PLOMS Journal of Artificial Intelligence (PLOMS AI)

PLOMS AI

Survey

Supply Chain Security in Information Systems: A Survey

Manar Said Al-Kindi[1], Hoor Alkalbani[1], Nasra Subeih Al-Hinai[1], and Rabie A. Ramadan [2]

[1]College of Economics, Management, and Information Systems, Nizwa, Oman
[2]AI Applications Chair, University of Nizwa, Nizwa PC616, Sultanate of Oman

Abstract: Supply chain security in information systems is a vital topic in the digital age, as it faces many challenges related to protecting data and information transmitted across supply networks. This economic study aims to analyze the potential risks that information systems may face in the context of the supply chain, in addition to the prevention strategies that can be adopted to reduce those risks. It also highlights the relationship between securing the supply chain and achieving economic efficiency in companies, which enhances the stability of business operations and increases their effectiveness. Supply chain security in information systems is also a topic of utmost importance in light of the rapid technological transformations that the world is witnessing today. Information systems contribute to facilitating business operations and achieving efficiency, but the exposure of these systems to security risks such as hacking and digital threats may significantly affect the stability and reputation of companies. This economic study aims to analyze the challenges facing information systems in the supply chain, identify their economic impacts on institutional performance, and review the strategies that companies can adopt to enhance security and data protection, and achieve a balance between cost and security to maintain business continuity.

Keywords: supply chain security; information systems; cybersecurity; risk management; digital threats; data protection

I. Introduction

Supply chain security in information systems is a vital topic in the digital age, as it faces many challenges related to protecting data and information transmitted across supply networks. This economic study aims to analyze the potential risks that information systems may face in the context of the supply chain, in addition to the prevention strategies that can be adopted to reduce those risks. It also highlights the relationship between securing the supply chain and achieving economic efficiency in companies, which enhances the stability of business operations and increases their effectiveness. Supply chain security in information systems is also a topic of utmost importance in light of the rapid technological transformations that the world is witnessing today. Information systems contribute to facilitating business operations and achieving efficiency, but the exposure of these systems to security risks such as hacking and digital threats may significantly affect the stability and reputation of companies. This economic study aims to analyze the challenges facing information systems in the supply chain, identify their economic impacts on institutional performance, and review the strategies that companies can adopt to enhance security and data protection, and achieve a balance between cost and security to maintain business continuity.

I.1 Definition

Supply chain security focuses on managing risks associated with external suppliers, vendors, logistics, and transportation. It involves identifying, analyzing, and mitigating risks related to both physical security and cybersecurity for software and devices. While there are no universal guidelines for supply chain security, a comprehensive strategy combines risk management principles, cyber defense, and adherence to government protocols. Supply chain security safeguards both physical integrity and defends against cyber threats. Physical risks include theft, sabotage, and terrorism, which can be mitigated through tracking and regulatory checks. Cybersecurity risks, such as malware, piracy, and unauthorized access, have become more prominent, exposing vulnerabilities in IT and software systems within the supply chain.

II. Supply Chain Applications

Supply chain applications are fundamental to the seamless operation of modern businesses. These systems facilitate the coordination of goods, services, data, and financial resources across complex networks. Examples include inventory management systems that track stock levels in real time, logistics platforms that optimize delivery routes, and order processing tools that ensure accurate fulfillment. To meet the growing demands for efficiency and security, advanced technologies are being integrated into these applications.

Blockchain technology provides an immutable and transparent ledger, which enhances traceability and accountability by recording every transaction or transfer within the supply chain. AI-powered analytics tools allow businesses to monitor operations in real-time, identify inefficiencies, and predict potential disruptions. IoT devices, such as smart sensors and connected trackers, enable continuous monitoring of physical assets, ensuring better control over inventory and logistics.

Furthermore, cybersecurity measures like encryption, firewalls, and intrusion detection systems protect sensitive data from unauthorized access or manipulation. These applications are particularly valuable in globalized supply chains, which involve multiple stakeholders across different regions. They address the complexities of diverse regulatory standards, cultural practices, and logistical challenges, ensuring that operations remain resilient and efficient even in the face of external pressures.

