International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Developing a vendor risk assessment model to secure supply chains in U.S. and Canadian Markets

Abidemi Adeleye Alabi [1,*], Olukunle Oladipupo Amoo [2], Christian Chukwuemeka Ike [3] and Adebimpe Bolatito Ige [4]

[1] *Ericsson Telecommunications Inc., Lagos.*
[2] *Amstek Nigeria Limited.*
[3] *GLOBACOM Nigeria Limited.*
[4] *Independent Researcher, Canada.*

International Journal of Science and Research Archive, 2021, 03(02), 230-247

Publication history: Received on 13 July 2021; revised on 23 September 2021; accepted on 25 September 2021

Article DOI: https://doi.org/10.30574/ijsra.2021.3.2.0122

Abstract

In an era of increasing global interconnectivity, securing supply chains has become a critical priority for organizations operating in the U.S. and Canadian markets. This study proposes a comprehensive vendor risk assessment model tailored to address vulnerabilities in supply chains while enhancing resilience and operational security. The model integrates qualitative and quantitative methodologies, leveraging data analytics, machine learning, and risk management frameworks to evaluate vendor reliability, financial stability, compliance with regulations, and cybersecurity preparedness. It incorporates a multi-dimensional approach, encompassing risk identification, assessment, mitigation strategies, and continuous monitoring to address dynamic market challenges. The research identifies key factors influencing vendor risk, including geopolitical instability, regulatory changes, and technological advancements, while emphasizing the importance of collaboration and information sharing between stakeholders. A comparative analysis of the U.S. and Canadian regulatory environments highlights similarities and differences that shape risk assessment practices, providing a basis for localized implementation strategies. The proposed model aims to mitigate risks such as supply chain disruptions, data breaches, and reputational damage by integrating predictive analytics and scenario planning. It emphasizes the role of advanced tools, such as blockchain for transparency, and artificial intelligence for early warning systems, to enable proactive decision-making. By fostering adaptability, the model supports businesses in navigating uncertainties while maintaining compliance with national and international standards. This study contributes to the discourse on supply chain security by offering a robust framework that enhances vendor selection and performance evaluation processes. The findings underscore the necessity of embedding risk assessment as a core element of supply chain management, ensuring sustainability and competitiveness in increasingly complex markets.

Keywords: Vendor Risk Assessment; Supply Chain Security; U.S. Markets; Canadian Markets; Risk Mitigation; Cybersecurity; Predictive Analytics; Regulatory Compliance; Blockchain; Artificial Intelligence; Supply Chain Resilience

1. Introduction

In today's highly interconnected and globalized economy, securing supply chains has become a critical priority for businesses in the U.S. and Canada. The increasing complexity of global supply networks, coupled with the growing reliance on international vendors, exposes organizations to various risks. These risks range from operational disruptions and geopolitical tensions to cybersecurity threats and natural disasters (Dalal, Abdul & Mahjabeen, 2016, Shafqat & Masood, 2016). Disruptions in supply chains can have severe consequences, including production delays,

* Corresponding author: Abidemi Adeleye Alabi

financial losses, reputational damage, and compliance issues, all of which can significantly impact business continuity and profitability.

The recent rise in supply chain disruptions, such as those caused by the COVID-19 pandemic and trade wars, has underscored the vulnerability of organizations to external shocks. As a result, businesses in North America are increasingly focusing on securing their supply chains to mitigate these risks. Effective supply chain security is essential not only for ensuring operational efficiency but also for maintaining customer trust and regulatory compliance. To achieve this, companies must adopt comprehensive risk management strategies that encompass the entire supply chain, from raw material sourcing to final delivery (Bodeau, McCollum & Fox, 2018, Georgiadou, Mouzakitis & Askounis, 2021).

This study aims to develop a robust vendor risk assessment model tailored to the specific needs of businesses in the U.S. and Canadian markets. The goal is to provide a framework that helps organizations identify, assess, and manage the risks associated with their suppliers and third-party vendors. By evaluating factors such as financial stability, cybersecurity practices, compliance with regulations, and resilience to disruptions, businesses can better understand the risks within their supply chains and take proactive measures to mitigate them (Buchanan, 2016, Clemente, 2018, Djenna, Harous & Saidouni, 2021). Ultimately, the model seeks to enhance the resilience and operational security of organizations by ensuring that they can respond effectively to potential disruptions while safeguarding their long-term success in a competitive market.

2. Literature Review

The increasing interdependence of global markets and the expanding scope of supply chains have brought both significant opportunities and notable risks for businesses in the U.S. and Canada. As organizations rely more heavily on external vendors and suppliers, the vulnerabilities associated with these external relationships have become more pronounced (Elujide, et al., 2021). Vendor risk is a critical consideration in securing supply chains, as disruptions can have cascading effects on business operations, regulatory compliance, and the financial performance of organizations (Aliyu, et al., 2020, Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016). Understanding these risks and creating a comprehensive risk assessment model is essential for businesses seeking to maintain resilience in the face of emerging threats.

Vendor risk in supply chains manifests in several common forms, with cybersecurity, compliance, and geopolitical risks being among the most critical. Cybersecurity risks arise from the growing integration of technology in supply chain operations, particularly as businesses rely on third-party vendors for services such as data storage, software applications, and logistics. These vendors often have access to sensitive data, systems, and intellectual property, making them prime targets for cyberattacks (Djenna, Harous & Saidouni, 2021, Sabillon, Cavaller & Cano, 2016). A breach in a vendor's system can expose an organization to data loss, intellectual property theft, and significant disruptions in services, potentially affecting business continuity. The vulnerability of vendors to cyberattacks can, in turn, compromise the security of the entire supply chain.

Compliance risks are another significant concern in vendor relationships. With the rise of global trade and regulatory complexity, businesses must ensure that their vendors adhere to relevant regulations, standards, and industry practices. In the U.S. and Canada, industries such as healthcare, finance, and manufacturing face stringent regulatory requirements that can vary from one jurisdiction to another (Amin, 2019, Cherdantseva, et al., 2016, Dupont, 2019). A vendor's failure to comply with these regulations can expose the contracting organization to legal liability, fines, and reputational damage. Non-compliance issues can arise in areas such as data privacy, environmental standards, and labor practices, and organizations must have processes in place to verify that their vendors are meeting these requirements.

Geopolitical risks have become increasingly prominent as global supply chains have become more interconnected. Tensions between countries, such as trade disputes, tariffs, and changes in government policies, can create disruptions in the supply of goods and services. Geopolitical events, such as the imposition of economic sanctions or the onset of trade wars, can destabilize established supply chains, forcing businesses to seek alternative vendors or face delayed shipments (Kovacevic & Nikolic, 2015, Pomerleau, 2019). Additionally, political instability in certain regions can affect the ability of vendors to fulfill contracts or deliver products on time. These geopolitical risks can have far-reaching consequences for organizations that rely on international supply networks. Strategic orientation of a sample of cyber supply chain initiatives as presented by Boyson, 2014, is shown in figure 1.

