International Journal of Marketing and Technology
Vol. 14 Issue 06, June 2024
ISSN: 2249-1058 Impact Factor: 6.559
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Impact of Cybersecurity and AI on global Supply Chain and economy

Nikhil Shahani <snk043019@gmail.com>
Apoorva Sehgal <apoorva.segal@gmail.com>

Abstract

This paper examines the role of technological advancements in enhancing cybersecurity within supply chain management, emphasizing the impact of the Internet of Things (IoT) and Artificial Intelligence (AI). It explores how IoT, by enabling interconnected devices, transforms data collection and processing, essential for improving supply chain efficiency. It addresses cybersecurity vulnerabilities, including spyware and malicious software, and emphasizes the necessity for robust network security measures outlining future directions, advocating for continuous testing, and updating of cybersecurity frameworks to safeguard against potential attacks. The paper also discusses the role of AI and machine learning advancements are highlighted for their predictive capabilities, aiding in market trend analysis, competitor pricing, and customer behavior, thus optimizing profitability and competitiveness. Additionally, the research emphasizes the importance of supply chain visibility into global markets to mitigate risks associated with supply disruptions.

Key Keyboards

Supply chain management, Cyber security, Logistics, Internet of Things (IOT), Artificial Intelligence

Introduction

Supply Chain integration is the lifeblood of any economy, facilitating the flow of goods and services from producers to consumers. The events in 2020 significantly disrupted supply chains, exposing the vulnerabilities and leading to severe economic implications. In response to these disruptions, technological applications have played a crucial role in enhancing the efficiency of supply chains. This paper reviews the intersection of technology and supply chain management, focusing on the critical role of cybersecurity.

Central to the discussion is the Internet of Things (IoT), a network of interconnected devices that communicate and interact without human intervention. The IoT has revolutionized data collection and processing, providing unprecedented insights into supply chain operations. Coupled with advancements in Artificial Intelligence (AI) and machine learning, these technologies offer enhanced predictability and decision-making capabilities, crucial for managing complex supply chains in real-time.

This paper reviews the current state of cybersecurity in supply chain management, emphasizing the need for robust measures to protect against vulnerabilities and cyber threats. It explores how organizational information theory can be leveraged to integrate IoT with 4G and 5G networks, addressing practical challenges in data streaming and processing. Furthermore, the paper discusses the implications of AI-driven insights for market trend analysis, competitor pricing, and customer behavior, highlighting the potential for optimized profitability and competitiveness.

As businesses increasingly prioritize sustainability, this paper also examines the role of generative AI in fostering environmentally friendly supply chain practices. It emphasizes the importance of supply chain visibility in global markets, essential for mitigating risks and ensuring continuity in the face of disruptions. By addressing these multifaceted aspects, this study aims to provide a comprehensive overview of the technological advancements shaping the future of supply chain management and the critical importance of cybersecurity in this domain.

Advancements in IoT for Supply Chain Management

The Internet of Things (IoT) has become popular and evolving daily by adding new devices. Personal devices, every organization, and even the house is being converted into Technology and intelligence with the help of the IoT. The electronic devices will work with the help of internet connectivity. There is a need for a continuous internet connection to those devices to use this product and install it in a place to make it automatic.

As data becomes vital in organizations, every collection resource has been installed with this IoT, trying to collect and gather data in all ways. The issue is that there are many disadvantages, and speed is deficient, which takes time to process all the devices. There is a deep dive into the new Technology, the fifth generation (5G), which came into existence to address all the issues of the fourth generation (4G). Therefore, through this research study, there is a clear understanding regarding the problem and how this will be addressed with this 5G Technology. As data has become crucial in businesses, every gathering resource has been integrated with this IoT and is attempting to collect and acquire data in all available ways.

The IoT is enabling machine collaboration and communication. Many platforms and networks have been developed for the IoT, and market segments have lately begun creating specialized IoT applications and services. Integration of heterogeneous IoT networks into existing networks, particularly cellular networks, is in high demand: the International Telecommunication Union (ITU) and the Third Generation Partnership Project. As a result, the principal aim should be the IoT network scalability and availability. The research highlights a framework for connecting 5G networks to heterogeneous IoT networks. The suggested solution considers the International Telecommunication Union and 3GPP standards for system scalability and availability. The proposed framework includes fundamental communication paradigms: software-defined networking (SDN), device-to-device communications (D2D), and mobile edge computing (MEC).

The devices connected internally with the help of an internet connection are called the IoT. All connected devices can send and receive data from one device to another. All the most advanced machines are helping people live and work better. The IoT relates to the billions of physical gadgets now linked to the Internet and collecting and exchanging data worldwide. With the advent of low-cost circuit boards and the pervasiveness of wireless connections, it is now feasible to transform anything, from a pill to an airliner, into a component of the IoT. It links these diverse products and attaches sensors to give digital awareness to otherwise dumb gadgets, allowing real-time data without engaging a human. The IoT makes the world more innovative and responsive by fusing the physical and digital realms.

Cybersecurity in Supply Chain Management

The increased usage of all kinds of proxy servers is important in implementing and the overall core operations of Supply Chain Management across the globe. Proxy servers have existed for many decades.