II.1 Security Issues

Despite advancements in technology, supply chains face numerous and increasingly sophisticated security threats. Software vulnerabilities remain one of the most critical issues, as attackers often exploit outdated or poorly secured systems, open-source components, or malicious updates to infiltrate supply chains. This allows them to introduce malware that spreads across networks, causing widespread disruption. State-sponsored threats are also on the rise, with foreign actors targeting supply chains to steal intellectual property, disrupt essential services, or destabilize economic systems. These attacks are particularly concerning for industries tied to national security or critical infrastructure.

Data breaches are another significant concern, as hackers often target smaller vendors with weaker defenses to gain access to larger organizations. Once inside, attackers can exfiltrate sensitive personal, financial, or operational data. Ransomware attacks, where systems are encrypted and held hostage until a ransom is paid, are becoming increasingly prevalent and can bring entire supply chains to a halt. Insider threats, whether malicious or accidental, pose additional risks, as employees or contractors may leak sensitive information or inadvertently compromise security protocols. Physical threats, such as the theft of goods or data during transit or storage, remain a longstanding challenge.

Globalization exacerbates these vulnerabilities, as international supply chains involve stakeholders from different countries with varying security standards, regulatory requirements, and practices. Natural disasters, political instability, and geopolitical conflicts further compound the risks by disrupting supply chain operations and exposing weaknesses in business continuity plans.

II.2 Mitigation Methods

The primary goal of supply chain security is to protect companies from attacks, which often involve malware disguised as software that spreads through various channels to exploit vulnerabilities. Addressing these challenges requires a comprehensive and proactive approach to supply chain security. Regular inspections and network assessments are critical to identifying vulnerabilities before they are exploited. These assessments ensure that potential vulnerabilities, such as outdated software or improperly configured systems, are addressed promptly, and that vendor and partner security measures are integrated using specialized threat intelligence and response frameworks.

Automated security checks should be integrated throughout the supply chain lifecycle, from software design and development to the distribution of goods and services. Vendor and partner security measures should be strengthened through comprehensive inspections, strict compliance requirements, and ongoing monitoring. Requiring vendors to provide software bills of materials improves transparency by detailing software components and identifying potential risks associated with open source or third-party software.

Regular analysis of operations support systems is essential to detect vulnerabilities, such as SQL injection attacks or unauthorized access attempts, and implement corrective measures. When systems are compromised, immediate updates, isolation, or replacement are essential to contain the damage and prevent further exploitation. Multi-factor authentication (MFA) should be implemented across all critical systems to enhance access control and protect against credential-based attacks.

Ongoing employee training and awareness programs are vital to reduce human error, which remains a leading cause of security breaches. Employees should be educated on the latest threats, best practices, and their roles in maintaining supply chain security. Additionally, advanced technologies such as blockchain, artificial intelligence, and the Internet of Things can be leveraged to enhance security measures. Blockchain ensures secure and transparent record keeping, AI enables predictive threat detection and rapid response, and the Internet of Things provides real-time monitoring of assets and operations. Together, these tools create a more robust and resilient supply chain framework.

III. Supply Chain Security: An Overview and Research Agenda

The importance of supply chain security (SCS) as part of an organization's broader security strategy has been recognized through comprehensive research analysis.

III.1 Study Objective

The study aims to develop a taxonomy of supply chain security based on current research, which can help academics and practitioners understand the field. The taxonomy is also designed to identify gaps in the current literature, helping to define a research agenda that can guide future studies on supply chain security.

III.2 Design

The researchers conducted a comprehensive literature review, examining academic articles, white papers, and industry journals. From this, they categorized the findings according to different approaches to supply chain security and discussed their practical implications. The taxonomy also helped identify areas that have not been adequately explored and need further empirical research.

III.3 Key Findings

The review identified that SCS remains a relatively unexplored area of academic research, with much of the existing literature being normative and lacking primary data. The researchers categorized the existing literature into four main approaches:

Intra-organizational: Focusing on internal security measures within an organization.

Inter-organizational: Focusing on collaboration and security across multiple organizations in the supply chain.

