International Journal of Scientific & Engineering Research Volume 11, Issue 5, May-2020
ISSN 2229-5518

The Importance of Cyber Security in Logistics

Joud Abdulfattah, Asmaa Munshi, Thana Aljohani, Remaz Alawaji, Suha Almuhanna
Department of Cybersecurity, College of Computer Science and Engineering
University of Jeddah, Saudi Arabia

Abstract
This study presents the importance of cybersecurity in logistics by performing a systematic literature review of the similarities between the physical and cyber supply chains, supply chain security and safeguarding transportation and shipping. In recent years, the number of cybersecurity threats has increased, resulting in problems caused by many gaps in confidentiality, integrity, and availability. Further, the study provides recommended solutions for logistics companies regarding information or cyber-attackers.

Keywords
Cyber Supply Chains, Supply Chain Management, supply chain security, Safeguarding Transportation and Shipping.

IJSER

Introduction
Nowadays, information is an economic resource and an essential tool for the success or failure of any organization at the national and international levels. This information can be subject to attacks and hacking aiming to use this information for his favor negatively. Therefore, every organization needs cybersecurity if it has information available online (Utriculi, et al., 2013).

In this paper, we will discuss the representation of cybersecurity in the supply chain and logistics for transportation and shipping protection. This is by presenting the similarities and differences between physical and cyber supply chains. As well as the significance of supply chain management in digital security. We clarify the role of IoT security to ensure the supply chain security system, what the cyber-attack is and the importance of logistics to the transport and shipping sector.

We have proposed future solutions and actions in this paper like the recommended solution for logistics companies regarding information or cyber-attackers including cyber Security governance. Security management guarantees that cybersecurity risks are enough limited by having security controls.

The advanced electronics company has a separate framework for formulating cybersecurity governance policies and procedures. For this reason, more research should be done to come up with more formalized standards and best practices on IoT supply chain systems.

Background and Literature Review

1. Similarities between the physical and cyber supply chains

1.1 Physical supply chain

1

"The physical supply chain means an integrated collection of activities that facilitate the flow of goods from the stage of origin (raw materials, component parts) through production/assembly to different warehouses/distribution centers, and in the end, for individual customers. This is through retail outlets or growingly, through direct delivery to individual residences/workplaces" (Boyson et al., 2009).

Firms generally have a vision that permanently makes clear - that supply chains are essential to the success of all operations. However, it is complicated and has many individual functions.

Suppliers, buyers, production, warehouse, transportation, wholesale managers, retailers, and customers. These jobs are effective and influential and are considered as part of the supply chain. If a problem, defect, or defect occurs in one of these functions, it will affect the system and its overall efficiency. (Boyson et al., 2009).

The ingenuity of the entire supply chain management and this is what the distinguished leader adopts, by using a comprehensive set of software applications that allow supply chain managers to evaluate the overall performance of the chain and intervene according to behavior when standard indicators indicate that a correction is necessary.

In administrative supervision in the supply chain and to ensure that every job inside it works as required and that individual tasks are carried out on time and comprehensively to achieve the desired results for companies and institutions, this achieves the overall superiority of the company as well as for the supply chain.

This oversight role extends to the organization's extended partners - suppliers, wholesalers, retailers, and customers. (Boyson et al., 2009).

1.2 Cyber Supply Chain.

" The cyber supply chain we know is the mass of IT systems (hardware, software, public networks, and categorized networks) that together allow the continued operation of key government and industrial base actors, such as the Department of Defense, the Department of Homeland Security, and its major suppliers. The cyber supply chain includes a full range of key actors, their organizational interactions, and the level of operations that plan, build, manage, maintain, and defend this infrastructure"(Boyson et al., 2009).

The figure below comprehensively illustrates the main roles and special responsibilities of the cyber supply chain ecosystem.