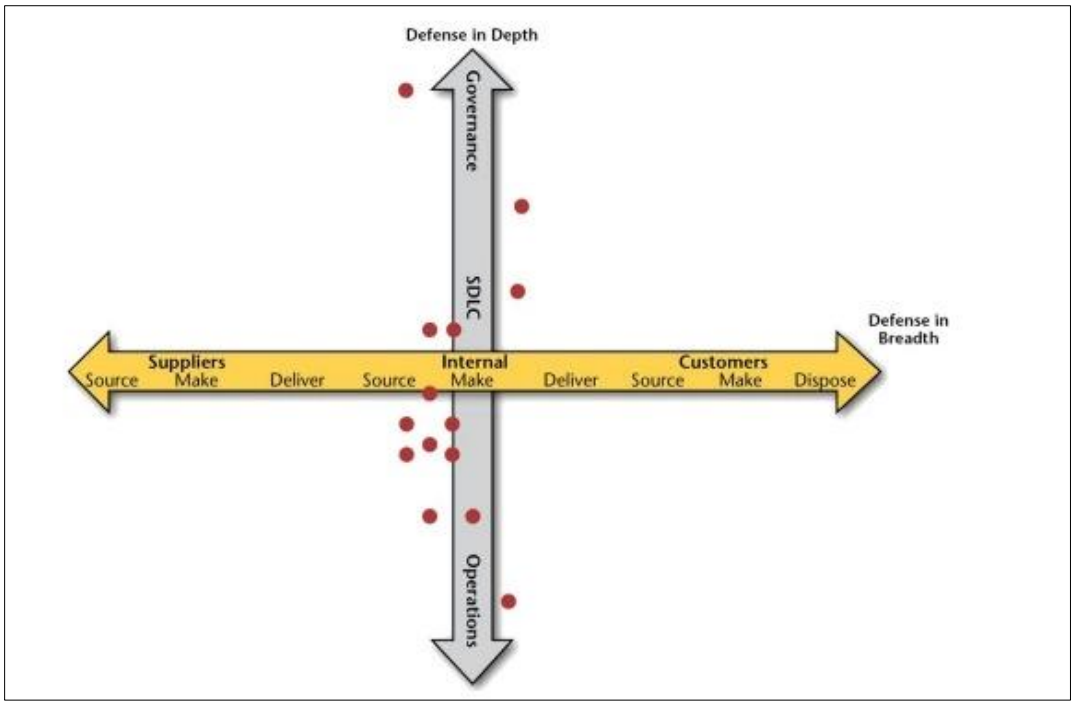

Figure 1 Strategic orientation of a sample of cyber supply chain initiatives (Boyson, 2014)

Case studies of supply chain disruptions in the U.S. and Canada provide a sobering view of the risks inherent in vendor relationships. For example, the 2011 earthquake and tsunami in Japan led to widespread disruptions in the global supply chain, particularly affecting the automotive and electronics industries. Many companies in North America were dependent on suppliers in Japan, and when these suppliers were incapacitated, production lines in the U.S. and Canada were delayed or shut down (Hussain, et al., 2021, Ike, et al., 2021). This event underscored the vulnerability of supply chains to natural disasters and highlighted the importance of having contingency plans in place. Similarly, the COVID-19 pandemic revealed the fragility of global supply chains, as businesses in both the U.S. and Canada faced disruptions in manufacturing, transportation, and inventory management. Companies that relied heavily on overseas suppliers were particularly affected, as lockdowns and restrictions led to delays in production and shipping.

The need for a robust vendor risk assessment model is evident in light of these vulnerabilities and disruptions. A strong risk assessment model helps organizations identify potential risks within their supply chain, assess the likelihood and impact of these risks, and develop strategies to mitigate them. Several existing risk assessment models are currently in use across various industries, but they often face limitations in terms of their comprehensiveness, adaptability, and integration with data-driven decision-making processes (Austin-Gabriel, et al., 2021, Clarke & Knake, 2019, Oladosu, et al., 2021).

Existing risk assessment models typically focus on identifying specific risks such as financial instability, operational performance, or legal compliance. These models often rely on qualitative assessments, historical data, and subjective judgment, which can limit their accuracy and relevance in rapidly changing environments (Austin-Gabriel, et al., 2021, Oladosu, et al., 2021). While useful in some contexts, traditional risk models may not be sufficiently dynamic to address the range of complex, interconnected risks faced by modern supply chains. For example, a traditional financial risk model may not account for the risks associated with cybersecurity or geopolitical instability, leaving significant vulnerabilities unaddressed. Supply chain risk assessment tools as presented by Schlegel & Trent, 2014, is shown in fiure 2.

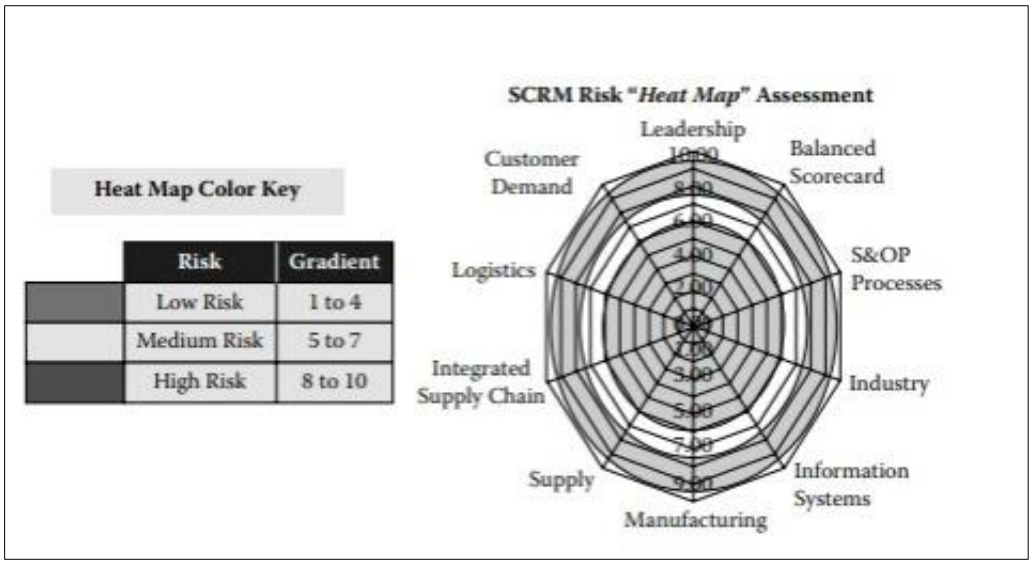

Figure 2 Tools: supply chain risk assessment (Schlegel & Trent, 2014)

Additionally, many existing models do not effectively integrate real-time data, which is increasingly necessary to assess and mitigate risks. In today's fast-paced business environment, supply chain risks can evolve rapidly, and relying on outdated data or static models can leave organizations ill-prepared for emerging threats. A more data-driven approach to vendor risk assessment is needed to provide businesses with the agility to respond to evolving risks (Aaronson & Leblond, 2018, Newlands, et al., 2020). Real-time data on vendor performance, compliance records, and security vulnerabilities can significantly enhance the effectiveness of risk assessment models by providing up-to-date insights into potential threats.

An integrated, data-driven vendor risk assessment model could address these limitations by incorporating multiple risk factors and leveraging advanced technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics. By using AI and ML, businesses can continuously monitor their supply chains, identify patterns and trends in risk behavior, and predict potential disruptions before they occur. For instance, machine learning algorithms could analyze past data to predict the likelihood of a cybersecurity breach or assess the potential impact of a vendor's non-compliance with regulatory standards (Elujide, et al., 2021, Igo, 2020). This predictive capability could enable organizations to take proactive measures to mitigate risks before they escalate.

Moreover, an integrated model would incorporate a holistic approach to risk, considering not just financial or operational factors but also cybersecurity, compliance, geopolitical, and environmental risks. By combining these various factors into a unified framework, businesses can gain a comprehensive understanding of the risks within their supply chains and make informed decisions about vendor selection, risk mitigation strategies, and contingency planning (Dwivedi, et al., 2020, Feng, 2019). This integrated approach would also allow for better coordination across different departments within an organization, from procurement and logistics to compliance and cybersecurity, ensuring that all relevant stakeholders are aligned in their efforts to secure the supply chain.

In conclusion, the development of a robust vendor risk assessment model is essential for securing supply chains in the U.S. and Canadian markets. The vulnerabilities associated with vendor relationships—ranging from cybersecurity and compliance risks to geopolitical disruptions—require businesses to adopt a more comprehensive and data-driven approach to risk management. Existing models, while useful, are often limited in their scope and adaptability, underscoring the need for an integrated, data-driven framework that can account for the full range of risks facing modern supply chains (Atkins & Lawson, 2021, Robinson, 2020). By leveraging advanced technologies and adopting a holistic risk assessment approach, businesses can enhance the resilience of their supply chains, reduce vulnerabilities, and ensure business continuity in an increasingly complex global marketplace.