Mixed intra-organizational and inter-organizational: A hybrid approach that combines internal and external perspectives of SCS.

Ignored: Areas where SCS has not been considered or integrated into research.

The researchers also propose an agenda for future research, with a particular focus on empirical primary studies that can add real-world data to support current theoretical models and practices.

III.4 Research Limitations

The literature review relies on secondary data, meaning that the findings are based on existing research rather than on new and original empirical studies. The study calls for future research to focus on filling the identified gaps and emphasizes the need for empirical data to validate the theoretical models discussed.

III.5 Implications

For academics and practitioners, the classification and research agenda provides valuable insight into the current state of SCS research and provides a clear path for future studies. By addressing the identified gaps, research can lead to more informed practices and policies in supply chain security risk management.

IV. Financial Losses in the Supply Chain

The financial and reputational losses are key risks that companies face, making them crucial objectives to address in supply chain security studies. Several factors contribute to these losses, including:

Firstly, delivery delays can lead to both financial losses and damage to a company's reputation. Delayed delivery of goods or products results in lost customers and potential penalties. This also harms the company's reputation, leading to decreased customer trust.

Secondly, theft and fraud are significant risks. Goods can be stolen during transportation or while stored in unsecured warehouses, and manipulation of information is also a form of financial fraud. This can lead to a loss of trust from partners and customers. Furthermore, dealing with unreliable suppliers-those with poor reputations or who fail to meet commitments-can result in the delivery of low-quality products, further harming the company's reputation.

Lastly, non-compliance with regulatory standards can lead to fines and legal consequences, incurring financial losses and damaging the company's image.

IV.1 Prevention Measures

To prevent these losses, strict security measures should be implemented, such as:

First, securing transportation by installing GPS tracking systems to monitor goods during transit, and using secure trucks and storage facilities.

Second, cybersecurity measures such as encryption systems should be adopted to protect data during transmission, along with regular vulnerability testing. Third, effective

supplier management involves verifying the reputation of each supplier before contracting, through performance reviews and evaluations, and establishing clear contracts that ensure quality and timely delivery.

Fourth, implementing compliance and audit programs, such as ISO 28000 (Supply Chain Security) and C-TPAT (Customs-Trade Partnership Against Terrorism), along with regular audits to ensure adherence to local and international regulations.

The benefits of preventing financial and reputational losses are numerous. These include increased customer loyalty, as satisfied customers will support and recommend the company; strengthened relationships with partners, ensuring that all suppliers and stakeholders contribute to the stability of operations and reduce risks; and maintaining market competitiveness, as a strong reputation attracts new customers and helps sustain market share.

V. Cyber Attacks in the Supply Chain

Supply chain attacks occur through the hacking of one of the suppliers or the entities responsible for it, and this attack is considered one of the attacks that occur in the modern era. There are several examples of these attacks, including the SolarWinds attack, which occurred in 2020, where the attacker was able to introduce some malware into one of the programs used by major companies. Also, the Kaseya attack, which occurred in 2021, was intended to sabotage the IT infrastructure and caused great damage to companies.

On the other hand, there are several effects that fall under these attacks, including: recording personal and sensitive data, which includes all financial losses, as well as damaging the reputation, as these fall under the control of the trust of the organization, and the disruption of business operations, so when the attack occurs, operations stop working properly due to the viruses or the malicious software that affected them.

Every problem that occurs must have a solution, and the problem of cyber attacks has several solutions that protect us from it, which are: ensuring that software is updated continuously, awareness and informing employees about these attacks that they encounter, and training employees to recognize the type of attacks and what methods they will use to reduce the occurrence of these attacks, and finally encryption because it is the ideal solution to protect sensitive and personal data.

VI. Supply Chain Examples

Supply chains represent the backbone of the modern economy. There are many different examples of supply chains that are widespread in our current era across several different sectors:

VI.1 Technology Sector

In the technology sector, the supply chain represents a complex model. For Apple, the journey begins with mining raw materials, such as lithium used in smartphone batteries. These materials are shipped to specialized factories to manufacture processor chips and other components. These parts are then transported to assembly plants, where iPhones are manufactured, which are then distributed to sales centers around the world. Thanks to the high efficiency in supply chain management, Apple ensures that its products are provided with reliable quality and in record time.

