise or resources to implement it. This research differs by focusing on scalable and practical measures, such as enhancement in encryption protocols and secure data-sharing agreements, which can be more globally applicable.

Visibility is one of the topmost important factors in cyber supply chain risk management, as put forth by Gani *et al.* Their results indicate that visibility helps achieve better decision-making, adding much-needed resilience. Layode *et al.* further supported this by framing visibility as part of holistic risk management practices. From beyond the insights developed in these two studies, neither integrates visibility into actionable strategies for a comprehensive approach toward third-party vulnerabilities. This framework is based on their insights by embedding visibility into all phases of the risk management cycle, from identification to mitigation, thus offering an even more integrated approach.

Zekhnini *et al.* resonated with the rising complexity of digital supply chains with the advent of Supply Chain 5.0 technologies. The method applied by the authors, that is, AHP and DEMATEL for prioritization, will be useful to deduce the underlying cause-and-effect relationship among risks. However, their model deals only with systemic risks such as technological dependence and complexity, which themselves do not take into consideration the challenges arising from third-party entities. This work extends the discussion by adding these neglected aspects to a more comprehensive analytical framework that emphasizes end-to-end risk assessment and mitigation.

Third-party risks remain an essential but relatively unexamined part of the entire sphere of supply chain cybersecurity, as noted by Hua *et al.* Their data-driven analysis documents the importance of supply chain network characteristics in predicting cyber risks. In fact, while their dependence on machine learning improves predictive performance, it limits practical application in environments where data availability or computational resources are at a premium. By contrast, the approach presented here is structured around established, practical, and universally

applicable criteria for evaluation: compliance, performance, and communication.

This is further reiterated in dynamic threats requiring adaptable frameworks in Khan's study on smart supply chains. His listing of the risks related to digital transformation, such as system complexity and failure of web applications, further agrees with the findings in this study. However, while Khan has gone ahead to list these risks, the work of Khan falls short in providing prescriptive measures for organizations in implementing its risk management strategy. This paper attempts to fill this gap by providing actionable measures, including blockchain for traceability, improved security protocols on IoT, and a comprehensive incident response plan.

Ozkan-Ozen *et al.* identified that data-driven technologies in sustainable supply chains introduce an additional layer of complexity. The review indicated that cyber security is interrelated with sustainability through critical vulnerabilities related to data privacy and IT system weaknesses. While the work focused on sustainability issues, the current study limits its scope to cyber security issues; some of the strategies that will be proposed below involve data encryption and secure data-sharing protocols, which do not conflict with sustainable practices.

The proposed framework responds to major gaps in the literature by focusing on third-party vulnerabilities and incorporating them into an integrated risk assessment model. Different from most of the existing frameworks, which either focus on internal organizational security or specific technological risks, this paper adopts a holistic approach that can be used to enhance supply chain resilience. Ensuring practical and scalable strategies also means that this framework could be adopted across a variety of supply chain contexts, thus making the framework a contribution.

Limitations of this study: The study does indeed rely on secondary data, whose capturing and theoretical validation of the framework could not provide realistic tests of its efficiency in real situations. Future studies should try to use this framework in practice, along with feedback from supply chain professionals, to sharpen its components. Apart from that, the implications for cybersecurity in supply chains brought about by the advancement of emerging technologies such as quantum computing need further exploration. Another promising avenue for future work is integrating sustainability considerations into cybersecurity frameworks.

Although there has been partial insight provided by existing research in this respect, this study adopts a framework considering third-party vulnerabilities of supply chain cybersecurity, imparts visibility, and provides actionable risk mitigation strategies. Thus, this would fall under a gap in the literature concerning the recovery from disruptions into a more practical solution to enhance the resilience and security of a modern digital supply chain.

7. Conclusions

While increased digitalization will indeed enhance supply chain efficiency and visibility, this heightens the potential scale of cyber threats from third-party de-

pendencies and IoT-driven logistics. The framework that was developed through the current study represents a truly all-encompassing cybersecurity risk assessment framework that will respond to such challenges from three levels: identification of vulnerabilities, evaluation of third-party risks, and effective mitigation strategies to conduct the assessed risk. This framework pulls together learning from extant literature with a focus on practical, scalable solutions and provides a structured approach towards supply chain resilience and security.

The framework enumerates vulnerabilities based on the categorization of threats into either technical threat, including malware attacks and unauthorized access, or operational threats, which include data breaches and system disruptions. It also provides criteria on risk evaluations such as likelihood, impact, and third-party compliance. It does so by making recommendations for addressing such concerns with actionable strategies, including blockchain-based traceability, enhanced data encryption, and robust incident response plans to ensure practical applicability across diverse supply chain contexts.

Although this study has significant impacts on the research field, the sole use of secondary data and theoretical validation has some shortcomings. Directions for future research must be done by implementing the proposed framework with real-world applications to validate its effectiveness and further refine its components based on practical feedback. Quantum computing and artificial intelligence are other newer technologies that are going to change the scenario, particularly in supply chain security.