2.1. Key Components of the Proposed Model

The development of a vendor risk assessment model for securing supply chains in the U.S. and Canadian markets is essential to address the growing challenges that organizations face in managing external vendor relationships. The proposed model seeks to offer a comprehensive approach to identifying, assessing, and mitigating vendor risks,

ensuring the resilience and continuity of supply chains (Bamberger & Mulligan, 2015, Voss & Houser, 2019). The model incorporates key components such as risk identification, risk assessment and analysis, risk mitigation strategies, and continuous monitoring and evaluation. Each of these elements plays a crucial role in building a robust framework that addresses the complexities of modern supply chains, ensuring businesses can proactively manage vulnerabilities and adapt to evolving risks.

Risk identification is the foundational step in the proposed model. It involves identifying potential risks associated with vendors and their impact on the supply chain. The model takes a comprehensive approach by incorporating various criteria to assess vendor risk. These include financial stability, regulatory compliance, and cybersecurity preparedness. Financial stability is essential because a vendor's financial health can directly affect their ability to meet contractual obligations, especially in times of economic stress (Jathanna & Jagli, 2017). Assessing the financial stability of vendors allows organizations to anticipate potential disruptions due to liquidity problems, bankruptcies, or other financial distress. Regulatory compliance is another critical criterion, as vendors need to adhere to relevant laws, standards, and industry practices. Non-compliance with local or international regulations, including those governing data privacy, labor practices, or environmental protection, can expose organizations to significant legal and reputational risks (Bello, et al., 2021, Yang, et al., 2017). Cybersecurity preparedness is increasingly important as organizations become more reliant on third-party vendors for services involving sensitive data and IT systems. A vendor's cybersecurity practices can directly impact the security of an organization's data and networks, making it essential to assess their capabilities in defending against cyber threats. The model also incorporates vendor segmentation based on criticality and risk levels, ensuring that organizations focus their resources on high-risk and critical vendors, while adopting proportionate risk management strategies for lower-risk vendors. This segmentation allows for prioritizing risk mitigation efforts in areas that would have the most significant impact on business operations.

The next component, risk assessment and analysis, evaluates the likelihood and potential impact of identified risks. The model utilizes specific metrics to determine the severity of these risks and to establish risk tolerance thresholds. Likelihood refers to the probability of a risk materializing, while impact assesses the potential consequences if the risk were to occur. By analyzing these two factors, organizations can determine the overall risk level associated with each vendor. Risk tolerance thresholds are used to define the acceptable levels of risk that an organization is willing to accept (Lanz, 2022, Shackelford, Russell & Haut, 2015, Shackelford, et al., 2015). These thresholds can be based on a variety of factors, including industry standards, the criticality of the vendor, and the organization's overall risk appetite. Techniques such as scoring models and heat maps are used to quantify and visualize risk. Scoring models assign numerical values to risks based on predefined criteria, making it easier to compare and prioritize vendors. Heat maps, on the other hand, visually represent risks by mapping their likelihood and impact on a color-coded grid. This allows organizations to quickly identify high-risk areas in their supply chains and allocate resources to mitigate these risks effectively. The four stages of a fraud, corruption, or supply chain disaster as presented by Schlegel & Trent, 2014, is shown in figure 3.

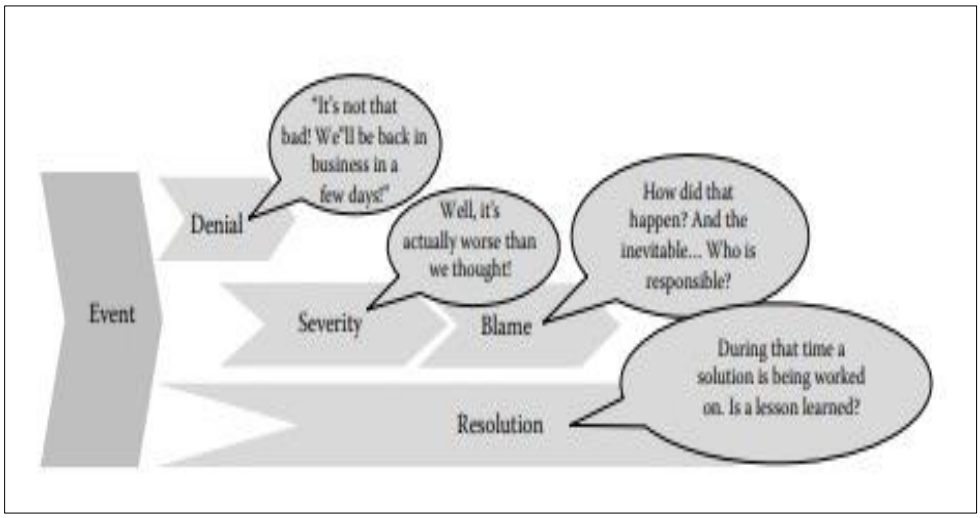

Figure 3 The four stages of a fraud, corruption, or supply chain disaster (Schlegel & Trent, 2014)

Once risks have been identified and assessed, the model moves to the risk mitigation strategies component. This step involves developing contingency plans and mitigation measures to address the risks identified in earlier stages.

Contingency plans are designed to provide businesses with predefined responses in the event that a risk materializes. These plans may include alternative sourcing strategies, backup suppliers, or alternative transportation routes in case of disruptions in the supply chain (Atkins & Lawson, 2021, Cohen, et al., 2022, Sabillon, Cavaller & Cano, 2016). Developing these plans ensures that businesses can maintain continuity in their operations even if their primary vendors face challenges. Mitigation measures aim to reduce the likelihood of a risk occurring or to minimize its impact if it does occur. These may include cybersecurity protocols, enhanced vendor audits, and contractual safeguards that hold vendors accountable for meeting certain standards. Additionally, the role of collaborative frameworks between vendors and stakeholders is critical to risk mitigation. By fostering a transparent and collaborative relationship, organizations can work together with their vendors to identify potential risks, share information, and implement solutions to improve risk resilience across the entire supply chain. These frameworks encourage proactive engagement and shared responsibility for risk management, which can lead to better outcomes in managing vendor-related risks.

The final key component of the proposed model is continuous monitoring and evaluation. Risk management is not a one-time exercise but an ongoing process that requires regular reassessment to remain effective. The use of real-time data and analytics is essential in ensuring that organizations can respond to emerging risks quickly and efficiently. With advancements in technology, businesses can continuously monitor their supply chains, collecting data on vendor performance, financial health, cybersecurity posture, and compliance status (Abraham, Chatterjee & Sims, 2019, Ustundag, et al., 2018). This data-driven approach provides a dynamic view of the supply chain, allowing organizations to make informed decisions about which vendors may require additional oversight or risk mitigation. The ability to track vendor performance over time also allows businesses to identify trends and patterns that may indicate a shift in risk levels. Mechanisms for periodic reassessment are built into the model to ensure that risk management practices remain relevant and effective. These reassessments can be conducted at regular intervals or in response to specific events or changes in the market, such as new regulatory requirements, shifts in geopolitical conditions, or changes in vendor behavior. Periodic evaluations allow organizations to adjust their risk management strategies in response to changing circumstances, ensuring that they remain agile and responsive to potential threats.

In conclusion, the proposed vendor risk assessment model for securing supply chains in the U.S. and Canadian markets incorporates essential components that work together to address the complexities of managing vendor relationships. Through a systematic approach to risk identification, assessment, mitigation, and continuous monitoring, the model empowers organizations to enhance supply chain resilience, reduce vulnerabilities, and maintain business continuity in an increasingly uncertain global marketplace (Ani, He & Tiwari, 2017, Djenna, Harous & Saidouni, 2021). By focusing on key criteria such as financial stability, regulatory compliance, and cybersecurity preparedness, and leveraging data-driven techniques like scoring models and heat maps, businesses can make informed decisions about managing vendor risks. Furthermore, by fostering collaboration with vendors and stakeholders, organizations can build stronger, more resilient supply chains capable of adapting to emerging threats and challenges. Continuous monitoring and periodic reassessment ensure that the model remains dynamic and responsive to the evolving risk landscape. Ultimately, this comprehensive approach to vendor risk management helps organizations secure their supply chains and safeguard their operations against disruptions.