VI.2 Food Industry

In the food industry, the supply chain shows how small farms can be the beginning of a long and complex journey. For example, bread production begins with farms that grow wheat, where it is collected and processed in specialized mills to turn it into flour. The flour is then transported to bread factories that turn it into a final product ready for distribution. The loaves are packaged in special bags, distributed via precise transportation networks to local or global stores, and finally to consumers. Nestlé, for example, offers an integrated supply chain management model that starts from farms and reaches store shelves around the world.

VI.3 Fashion Industry

In the fashion industry, the speed of response to market changes is a crucial factor, and this is clearly demonstrated in Zara's supply chain. The process begins with designing clothes according to the latest trends, then the factory produces the clothes using high-quality raw materials. Once production is complete, the pieces are transported to Zara stores around the world and displayed on shelves within a few weeks of their design, giving the company a huge competitive advantage.

VI.4 Automotive Sector

The automotive sector is another great example of how to manage the supply chain. In car factories, the process starts from extracting metals such as iron and aluminum to make the bodies, through to producing engines and tires, and ending with the complete assembly of the car. The cars are then shipped via global transportation networks to authorized dealers in different countries. Toyota, for example, manages a global supply chain with a combination of precision and efficiency, making it a role model in the industry.

The supply chain plays a critical role in the success of any company. By managing it effectively, costs can be reduced, quality can be increased, and deliveries can be acceler-

ated. Technology has also contributed significantly to improving the efficiency of supply chains, using technologies such as artificial intelligence and big data to forecast demand.

VII. Distributed Supply Chain Security Management

Supply chains present performance bottlenecks that contribute to higher costs, degraded product quality, and impacted productivity. Examples of these bottlenecks include bullwhip effects, new product lines, high inventory, and restrictive data flows. These bottlenecks can force manufacturers to source more raw materials and increase production significantly. Restrictive data flows in complex global supply chain networks also slow down the movement of goods and services in general.

The use of distributed ledger technologies in supply chain management demonstrates the potential to reduce these bottlenecks through transparency, decentralization, and data governance improvements. These technologies promise to enhance the reliability of entities within supply chains, ensure the accuracy of data-driven processes, and enable current supply chain management processes to move from a linear to a fully circular economy.

VII.1 Improving Information Security

The core security objectives (including confidentiality, integrity, availability, and accountability, CIAA) are analyzed. In turn, system security vulnerabilities are identified. A stochastic model is presented using measurable values to describe the security of an information system for supply chain management.

Information security is an essential and integral part of the supply chain network. Each chain or engine requires a different level of security depending on the services it contributes to the overall supply chain management system. Different probability weights are assigned to the four CIAA security objectives depending on the mission of the supply chain management engine.

A semi-Markov chain model is used to describe the probabilistic nature of the different security levels of each engine in the system. A comparison of the steady-state security of a multi-engine model with different levels of attack is made, and the results are analyzed. Enhanced supply chain security can be achieved by identifying the impacts of attacks on the organization's security objectives. Using this model helps identify vulnerabilities in the security of the supply chain system and provides hints on how to strengthen them.

VIII. The Role of External Development in Shaping Modern Supply Chain

The supply chain is not a standalone system that functions without external influences. Rather, it is a dynamic ecosystem that is continuously changing and greatly impacted by outside events. The term "external development" describes the range of factors that have a major influence on the effectiveness and performance of supply chains, including globalization, technical breakthroughs, political and economic shifts, and international crises. External development is essential to enhancing the adaptability, transparency, and general efficacy of supply chain operations in the rapidly evolving world of today.

Modern technology has played a major role in the development of supply chains. Supply chain management has been completely transformed by innovations like blockchain, the Internet of Things, and artificial intelligence (AI). Real-time tracking, demand forecasting, and increased supplier-company transparency are made possible by these technologies. Businesses may ensure operational efficiency and minimize delays and losses by using IoT devices to monitor shipments while they are in transit. AI-powered predictive analytics assists businesses in anticipating changes in demand, which helps them optimize inventory control and production schedules.