1. Potentially unwanted applications (PUA), such as malicious browser extensions
2. Links to web spam and fraudulent advertising
3. Browser vulnerabilities
4. Browser redirection and clickjacking

There are several types of malicious software that hackers leverage,

1. "Primary loads", such as Trojans and utilities that facilitate the initial infection of a user's computer (a macro virus in a malicious Word document is an example of this type of tool)
2. PUA, which include malicious browser extensions
3. Suspicious windows binaries that spread threats

Spyware

Spyware can infect the system the same way as any other form of malware, and most online advertising software on the Internet is unwanted application (PUA) and spyware. There are many spyware providers that advertise their software as legal tools that provide useful services and adhere to end-user license agreements however the spyware disguised as PUA is software that secretly collects information about a user's computer activity.

Measures for enhancing Cybersecurity

The dangers to innovation show that a traceability framework can be inclined to a few network safety assaults. The contribution of different partners and a heterogeneous framework scene intensifies the assault surface and their effect. In the absence of solutions that provide real-time monitoring and leak path detection, attackers can move around the network undetected, potentially causing severe damage. Also, there is a need for testing segmentation policies and implementing robust tools to verify their effectiveness. The network security teams must take an initiative and effort to test and check the lists of managed devices on the network devices to avoid long term impact. Additionally, there must be regular and automatic testing of the corporate network, cloud infrastructure and end-device infrastructure that constantly get updated.

Digital Transformation and Reimagining the overall Industry

Digital transformation is the crucial bridge between the business of today and the digital business of the future. There have been major digital investments which are accelerating, digital return in the form of growth and competitive advantage remains elusive. A strategic approach to digital transformation is crucial and essential and hence digital possibilities shape the future's strategy. There are technological and operational decisions which need to be adaptive and aligned.

Also, not everyone needs a digital business to tap into digital thinking, and gaining an edge from it by adopting a technology or process is not the key. Organizations willing to reimagine operations and then incorporate the technologies that support new processes create significant value for customers and shareholders.

Challenges of Defense Enterprise

Currently there is a significant lack of current coordination strategy within defense organizations that addresses enterprise-level coordination challenges, therefore making it difficult to translate lessons from Defense's history and current industry into an integrated management model.

Enhancing Supply Chain Experience with Intelligence and Analytics

One of the significant advancements brought by AI and machine learning is enhanced predictability and the ability to identify patterns and connections to various external events. This capability enables the prediction and analysis of trends and their potential impacts. The insights generated by generative AI into market trends, competitor pricing, and customer behavior are crucial. These insights empower decision-making around price adjustments, leading to optimized profitability and competitiveness. Additionally, the ability to instantly adapt prices based on demand fluctuations ensures maximum revenue generation without alienating customers.

Part of the business complexity for some of the world's best-known brands is hidden inside huge supply chains. Things like keeping track of the vast labor force, individual components and a vast array of suppliers and sub-suppliers are incredibly complex tasks for companies without sophisticated supply chain expertise. Traceability has emerged as a cornerstone in supply chain management and is increasingly mandated by governments across the globe to ensure product safety and consumer protection.

Environmentally friendly Supply Chain Management

As sustainability continues to be thrust into the limelight, Generative Artificial Intelligence (Gen AI) plays a crucial role in creating environmentally friendly supply chain management systems. The ability to make decisions that interconnect profitability and coordination requirements with analyses of carbon emissions, transportation modes, and material sourcing, enables businesses to meet their business goals while staying committed to corporate social responsibilities and the values of operating green.

Supply Chain Visibility and Risk Management

Supply chains across the world are significantly harder to manage as the industry supply chains are often intertwined. For example, automobile supply chains have suppliers that are within the medical industry. And the medical supply chain shares suppliers in consumer products as consumers healthcare expectations change. The inability to predict disruptions and manage expanding supply chains has a significant negative impact on a brand. To expand, organizations must drive to newer markets specifically for cost advantages and to serve new consumers which would require selecting new suppliers and getting a deep understanding of new cultures and businesses.

Global manufacturing companies that have built a variety of great products for all major industries identify themselves as unique supply chain opportunities among massive stores of digital information about suppliers, customers, coordination and more. Better still, visibility into multiple markets means predicting this type of supply shortage before it happens and creating a supply chain strategy that minimizes this sort of risk.

References

Bartol, N. (2014). Cyber supply chain security practices DNA–filling in the puzzle using a diverse set of disciplines. Technovation.

Beyer, H. G., et al. (2007). Robust optimization–a comprehensive survey. Computer Methods in Applied Mechanics and Engineering.

Biswal, A. K., et al. (2018). Warehouse efficiency improvement using RFID in a humanitarian supply chain: Implications for Indian food security system. Transportation Research Part E: Logistics and Transportation Review.

Boiko, A., et al. (2019). Information systems for supply chain management: uncertainties, risks, and cyber security. Procedia Computer Science.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation.

Caldwell, T. (2015). Securing small businesses–the weakest link in a supply chain? Computer Fraud & Security.

Casino, F., et al. (2019). A systematic literature review of blockchain-based applications: current status, classification, and open issues. Telematics and Informatics.