3. Comparative Analysis of U.S. and Canadian Regulatory Environments

In developing a vendor risk assessment model to secure supply chains in U.S. and Canadian markets, understanding the regulatory environments of both countries is essential. The regulatory frameworks in the U.S. and Canada share certain similarities but also exhibit significant differences, which have important implications for vendor risk management practices. The diverse regulatory landscapes of the two nations necessitate tailored strategies to ensure compliance and effective risk assessment practices when managing vendors in each jurisdiction. The comparative analysis of these regulatory environments is crucial in designing a model that addresses the specific needs and requirements of both markets while maintaining a unified approach to securing supply chains.

The regulatory frameworks governing business practices in the U.S. and Canada share several key similarities, especially in areas related to data protection, financial regulations, and environmental standards. Both countries have robust regulatory regimes aimed at protecting consumers, ensuring fair business practices, and promoting operational transparency. For instance, both the U.S. and Canada adhere to international standards in cybersecurity and privacy protection. The U.S. has the Federal Trade Commission (FTC) and the Cybersecurity and Infrastructure Security Agency (CISA), which enforce regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR)-aligned California Consumer Privacy Act (CCPA) at the state level (Smart, 2017, Yeung, et al., 2017). Similarly, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) provides a regulatory framework for data privacy and security, which aligns with global standards like the GDPR.

However, key differences exist between the U.S. and Canadian regulatory environments. One major distinction is the approach to data sovereignty and protection. While both countries are committed to safeguarding personal data, Canada places a stronger emphasis on protecting data within its borders through policies that prioritize data residency. This has implications for vendor risk assessments, as companies operating in Canada must ensure that their data storage and management practices comply with the requirements for storing and processing data locally (Flores, 2019, Park, 2015). In contrast, U.S. regulations often prioritize cross-border data flows, and American companies tend to favor global cloud-based solutions that store data in various international jurisdictions. These differing approaches influence the way vendors are assessed in each market, as companies in Canada may require additional safeguards and compliance assurances from vendors who handle sensitive data.

Another notable difference is the regulatory approach toward anti-corruption and bribery laws. The U.S. has stringent regulations in this regard, notably the Foreign Corrupt Practices Act (FCPA), which makes it illegal for U.S. companies to engage in bribery or corrupt practices with foreign officials. The FCPA also has extraterritorial reach, meaning it applies to foreign entities that do business with U.S. firms. In Canada, the equivalent is the Corruption of Foreign Public Officials Act (CFPOA), but the enforcement and application of this law are perceived to be less aggressive than the FCPA (Callaghan, 2018, Trew, 2021). This distinction creates a unique challenge for companies operating across both markets, as they must ensure that their vendor relationships and supply chain practices comply with these differing standards.

The implications of these regulatory differences for vendor risk assessment practices are significant. In the U.S., the focus is more on ensuring that vendors comply with laws governing data protection, cybersecurity, and anti-corruption, often with a view to facilitating global trade and operational flexibility. Vendor risk assessments in the U.S. tend to place a heavier emphasis on ensuring vendors adhere to broad, national regulations like the FCPA, as well as state-level privacy regulations such as CCPA (Al-Hassan, et al., 2020, Haugh, 2018, Zaccari, 2016). In Canada, however, risk assessments must consider stricter data residency and localization requirements, in addition to ensuring compliance with Canadian privacy laws. Companies must carefully evaluate their vendors' data handling practices and assess the risk associated with cross-border data transfers, particularly with vendors based outside of Canada.

The different regulatory approaches also affect how companies in each market approach financial regulations. The U.S. has a complex web of financial regulations at the federal and state levels, including the Sarbanes-Oxley Act (SOX), the Dodd-Frank Act, and various state-specific regulations. These laws impose stringent requirements on vendors who provide financial services, requiring thorough due diligence and compliance audits to ensure vendors meet the necessary financial and reporting standards (Ele & Oko, 2016, Nicho, et al., 2017, Papazafeiropoulou & Spanaki, 2016). In Canada, financial regulations are more centralized, with the Office of the Superintendent of Financial Institutions (OSFI) overseeing the financial sector’s regulatory framework. The streamlined regulatory environment in Canada means that vendor risk assessments may be simpler in this domain, but companies must still account for specific industry regulations and maintain robust financial oversight in their relationships with vendors.

Localization strategies for implementing a vendor risk assessment model in the U.S. and Canada are necessary to address these regulatory differences while ensuring a consistent and effective approach to vendor risk management. For U.S.-based companies, the focus should be on building flexibility into the risk assessment model to accommodate the diverse regulatory landscape. This may involve integrating compliance tools that address state-specific privacy laws like CCPA, while also ensuring that vendors comply with federal regulations such as HIPAA and FCPA (Recor & Xu, 2016, Sanaei, et al., 2016, Sikdar, 2021). The model should also incorporate tools for assessing the cybersecurity practices of vendors to ensure compliance with national standards such as those set by CISA and the National Institute of Standards and Technology (NIST).

For Canadian companies, the model should be more focused on data residency and sovereignty, ensuring that vendors comply with PIPEDA and other Canadian privacy laws. This can be achieved by implementing more rigorous vendor vetting processes to ensure that vendors adhere to strict data protection and storage requirements. It may also involve the use of compliance software that specifically addresses Canadian regulations, helping businesses track and manage their vendor relationships in line with Canadian legal standards (Govindji, Peko & Sundaram, 2018). For both U.S. and Canadian markets, the vendor risk assessment model should incorporate mechanisms for tracking the evolving regulatory landscape, ensuring that companies can remain agile and respond to regulatory changes as they arise.

Furthermore, localization strategies should address the operational and cultural differences between the two countries. In the U.S., businesses tend to prioritize operational flexibility and scalability, which may encourage the adoption of cloud-based systems and global supply chain practices. The vendor risk assessment model in the U.S. should incorporate criteria that reflect this global mindset, such as evaluating a vendor’s ability to meet international standards and handle cross-border data transfers (Fefer, 2019, Sullivan, 2019, Voss, 2019). In contrast, Canadian companies may place greater

emphasis on vendor risk mitigation strategies that are focused on local compliance and regulatory adherence. The model should therefore incorporate specific considerations for managing risks associated with cross-border data flows, especially in sectors like finance and healthcare.

In conclusion, the comparative analysis of the U.S. and Canadian regulatory environments highlights the need for a tailored approach to developing a vendor risk assessment model. While both countries share similar regulatory goals in terms of data protection, financial regulations, and anti-corruption laws, there are distinct differences that must be taken into account (Minssen, et al., 2020, Tian, 2016). Companies operating in both markets must ensure their vendor risk assessment practices are adaptable and localized to comply with the unique regulatory requirements of each country. By understanding the regulatory nuances of the U.S. and Canada, organizations can develop a comprehensive, effective model for securing their supply chains and minimizing vendor-related risks.

4. Methodology

The methodology for developing a vendor risk assessment model to secure supply chains in U.S. and Canadian markets involves a structured approach that integrates both qualitative and quantitative research methods. A mixed-methods approach provides a comprehensive understanding of the complex dynamics that shape vendor risk and supply chain vulnerabilities in these markets. By combining qualitative insights from supply chain professionals with quantitative data on risks and disruptions, the methodology ensures that the model developed is both practical and data-driven, capable of adapting to the evolving landscape of global supply chains.