However, blockchain has brought a new degree of transparency and trust, guaranteeing safe and unchangeable transaction records across the supply chain. By creating new markets and enabling companies to acquire goods and materials from around the globe, globalization has also changed the structure of supply chains. Now that suppliers are more affordable and of greater quality, businesses can reach them, greatly increasing profitability.

For example, in order to lower production costs, many international firms rely on manufacturing in nations like China and India. Supply chains are now more susceptible to worldwide crises and interruptions as a result of the complications brought about by globalization, such as reliance on international logistics and transportation.

Supply networks are influenced equally by political and economic considerations. The seamless flow of goods across borders is made possible by government policies that support trade, such as reducing tariffs, enhancing transportation infrastructure, and establishing free trade agreements. In contrast, supply networks may be disrupted and costs raised by trade wars, economic sanctions, or modifications to regulatory regimes. For example, limiting the export of essential raw materials might impact international markets and cause industrial bottlenecks.

The efficiency of the supply chain has been further improved by developments in logistics and transportation. Shipping procedures have been made more efficient by innovations like drone deliveries, driverless cars, and advanced transportation management systems (TMS). These advancements enable businesses to cut expenses and expedite delivery.

Global disasters like the COVID-19 pandemic have highlighted supply chain weaknesses, forcing companies to reconsider their approaches. Significant flaws including an excessive reliance on a single source and a lack of backup preparations for unforeseen disruptions were made clear by the pandemic. To improve resilience, several businesses have responded by diversifying their supply base, implementing digital technologies for remote monitoring, and creating strategic inventory reserves.

Another important area of concern in supply chains' external development is sustainability. Businesses are integrating eco-friendly practices into their supply chains as a result of rising consumer awareness of environmental issues and regulatory pressure. This entails using sustainable materials, embracing renewable energy sources, and lowering carbon footprints. Businesses that prioritize recycled materials and ecologically friendly production techniques, such as Patagonia, are prime examples of this change.

Changes in consumer behavior and culture have also fueled supply networks' development. The increasing need for customized goods and expedited delivery has compelled businesses to reconsider their operational plans. Just-in-time manufacturing, regional distribution hubs, and on-demand production methods have all been adopted as a result. These adjustments enhance the supply chain's overall responsiveness and agility while also meeting customer expectations.

Furthermore, new technologies like machine learning and quantum computing, along with geopolitical trends, promise to dramatically transform supply chains in the near future. For example, quantum computing may instantly optimize intricate logistical networks, and sophisticated artificial intelligence could forecast market upheavals with previously unheard-of precision. The effectiveness of global supply networks will probably be redefined by these advancements when combined with automation, becoming more flexible.

Finally, for supply chains, external development presents both a problem and an opportunity for innovation and expansion. Technology, globalization, sustainability, and economic change all interact to produce a dynamic environment that forces supply chains to change all the time. Companies that adapt to these outside shifts are better equipped to handle ambiguities, cut expenses, and provide their clients with greater value. Supply chains will continue to be at the forefront of international trade as the world develops, adjusting to new conditions and propelling economic growth.

IX. The Role of Governments and Policies in the Supply Chain

At the local and global levels, governments and their policies are crucial in forming and guiding the supply chain. To achieve efficiency and sustainability, the supply chain needs a stable and forward-thinking regulatory environment because it is a complex system

influenced by many different elements. Beyond only passing legislation, governments also have a responsibility to guide investments, improve infrastructure, and foster a climate that is conducive to business and enables firms to successfully balance supply and demand.

In the supply chain, controlling cross-border trade is one of the main responsibilities of governments. The goal of trade agreements, including free trade agreements, is to lower tariffs and non-tariff trade obstacles that impede international trade. These pacts assist save expenses, boost productivity, and motivate businesses to grow their worldwide supply chains. By facilitating imports and exports, for instance, government regulations have allowed numerous businesses to lower production costs, which has allowed them to provide consumers competitively priced goods.