Based on the findings, organizations are recommended to do a periodic third-party risk assessment. Organizations should be bound to grade their suppliers and partners on pre-set criteria such as cybersecurity standards compliance, audit performances amongst others. Also, organizations are recommended to have supply chain visibility to be able to create traceability, track everything in real-time over their supply chains using block-chain and IoT technologies. In addition, organizations are recommended to have scalable risk mitigation strategies. Pragmatic measures such as encryption protocols, secure data-sharing agreements, and periodic security audits should be embraced as the principal means of mitigating high-risk vulnerabilities. Moreover, they are recommended to have plenty of training programs to give necessary training for supply chain stakeholders down to third-party vendors for proper security protocol awareness and compliance. Also, integrating sustainability into cybersecurity. This means that any future framework should consider the interaction between cybersecurity and sustainability, where data-driven technologies reinforce green and social objectives.

This framework fills the gap in existing studies and provides an integrated view of cybersecurity risk management in digital supply chains. The focus is on vulnerabilities within third-party elements, and actionable strategies will cement these results together to ensure a secure and robust global supply chain ecosystem. Future research should build on this foundation and extend the framework to include novel threats and changing landscapes of technologies.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Linton, J.D., Boyson, S. and Aje, J. (2014) The Challenge of Cyber Supply Chain Security to Research and Practice—An Introduction. *Technovation*, **34**, 339-341. https://doi.org/10.1016/j.technovation.2014.05.001

[2] Manuj, I. and Mentzer, J.T. (2008) Global Supply Chain Risk Management Strategies. *International Journal of Physical Distribution & Logistics Management*, **38**, 192-223. https://doi.org/10.1108/09600030810866986

[3] Luiijf, E., Besseling, K. and Graaf, P.D. (2013) Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructures*, **9**, 3-31. https://doi.org/10.1504/ijcis.2013.051608

[4] Reade, C. (2009) Human Resource Management Implications of Terrorist Threats to Firms in the Supply Chain. *International Journal of Physical Distribution & Logistics Management*, **39**, 469-485. https://doi.org/10.1108/09600030910985820

[5] Mu, R.P. and Fan, Y.G. (2014) Security in the Cyber Supply Chain: A Chinese Perspective. *Technovation*, **34**, 385-386. https://doi.org/10.1016/j.technovation.2014.02.004

[6] Manzouri, M., Ab Rahman, M.N., Nasimi, F. and Arshad, H. (2013) A Model for Securing Sharing Information across the Supply Chain. *American Journal of Applied Sciences*, **10**, 253-258. https://doi.org/10.3844/ajassp.2013.253.258

[7] Huong Tran, T.T., Childerhouse, P. and Deakins, E. (2016) Supply Chain Information Sharing: Challenges and Risk Mitigation Strategies. *Journal of Manufacturing Technology Management*, **27**, 1102-1126. https://doi.org/10.1108/jmtm-03-2016-0033

[8] Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J. and Kott, A. (2013) Resilience Metrics for Cyber Systems. *Environment Systems and Decisions*, **33**, 471-476. https://doi.org/10.1007/s10669-013-9485-y

[9] Syed, N.F., Shah, S.W., Trujillo-Rasua, R. and Doss, R. (2022) Traceability in Supply Chains: A Cyber Security Analysis. *Computers & Security*, **112**, Article ID: 102536. https://doi.org/10.1016/j.cose.2021.102536

[10] Alzahrani, A. and Asghar, M.Z. (2024) Cyber Vulnerabilities Detection System in Logistics-Based Iot Data Exchange. *Egyptian Informatics Journal*, **25**, Article ID: 100448. https://doi.org/10.1016/j.eij.2024.100448

[11] Gani, A.B.D., Fernando, Y., Lan, S., Lim, M.K. and Tseng, M. (2022) Interplay between Cyber Supply Chain Risk Management Practices and Cyber Security Performance. *Industrial Management & Data Systems*, **123**, 843-861. https://doi.org/10.1108/imds-05-2022-0313

[12] Layode, O., Naiho, H.N.N., Labake, T.T., Adeleke, G.S. and Johnson, E. (2024) Addressing Cybersecurity Challenges in Sustainable Supply Chain Management: A Review of Current Practices and Future Directions. *International Journal of Management & Entrepreneurship Research*, **6**, 1954-1981. https://doi.org/10.51594/ijmer.v6i6.1208

[13] Zekhnini, K., Chaouni Benabdellah, A., Bag, S. and Gupta, S. (2024) Supply Chain 5.0 Digitalization: An Integrated Approach for Risk Assessment. *Management Decision*. https://doi.org/10.1108/md-12-2023-2329

[14] Hua, K., Levia, R., Yahaloma, R. and Zerhounia, E.G. (2022) Supply Chain Charac-

teristics as Predictors of Cyber Risk: A Machine-Learning Assessment. *International Journal of Unconventional Computing*, **18**, 115-144.

[15] Khan, K. (2021) Developing a Framework for Smart Supply Chain Risk Assessment. MSc Thesis, Ryerson University.

[16] Ozkan-Ozen, Y.D., Sezer, D., Ozbiltekin-Pala, M. and Kazancoglu, Y. (2022) Risks of Data-Driven Technologies in Sustainable Supply Chain Management. *Management of Environmental Quality*: *An International Journal*, **34**, 926-942. https://doi.org/10.1108/meq-03-2022-0051