The research design is based on a mixed-methods approach, where both qualitative and quantitative analysis are used to collect a rich set of data. This methodology allows for an in-depth exploration of the factors influencing vendor risk while also providing a solid statistical foundation for risk assessment. Qualitative methods, including interviews and surveys with industry experts, provide insights into the subjective aspects of vendor risk, such as vendor reliability, compliance culture, and operational risk factors that may not be captured in existing quantitative datasets (Celeste & Fabbrini, 2020, Mattoo & Meltzer, 2018, Tehrani, Sabaruddin & Ramanathan, 2018). These expert opinions are crucial for understanding the nuanced relationships between vendors and the various operational, financial, and geopolitical challenges that impact supply chain security in the U.S. and Canadian contexts. On the other hand, quantitative analysis involves gathering empirical data on vendor performance, historical disruptions, and risk events to provide statistical evidence of patterns and correlations that can inform the development of the model.

Data collection methods are designed to capture a broad spectrum of insights, focusing on both the strategic and operational dimensions of vendor risk management. Surveys and interviews with supply chain professionals in both the U.S. and Canada will serve as the primary sources of qualitative data. These will target professionals from industries such as manufacturing, logistics, technology, and healthcare, where vendor risk management is critical to operational success (Malhotra, 2018, McCubbrey, 2020). The survey instrument will include questions designed to assess how these professionals perceive risks associated with vendors, their experiences with vendor-related disruptions, and the existing strategies they use to manage vendor relationships. The interviews will provide deeper insights into the decision-making processes surrounding vendor selection, risk mitigation, and crisis management, offering valuable qualitative data on best practices and challenges faced by supply chain managers.

In addition to primary data collection from professionals, case studies of successful and failed vendor partnerships will be examined. These case studies will offer concrete examples of vendor risks in action and highlight the practical challenges of assessing vendor performance and mitigating risks in real-world scenarios. The case studies will include both U.S. and Canadian firms, allowing for a comparative analysis of how vendor risk management is approached in different regulatory and market contexts (Aboelfotoh & Hikal, 2019, Garrett, 2018, Shackelford, et al., 2015). By studying the outcomes of these partnerships, the research will identify key factors that contribute to successful vendor relationships and supply chain resilience, as well as the lessons learned from failed partnerships.

Once the data is collected, the next phase of the methodology involves applying advanced data analysis techniques to process and interpret the findings. Statistical modeling and predictive analytics will be used to quantify the risks associated with various vendor characteristics, such as financial stability, cybersecurity preparedness, and compliance with industry regulations. This approach will help establish the correlation between specific vendor attributes and the likelihood of disruptions, enabling the identification of high-risk vendors and critical vulnerabilities within the supply chain. Statistical models, such as regression analysis or factor analysis, will allow for the measurement of risk factors across different vendor types and industry sectors, providing actionable insights into how supply chain risks can be mitigated at various levels of vendor engagement.

In addition to traditional statistical methods, machine learning techniques will be employed to improve the predictive power of the vendor risk assessment model. Machine learning algorithms, such as decision trees, support vector machines, or neural networks, will be trained on historical data from vendor partnerships and supply chain disruptions. These models can learn from patterns in the data and predict future risk events based on input features like vendor location, industry, historical performance, and external factors such as geopolitical risk or economic downturns (Franco, Lacerda & Stiller, 2022, Georgiadou, Mouzakitis & Askounis, 2021, Knowles, et al., 2015). Machine learning techniques will be particularly useful in scenario planning and risk prediction, allowing businesses to simulate potential risks under various scenarios and develop contingency plans accordingly. By leveraging these advanced techniques, the vendor risk assessment model will not only assess current risks but also forecast potential disruptions, enabling proactive risk management.

The final stage of the methodology involves validating and testing the developed vendor risk assessment model in real-world supply chain environments. Pilot testing will be conducted with a select group of companies that represent different sectors and supply chain complexities in the U.S. and Canada. These companies will implement the model within their operations, assessing its ability to identify and mitigate vendor risks effectively. The pilot testing phase will involve using the model to evaluate existing vendor relationships, monitor supply chain performance, and simulate potential risks to gauge the model's accuracy and effectiveness (Sabillon, et al., 2017, Shackelford, Russell & Haut, 2015). Feedback from participating companies will be crucial in refining the model, as it will provide insights into any limitations or gaps in the assessment process. For instance, companies may find that certain vendor attributes are more predictive of risk than others, or that the model's complexity makes it difficult to apply in certain supply chain contexts.

Iterative improvement will be a key feature of the testing phase. After the initial round of pilot testing, the model will be adjusted based on feedback and new data collected from the testing phase. This may involve tweaking the risk assessment criteria, refining the data analysis techniques, or integrating additional risk factors that were not previously considered. Feedback loops will ensure that the model evolves continuously to meet the dynamic nature of supply chain risks (Burke, et al., 2019, Demchak, et al., 2016, Kour, Karim & Thaduri, 2020). The iterative process of testing, feedback, and improvement will help ensure that the final model is both accurate and adaptable to the diverse needs of companies operating in the U.S. and Canadian markets.

Moreover, the feedback gathered during pilot testing will not only help refine the risk assessment model but also inform the broader implementation strategy for businesses seeking to adopt it. Companies that participate in the pilot testing phase will provide valuable insights into how the model can be incorporated into existing supply chain management systems, what training and support will be required for successful adoption, and any challenges that companies face when using the model in their operations (Aliyu, et al., 2020, Brown, 2018, Miron, 2015). By incorporating real-world feedback into the development process, the methodology ensures that the final model is both practical and effective in enhancing the security and resilience of supply chains in U.S. and Canadian markets.

In conclusion, the methodology for developing a vendor risk assessment model to secure supply chains in U.S. and Canadian markets integrates both qualitative and quantitative data collection methods, advanced data analysis techniques, and iterative validation processes. By leveraging insights from supply chain professionals, case studies, statistical modeling, and machine learning, the research will develop a robust, data-driven model that can help businesses identify, assess, and mitigate vendor-related risks (Miron & Muita, 2014). Through pilot testing and continuous feedback loops, the model will be refined to ensure that it meets the evolving needs of supply chain managers in both countries, providing them with the tools they need to secure their vendor relationships and enhance supply chain resilience.

4.1. Technological Integration in the Model

Technological integration plays a critical role in developing a comprehensive vendor risk assessment model for securing supply chains in U.S. and Canadian markets. By leveraging cutting-edge technologies such as blockchain, artificial intelligence (AI), and robust cybersecurity measures, the model can enhance its effectiveness, offering businesses advanced tools for risk identification, assessment, and mitigation. These technologies provide transparency, predictive insights, and security, which are essential for safeguarding the integrity of supply chains and ensuring compliance with evolving regulations and standards.

Blockchain technology can play a significant role in enhancing transparency and traceability in supply chains. Blockchain is a decentralized and immutable ledger system that records transactions across multiple computers in such a way that the records cannot be altered retroactively. In the context of vendor risk assessment, blockchain can be used to track the entire lifecycle of products and services across the supply chain. By creating an immutable and transparent

record of all transactions between vendors and stakeholders, blockchain allows for improved visibility into the flow of goods, financial transactions, and compliance with standards (Burns, 2019, Shackelford & Bohm, 2016, Stoddart, 2016). This transparency reduces the risk of fraud, non-compliance, and operational inefficiencies, as every party involved in the supply chain can view and verify the information in real-time. Blockchain also ensures that vendors are held accountable for their actions, as their records are accessible, preventing issues like false reporting or failure to meet agreed-upon standards. In addition, blockchain technology can provide an auditable trail of all actions, which is crucial in ensuring compliance with regulatory frameworks and responding to audits or investigations related to vendor performance.

Artificial Intelligence (AI) has the potential to revolutionize the way supply chain risks are assessed and managed. One of the key applications of AI in this context is predictive analytics, which leverages machine learning algorithms to forecast potential risks based on historical data, patterns, and trends. Predictive analytics can be used to assess the likelihood of specific risks occurring within a given vendor relationship or across a supply chain network. For example, by analyzing vendor performance data, AI algorithms can identify warning signs of financial instability, compliance violations, or operational disruptions before they happen. This allows companies to take proactive measures to address potential risks before they manifest, reducing the likelihood of costly disruptions and improving the resilience of the supply chain. Early warning systems, powered by AI, can alert supply chain managers to emerging risks and provide them with the necessary insights to act swiftly and make informed decisions. By incorporating AI-driven predictive models into the vendor risk assessment process, companies can ensure that they are prepared for potential disruptions, rather than reacting to them after they have already occurred.