Government control over transportation and logistics infrastructure is another crucial element. Airports, ports, and highways make up the supply chain's core. Governments that make investments in upgrading and developing their infrastructure greatly help to cut down on travel expenses. Another tool used by the government to affect the supply chain is taxation. The degree to which businesses compete in international marketplaces can be influenced by import and export taxes. High taxes on imported raw materials, for instance, can raise operating expenses for businesses and make it more difficult for them to provide reasonably priced goods. Conversely, advantageous tax laws can stimulate local industries and investment, resulting in a prosperous and long-lasting business climate.

Global emergencies like the COVID-19 epidemic have brought attention to how important governments are in assisting the supply chain. In the face of travel restrictions and lockdowns, governments had to act quickly to guarantee the steady supply of necessities like food and medication. Certain countries made cross-border transit easier by streamlining customs processes and lifting short-term prohibitions that would have impeded the flow of products. In order to maintain supply chains in the face of extraordinary difficulties, they simultaneously offered impacted businesses financial and logistical support.

With the growing reliance on digital technology, cybersecurity has also become a crucial component of supply chain-related government laws. Governments are currently drafting laws to safeguard private information and supply chain data. Some nations offer businesses technical assistance and security tactics to reduce risks and safeguard their digital infrastructure in light of the increase in cyberattacks that target commercial networks.

Another area where governments have a big impact on supply chains is sustainability. Environmental policies are becoming a key emphasis due to the growing concern about climate change on a worldwide scale. Strict regulations are currently being enforced by governments to lower carbon emissions and promote the use of recyclable materials and renewable energy sources. Businesses that participate in eco-friendly supply chains gain

from government assistance, including tax breaks and financial incentives, which raises their level of market competitiveness.

Additionally, governments invest and fund the growth of supply chain-dependent enterprises. For example, providing small and medium-sized businesses with grants or low-interest loans might support the development of regional supply chains. Governments simultaneously start programs to educate and prepare workers to meet the evolving demands of the market, guaranteeing the supply of qualified labor needed for effective supply chain management and operation.

Governments play a role in international cooperation as well as regulation. The stability of international supply chains can be improved by governments working together with other nations. Economic alliances such as the North American Free Trade Agreement (NAFTA) and the European Union, for instance, make it easier for member states to exchange commodities and services, fostering a more stable and connected business climate.

X. The Importance of Modern Technologies in the Supply Chain

The supply chain is one of the most critical components for the success of any company or organization, as it integrates various processes such as planning, production, transportation, storage, and distribution. With the rapid development of technology, modern technologies have become a decisive factor in improving the performance of the supply chain, making it more efficient and flexible. Through these technologies, companies can achieve their goals faster, reduce costs, and enhance customer satisfaction.

X.1 Improving Planning and Forecasting

Good planning is the foundation of an effective supply chain. Thanks to modern technologies like Artificial Intelligence (AI) and predictive analytics, companies can now forecast demand more accurately based on market data and past trends. These tools help reduce excess inventory or shortages, leading to cost savings and ensuring customer needs are met on time. For example, e-commerce companies like Amazon use demand forecasting tools to predict the products their warehouses will need in the near future.

X.2 Increasing Efficiency in Transportation and Logistics

Modern technologies have revolutionized the transportation and logistics sector, which is a key part of the supply chain. Companies now use GPS tracking systems and fleet management technologies to monitor shipments and ensure timely deliveries. Furthermore,

automation and robotics are increasingly being used to reduce manual labor and enhance efficiency, whether in loading, unloading, or even delivering products to customers.

X.3 Inventory Management

Inventory management is one of the biggest challenges faced by supply chains, but with the implementation of modern technologies, it has become significantly more manageable. For example, the Internet of Things (IoT) can provide real-time, accurate visibility into inventory levels. IoT-enabled sensors can monitor inventory levels and alert companies when restocking is necessary. This not only reduces waste but also ensures operations continue uninterrupted.

X.4 Enhancing Transparency in Operations

Transparency is a critical element in improving relationships between suppliers and customers. Thanks to technologies like blockchain, companies can create secure and transparent digital records for every transaction in the supply chain. This ensures traceability of materials from the source to the final product, which enhances trust and reduces the risks of counterfeiting or fraud. For example, in the food industry, blockchain helps trace the origins of ingredients and ensures product safety.