Furthermore, AI can enhance the vendor selection process by analyzing large datasets to identify the best vendors based on a variety of factors, including financial health, compliance history, and past performance. AI can evaluate these factors at a speed and scale far beyond human capabilities, ensuring that businesses can make data-driven decisions when selecting or managing vendors. This ability to process vast amounts of data also supports more accurate and timely risk assessments, as AI can integrate and analyze data from diverse sources, including financial statements, regulatory filings, social media sentiment, and news articles. Additionally, AI can be used for continuous monitoring of vendor activities, ensuring that any deviations from expected performance are detected early and acted upon promptly.

Cybersecurity measures are another critical component of the vendor risk assessment model. In an increasingly interconnected world, ensuring secure data exchange between vendors and stakeholders is essential for protecting sensitive information and maintaining the integrity of the supply chain. Cybersecurity measures help mitigate the risks associated with data breaches, hacking, and cyberattacks, which can have devastating effects on supply chain operations. By integrating strong cybersecurity protocols into the vendor risk assessment process, businesses can ensure that the exchange of information between vendors, partners, and stakeholders is secure and protected from external threats.

The first step in integrating cybersecurity into the model is the establishment of secure communication channels between all parties involved in the supply chain. This can be achieved through the use of encryption technologies, which ensure that data exchanged between vendors and stakeholders is unreadable to unauthorized parties. Encryption provides a safeguard against cyberattacks, such as man-in-the-middle attacks, where malicious actors intercept and manipulate data during transmission (Gow, 2019, Pomerleau & Lowery, 2020). In addition to encryption, businesses should implement multi-factor authentication (MFA) to ensure that only authorized users can access sensitive supply chain data. MFA requires users to provide multiple forms of identification before gaining access, making it significantly more difficult for cybercriminals to gain unauthorized access to critical systems.

Another important aspect of cybersecurity in the vendor risk assessment model is the continuous monitoring of vendors' security practices. Vendors should be required to implement stringent cybersecurity measures, such as firewalls, intrusion detection systems (IDS), and regular vulnerability assessments. These measures help detect and prevent potential security breaches, ensuring that vendor systems are secure from cyberattacks. Additionally, vendors should be regularly audited for compliance with security standards and best practices, with any deficiencies addressed promptly (Rass, et al., 2020, Stellios, et al., 2018). By continuously monitoring vendor cybersecurity practices, businesses can identify potential weaknesses in the supply chain's security infrastructure and take corrective action before these weaknesses are exploited by malicious actors.

Moreover, businesses should implement a system of data classification and access control to ensure that sensitive information is only accessible to authorized personnel. This means that vendors must restrict access to confidential data, such as intellectual property, trade secrets, or customer information, and implement strict protocols for data sharing. Data classification systems can help organizations identify which information is most sensitive and ensure that

it is protected with the highest levels of security. For example, access to highly sensitive data could be restricted to a small group of trusted individuals, while less critical information could be more widely accessible.

The integration of these cybersecurity measures into the vendor risk assessment model will ensure that data exchanged between vendors and stakeholders remains secure, minimizing the risk of data breaches, intellectual property theft, and other cyber-related threats. By requiring vendors to adhere to robust cybersecurity standards, businesses can safeguard their supply chain from the increasing threat of cyberattacks and ensure that their operations remain secure and resilient.

In conclusion, the integration of blockchain, artificial intelligence, and cybersecurity measures into the vendor risk assessment model provides a comprehensive solution to securing supply chains in U.S. and Canadian markets. Blockchain enhances transparency and traceability, AI enables predictive analytics and early warning systems, and cybersecurity measures ensure secure data exchange between vendors and stakeholders (Cantelmi, Di Gravio & Patriarca, 2021, Carter & Sofio, 2017).. By incorporating these advanced technologies, businesses can proactively identify, assess, and mitigate vendor risks, enhancing the resilience and security of their supply chains. As supply chains continue to become more complex and interconnected, the role of technological integration will only grow, providing companies with the tools they need to navigate the challenges of an increasingly digital and globalized marketplace.

5. Results and Discussion

The development of a Vendor Risk Assessment Model to secure supply chains in the U.S. and Canadian markets has yielded valuable insights regarding its effectiveness, challenges, and potential for future research. The model's key objective is to create a data-driven, comprehensive framework that enables organizations to identify, assess, and mitigate risks within their supply chain networks. Through pilot testing and feedback from stakeholders, the model has shown potential in improving the resilience and security of supply chains, although challenges and limitations have been identified that require further exploration and refinement.

One of the key findings from the pilot testing of the proposed vendor risk assessment model is its effectiveness in providing a structured and data-driven approach to risk identification and evaluation. The pilot testing, conducted with a select group of companies across diverse industries, demonstrated that the model's risk identification process effectively captured a wide range of potential threats, including financial instability, cybersecurity vulnerabilities, and compliance issues (Bridge & Bradshaw, 2017, Papert & Pflaum, 2017). Stakeholders, including supply chain managers and procurement officers, reported that the model's segmentation of vendors based on criticality and risk levels enabled them to prioritize their risk mitigation efforts more effectively. This prioritization is critical for organizations operating in dynamic and highly competitive markets, where resource constraints often necessitate focusing on the most critical risks first.

Furthermore, the use of predictive analytics and machine learning techniques to assess and predict vendor-related risks has proven to be a valuable component of the model. The ability to forecast potential risks based on historical data and patterns has provided organizations with early warnings about emerging vulnerabilities, enabling them to take preventive measures before disruptions occur. Companies involved in the pilot testing also appreciated the use of AI-driven early warning systems, which helped them monitor vendor performance continuously and adjust their strategies accordingly. The combination of these advanced technologies allowed for a more proactive approach to risk management, which is essential in minimizing the negative impact of supply chain disruptions.

However, despite the positive results from pilot testing, several challenges and limitations have been identified during the implementation process. One of the primary barriers is the lack of standardization across supply chains, especially when dealing with multiple vendors from different regions and industries. Variations in data formats, reporting standards, and compliance requirements make it difficult to collect and analyze data consistently across the supply chain network. While the proposed model aims to address these discrepancies through the integration of diverse data sources, the lack of standardized data remains a significant hurdle (Chen, Zhang & Delaurentis, 2014, Urciuoli, et al., 2014). This challenge is particularly evident when working with small or mid-sized vendors who may lack the resources or infrastructure to implement the data-sharing protocols necessary for effective risk assessment. In these cases, ensuring data accuracy and consistency becomes increasingly difficult, which may compromise the reliability of the risk assessment process.

Another significant challenge lies in the scalability of the model. Although the model has shown promise in smaller-scale pilot tests, scaling it across large, complex supply chains with numerous vendors introduces several logistical and operational challenges. Larger supply chains often involve a vast number of vendors, each with its own set of risks and

unique characteristics. This complexity can overwhelm the model's capacity to effectively assess risks in real-time, especially in dynamic environments where risk factors can change rapidly (Gao, et al., 2020, Schlegel & Trent, 2014). As a result, organizations may struggle to apply the model universally across their entire supply chain, limiting its overall effectiveness. Furthermore, the reliance on machine learning and predictive analytics requires significant amounts of historical data, which may not always be available for every vendor, especially in cases where vendors are newly onboarded or operate in emerging markets.

Another barrier to the model's implementation is the cost associated with integrating advanced technologies such as blockchain, AI, and machine learning into existing supply chain management systems. Small and medium-sized enterprises (SMEs), in particular, may find it challenging to invest in the necessary infrastructure to support the model, limiting its adoption across different types of organizations. While larger corporations with more resources may be able to integrate these technologies with relative ease, smaller organizations may struggle to bear the initial costs, which could delay or prevent widespread adoption of the model.

Despite these challenges, there are several recommendations for overcoming the limitations of the proposed model and enhancing its overall effectiveness. One key recommendation is to focus on improving data standardization across supply chains. By collaborating with industry groups, regulatory bodies, and technology providers, companies can work toward creating standardized data formats and reporting requirements that make it easier to share and analyze data across vendor networks (Hobbs, 2020, Lawrence, et al., 2020). This would help ensure that the data used in risk assessments is accurate, consistent, and comparable, regardless of the size or location of the vendor. In addition, businesses could benefit from developing partnerships with data-sharing platforms and third-party providers who specialize in aggregating and analyzing supply chain data. These platforms can offer pre-built integrations with a wide range of vendors, making it easier for companies to gather and assess data without having to invest in complex data collection and management systems.

To address the scalability issue, future iterations of the model should focus on developing modular and customizable risk assessment tools that can be adapted to different supply chain contexts. A more flexible approach would allow businesses to tailor the model to their specific needs, taking into account the size, complexity, and geographical scope of their supply chain operations. This customization could include the ability to assess different types of risks based on the unique characteristics of individual vendors, such as financial stability, cybersecurity preparedness, or geopolitical risks. By offering a more adaptable framework, the model would be better equipped to handle the diverse range of challenges that arise in larger, more complex supply chains.

Another key recommendation is to improve the accessibility of advanced technologies, such as AI and blockchain, for smaller organizations. This could be achieved by providing more affordable and user-friendly solutions, including cloud-based platforms and software-as-a-service (SaaS) offerings that allow businesses to access these technologies without the need for large upfront investments (Kumar, Himes & P. Kritzer, 2014, Monaghan & Walby, 2017). Additionally, industry partnerships could be leveraged to create shared infrastructure for risk assessment, reducing the cost burden on individual organizations while increasing the overall efficiency and effectiveness of the model.

Finally, future research should explore the long-term impact of the vendor risk assessment model on supply chain resilience and security. While the pilot tests have demonstrated the model's potential to enhance risk management, further studies are needed to assess its effectiveness in the long term, particularly in the context of large, dynamic supply chains. Researchers should also investigate the potential for integrating the model with other risk management frameworks, such as business continuity planning and disaster recovery, to create a more comprehensive approach to supply chain security.

In conclusion, the development of a Vendor Risk Assessment Model to secure supply chains in the U.S. and Canadian markets has shown promising results in improving risk identification, assessment, and mitigation. While challenges related to data standardization, scalability, and technology integration remain, there are clear opportunities to refine the model and overcome these barriers (Boyson, 2014, Linkov, et al., 2014). By focusing on data standardization, scalability, and accessibility, businesses can unlock the full potential of the model and improve the resilience and security of their supply chains. Future research will be essential in refining the model and exploring its long-term impact on supply chain operations.

6. Conclusion

In conclusion, the development of a comprehensive Vendor Risk Assessment Model to secure supply chains in the U.S. and Canadian markets represents a significant advancement in the way organizations approach risk management. This

model offers a systematic and data-driven framework to identify, assess, and mitigate risks within supply chains, addressing critical vulnerabilities such as cybersecurity, financial stability, and regulatory compliance. By incorporating advanced technologies like artificial intelligence, machine learning, and blockchain, the model enables businesses to not only monitor risks in real-time but also predict potential disruptions before they escalate, allowing for proactive risk management strategies.

The implementation of this model promises long-term benefits for businesses operating in the U.S. and Canadian markets. As supply chains become more interconnected and globalized, the ability to efficiently and accurately assess vendor risks is crucial to maintaining operational continuity and resilience. Organizations can leverage this model to enhance decision-making, prioritize resources, and ensure that their vendor relationships align with broader business objectives, regulatory requirements, and security standards. Furthermore, the model's focus on continuous monitoring and evaluation ensures that businesses can adapt to changing market conditions and evolving risks, further strengthening the overall resilience of their supply chains.

This model has the potential to drive significant improvements in supply chain management practices. It empowers businesses to take a more proactive and informed approach to risk assessment, moving away from reactive strategies that often leave organizations vulnerable to disruptions. By emphasizing the importance of collaboration between vendors, stakeholders, and regulatory bodies, the model fosters a culture of transparency and accountability within supply chains, promoting greater trust and long-term partnerships. Additionally, the use of advanced analytics and predictive technologies contributes to a more agile and responsive supply chain, enabling businesses to quickly adapt to unforeseen challenges while safeguarding their operations.

As businesses in both the U.S. and Canada continue to navigate the complexities of global supply chains, the adoption of the proposed Vendor Risk Assessment Model will be a critical step in enhancing supply chain security and resilience. While challenges remain, particularly around data standardization and scalability, the model provides a valuable foundation for improving risk management practices. Future research and continuous refinement of the model will ensure that it remains a robust and adaptable solution for businesses seeking to secure their supply chains against emerging risks and disruptions.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Reference

[1] Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245-272.

[2] Aboelfotoh, S. F., & Hikal, N. A. (2019). A review of cyber-security measuring and assessment methods for modern enterprises. *JOIV: International Journal on Informatics Visualization*, *3*(2), 157-176.

[3] Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), 539-548.

[4] Al-Hassan, A., Burfisher, M. E., Chow, M. J. T., Ding, D., Di Vittorio, F., Kovtun, D., ... & Youssef, K. (2020). *Is the whole greater than the sum of its parts? Strengthening caribbean regional integration*. International Monetary Fund.

[5] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660.

[6] Amin, Z. (2019). A practical road map for assessing cyber risk. *Journal of Risk Research*, *22*(1), 32-43.

[7] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74.

[8] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.

[9] Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847-861.

[10] Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1), tyab024.

[11] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[12] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[13] Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: driving corporate behavior in the United States and Europe*. MIT Press.

[14] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

[15] Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. *Mitre Corp, Mclean*, 2021-11.

[16] Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342-353.

[17] Bridge, G., & Bradshaw, M. (2017). Making a global gas market: Territoriality and production networks in liquefied natural gas. *Economic Geography*, *93*(3), 215-240.

[18] Brown, R. D. (2018). Towards a Qatar cybersecurity capability maturity model with a legislative framework. *International Review of Law*.

[19] Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

[20] Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019, January). Cybersecurity indexes for eHealth. In *Proceedings of the australasian computer science week multiconference* (pp. 1-8).

[21] Burns, M. G. (2019). *Managing energy security: an all hazards approach to critical infrastructure*. Routledge.

[22] Callaghan, R. (2018). *The impact of protectionism on the completion and duration of cross-border acquisitions* (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington).

[23] Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, *41*(3), 341-376.

[24] Carter, W. A., & Sofio, D. G. (2017). Cybersecurity legislation and critical infrastructure vulnerabilities. *Foundations of Homeland Security: Law and Policy*, 233-249.

[25] Celeste, E., & Fabbrini, F. (2020). Competing jurisdictions: Data privacy across the borders. *Data Privacy and Trust in Cloud Computing*, 43-58.

[26] Chen, C., Zhang, J., & Delaurentis, T. (2014). Quality control in food supply chain management: An analytical model and case study of the adulterated milk incident in China. *International Journal of Production Economics*, *152*, 188-199.

[27] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27.

[28] Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin.

[29] Clemente, J. F. (2018). *Cyber security for critical energy infrastructure* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[30] Dalal, A., Abdul, S., & Mahjabeen, F. (2016). Leveraging Artificial Intelligence for Cyber Threat Intelligence: Perspectives from the US, Canada, and Japan. *Revista de Inteligencia Artificial en Medicina*, *7*(1), 18-28.

[31] Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2016). Cyber readiness at a glance. *Potomac Institute for Policy Studies*, 1-44.

[32] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.

[33] Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

[34] Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., ... & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International journal of information management*, *55*, 102211.

[35] Ele, S. I., & Oko, J. O. (2016). Governance, risk and compliance (Grc): a. *Journal of Integrative Humanism*, *6*(1), 161.

[36] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Application of deep and machine learning techniques for multi-label classification performance on psychotic disorder diseases. Informatics in Medicine Unlocked, 23, 100545.