X.5 Improving Customer Experience

Modern technologies help companies offer better customer service by enhancing the speed and accuracy of operations. For instance, data analytics can more accurately predict customer preferences and offer personalized solutions to meet their needs. Additionally, technologies like automation and robotics reduce product delivery times and improve service quality.

X.6 Flexibility and Adaptation

In a rapidly changing world filled with challenges such as natural disasters and health crises like the COVID-19 pandemic, the flexibility of the supply chain has become more important than ever. Modern technologies help companies adapt quickly to these changes by providing real-time information and accurate analytics, enabling data-driven strategic decisions.

X.7 Sustainability

Sustainability has become a priority for many companies, and modern technologies play a key role in achieving this. By utilizing data analytics and IoT, companies can optimize resource usage and reduce carbon emissions from transportation or production processes. Furthermore, technologies like 3D printing help reduce waste and conserve raw materials.

X.8 The Future of Supply Chains

There is no doubt that modern technologies have become a fundamental pillar in developing the supply chain. With ongoing technological advancements, supply chains will continue to become smarter and more sustainable, capable of adapting to the ever-changing needs of markets and customers. Therefore, companies that invest in these technologies will remain competitive and stay at the forefront.

XI. Conclusion

Supply chains vary widely across organizations, so no single set of security guidelines applies universally. A comprehensive security plan combines risk management, robust cyber defense, and adherence to government or customs protocols for international trade. The spend analysis framework adds value by helping organizations track critical data, identify risks, and develop proactive mitigation strategies. It also supports continuous monitoring and enforcement of policies across complex environments, while ensuring timely software updates to mitigate vulnerabilities from legacy or compromised systems.

Securing supply chains is no longer just an operational necessity, but a critical strategic priority for modern businesses. As global networks become increasingly interconnected and complex, the risks associated with cyber threats, data breaches, and physical disruptions continue to grow.

By embracing advanced technologies, implementing robust security measures, and fostering a culture of vigilance, organizations can mitigate vulnerabilities and enhance the resilience of their supply chains. A secure supply chain not only protects critical assets, it builds trust, ensures compliance, and drives long-term success in a highly competitive and dynamic global marketplace. Prioritizing supply chain security is an investment in operational stability and a foundation for sustainable growth.

Supplementary Materials

The following are available online at www.mdpi.com/xxx/s1, Figure S1: title, Table S1: title, Video S1: title.

Author Contributions

For research articles with several authors, a short paragraph specifying their individual contributions must be provided. Conceptualization, M.S.A.-K., H.A. and N.S.A.-H.; methodology, M.S.A.-K.; software, H.A.; validation, M.S.A.-K., H.A. and N.S.A.-H.; formal analysis, N.S.A.-H.; investigation, M.S.A.-K.; resources, H.A.; data curation, N.S.A.-H.; writing—original draft preparation, M.S.A.-K.; writing—review and editing, H.A.; visualization, N.S.A.-H.; supervision, M.S.A.-K.; project administration, H.A.; funding acquisition, N.S.A.-H. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Acknowledgments

In this section you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Keeper security. (2021). Supply Chain Security Solutions. Retrieved from Keeper Security website.

[2] Telecome Review Arabia. (2020). Cybersecurity in Supply Chain Management. Telecome Review Arabia Journal.

[3] Cyberbedia blog. (2021). Supply Chain Attacks and Defense Strategies. Cyberbedia Publications.

[4] Zalud, B. (2016, April 1). Supply chain security challenges in the digital age. Security Magazine.

[5] Sharma, A., & Jain, D.K. (2020). A Roadmap to Industry 4.0: Smart Production, Sharp Business and Sustainable Development (pp. 23–38). Springer: Cham, Switzerland.

[6] Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. In Proceedings of the 50th Hawaii International Conference on System Sciences.

[7] Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system.

[8] Ashenden, D. (2008). Information security management: a human challenge. Information Security Technical Report, 13(4), 195-201.