[37] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Informatics in Medicine Unlocked.

[38] Fefer, R. F. (2019). Data flows, online privacy, and trade policy. *Congressional Research Service*.

[39] Feng, Y. (2019). The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, *27*(1), 62-82.

[40] Flores, M. C. (2019). Challenges for Macroprudential Policy in the Euro Area: Cross-Border Spillovers and Governance Issues.

[41] Gao, Q., Guo, S., Liu, X., Manogaran, G., Chilamkurti, N., & Kadry, S. (2020). Simulation analysis of supply chain risk management system based on IoT information platform. *Enterprise Information Systems*, *14*(9-10), 1354-1378.

[42] Garrett, G. A. (2018). *Cybersecurity in the Digital Age: Tools, Techniques, & Best Practices*. Aspen Publishers.

[43] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267.

[44] Govindji, S., Peko, G., & Sundaram, D. (2018). A context adaptive framework for IT governance, risk, compliance and security. In *Context-Aware Systems and Applications, and Nature of Computation and Communication: 6th International Conference, ICCASA 2017, and 3rd International Conference, ICTCC 2017, Tam Ky, Vietnam, November 23-24, 2017, Proceedings 6* (pp. 14-24). Springer International Publishing.

[45] Gow, G. A. (2019). *Policymaking for critical infrastructure: a case study on strategic interventions in public safety telecommunications*. Routledge.

[46] Haugh, T. (2018). Harmonizing governance, risk management, and compliance through the paradigm of behavioral ethics risk. *U. Pa. J. Bus. L.*, *21*, 873.

[47] Hobbs, J. E. (2020). Food supply chains during the COVID-19 pandemic. *Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie*, *68*(2), 171-176.

[48] Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2021.2.2.0059

[49] Igo, S. E. (2020). *The known citizen: A history of privacy in modern America*. Harvard University Press.

[50] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews, 2*(1), 074–086. https://doi.org/10.30574/msarr.2021.2.1.0032

[51] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. *International Journal of Engineering Research and Applications*, *7*(6), 31-38.

[52] Kaplan, R. S., & Mikes, A. (2016). Risk management—The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8-18.

[53] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80.

[54] Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways–A maturity model. *Proceedings of the institution of mechanical engineers, Part F: Journal of Rail and Rapid Transit*, *234*(10), 1129-1148.

[55] Kovacevic, A., & Nikolic, D. (2015). Cyber attacks on critical infrastructure: Review and challenges. *Handbook of research on digital crime, cyberspace security, and information assurance*, 1-18.

[56] Kumar, S., J. Himes, K., & P. Kritzer, C. (2014). Risk assessment and operational approaches to managing risk in global supply chains. *Journal of Manufacturing Technology Management*, *25*(6), 873-890.

[57] Laidlaw, E. (2021). Privacy and cybersecurity in digital trade: The challenge of cross border data flows. *Available at SSRN 3790936*.

[58] Lawrence, J. M., Hossain, N. U. I., Jaradat, R., & Hamilton, M. (2020). Leveraging a Bayesian network approach to model and analyze supplier vulnerability to severe weather risk: A case study of the US pharmaceutical supply chain following Hurricane Maria. *International Journal of Disaster Risk Reduction*, *49*, 101607.

[59] Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature climate change*, *4*(6), 407-409.

[60] Malhotra, Y. (2018). Bridging networks, systems and controls frameworks for cybersecurity curriculums and standards development. *Journal of Operational Risk*, *13*(1).

[61] Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

[62] McCubbrey, D. S. (2020). *Cybersecurity Penetration Assessments in the Context of a Global Cybersecurity Skills Gap* (Doctoral dissertation, Capella University).

[63] Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019, November). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In *2019 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-13). IEEE.

[64] Minssen, T., Seitz, C., Aboy, M., & Compagnucci, M. C. (2020). The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR: What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector?. *EPLR*, *4*, 34.

[65] Miron, W. R. (2015). *Adoption of Cybersecurity Capability Maturity Models in Municipal Governments* (Doctoral dissertation, Carleton University).

[66] Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review*, *4*(10), 33.

[67] Monaghan, J., & Walby, K. (2017). Surveillance of environmental movements in Canada: Critical infrastructure protection and the petro-security apparatus. *Contemporary Justice Review*, *20*(1), 51-70.

[68] Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

[69] Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017, September). Managing information security risk using integrated governance risk and compliance. In *2017 International Conference on Computer and Applications (ICCA)* (pp. 56-66). IEEE.

[70] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.2.0086

[71] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.1.0076

[72] Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*, 1251-1263.

[73] Papert, M., & Pflaum, A. (2017). Development of an ecosystem model for the realization of internet of things (IoT) services in supply chain management. *Electronic Markets*, *27*(2), 175-189.

[74] Park, S. K. (2015). Special economic zones and the perpetual pluralism of global trade and labor migration. *Geo. J. Int'l L.*, *47*, 1379.

[75] Pomerleau, P. L. (2019). Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection. *Order*, (27540959).

[76] Pomerleau, P. L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. In *A Private and Public Partnership Approach to Critical Infrastructure Protection*. Springer.

[77] Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). *Cyber-security in critical infrastructures* (Vol. 297). Springer International Publishing.

[78] Recor, J., & Xu, H. (2016). GRC technology introduction. In *Commercial Banking Risk Management: Regulation in the Wake of the Financial Crisis* (pp. 305-331). New York: Palgrave Macmillan US.

[79] Robinson, R. (2020). *Exploring strategies to ensure United States critical infrastructure of the water sector maintains proper cybersecurity* (Doctoral dissertation, Colorado Technical University).

[80] Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

[81] Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.

[82] Sanaei, M. R., Movahedi Sobhani, F., & Rajabzadeh, A. (2016). Toward An E-business Governance Model Based on GRC Concept. *The International Journal of Humanities*, *23*(3), 71-85.

[83] Schlegel, G. L., & Trent, R. J. (2014). *Supply chain risk management: An emerging discipline*. Crc Press.

[84] Shackelford, S. J., & Bohm, Z. (2016). Securing North American critical infrastructure: A comparative case study in cybersecurity regulation. *Can.-USLJ*, *40*, 61.

[85] Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.

[86] Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ*, *16*, 217.

[87] Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129-136.

[88] Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, 14-30.

[89] Sikdar, P. (2021). *Strong Security Governance Through Integration and Automation: A Practical Guide to Building an Integrated GRC Framework for Your Organization*. Auerbach Publications.

[90] Smart, C. (2017). Regulating the Data that Drive 21st-Century Economic Growth.

[91] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495.

[92] Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, *92*(5), 1079-1105.

[93] Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *computer law & security review*, *35*(4), 380-397.

[94] Tehrani, P. M., Sabaruddin, J. S. B. H., & Ramanathan, D. A. (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. *Computer law & security review*, *34*(3), 582-594.

[95] Tian, G. Y. (2016). Current issues of cross-border personal data protection in the context of cloud computing and trans-Pacific partnership agreement: join or withdraw. *Wis. Int'l LJ*, *34*, 367.

[96] Trew, S. J. (2021). *International Regulatory Cooperation and the Making of "Good" Regulators: A Case Study of the Canada–US Regulatory Cooperation Council* (Doctoral dissertation, Carleton University).

[97] Urciuoli, L., Mohanty, S., Hintsa, J., & Gerine Boekesteijn, E. (2014). The resilience of energy supply chains: a multiple case study approach on oil and gas supply chains to Europe. *Supply Chain Management: An International Journal*, *19*(1), 46-63.

[98] Ustundag, A., Cevikcan, E., Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. *Industry 4.0: managing the digital transformation*, 267-284.

[99] Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, *29*, 485.

[100] Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal*, *56*(2), 287-344.

[101] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53.

[102] Yeung, M. T., Kerr, W. A., Coomber, B., Lantz, M., & McConnell, A. (2017). *Declining international cooperation on pesticide regulation: frittering away food security*. Springer.

[103] Zaccari, L. (2016). Addressing a successful implementation of a governance, risk and compliance management system.