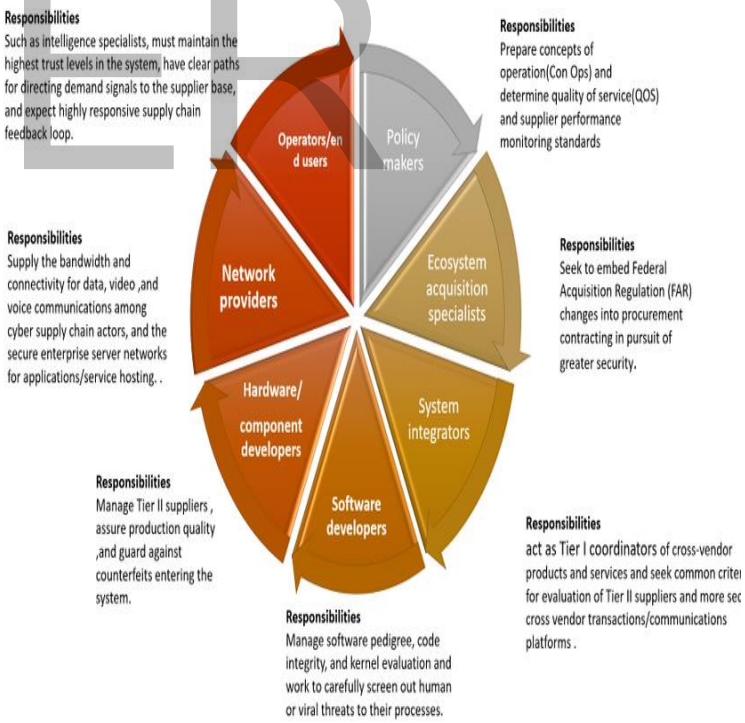

Chart1-1: The Cyber Supply Chain Ecosystem [1]

The cyber supply chain of IT systems is like the physical supply chain in its process from start to finish. Where software developers begin, and their role is similar to suppliers in the physical supply chain.

[1] *Boyson, S., Corsi, T., & Rossman, H. (2009). Building a cyber-supply chain assurance reference model. Science Applications International Corporation (SAIC).*

IJSER

We found similarities and compatibility between the roles of purchasing agents and production and distribution managers in the cyber supply chain and physical supply chain. It includes similar roles for policymakers,system integrators, hardware/component developers, and network providers in the cyber supply chain.(Boyson et al., 2009).

1.3 supply Chain Management

"Supply chain management is an integrating function with primary responsibility for linking major business functions and business processes within and across companies into a cohesive and high performing business model. It includes all logistics management activities as well as manufacturing operations, and it drives coordination of processes and activities within and across marketing, sales, product design, finance, and information technology" (Boyson, 2014).

By Supply Chain Security Management (SCSM), particularly in the global context, advancing and incorporating portions of the regular security management into comprehensive management of integrated supply chains. SCSM is spread in several areas such as Supply Chain Management, International trade management, cross border logistics services, processes, supply chain flexibility management, quality management, risk management, insurance documents and tools, policies, procedures, and reforms of customs (Hintsa et al., 2009).

Security programs of supply chain, systems, and standards have become more active in design for governments and international organizations. As for companies, they have complied with mandatory procedures and are also involved in designing some of these new procedures. So, the difficulties facing governments today are to realize and implement suitable control measures that increase security without endangering trade or increasing the burden on themselves and companies with extra working expenses.

The primary challenge of companies is to invest wisely in security in a manner consistent with new regulations while achieving the potential additional benefits that contribute to the efficiency of their supply chain. (Hintsa et al., 2009).

2. Supply chain security

There are many different types of crimes that occur in the supply chain and may depend on the way the goods are transported and the type of cargo. The site of the attack and the level of ability and experience of the criminal association. (Utriculi, et al., 2013).

It is no longer approved for companies to focus on internal security measures geared to preventing theft and contingency planning for factory sites and distribution centers only, which are called "the four walls". Instead, supply chain security is assumed and required, which of course goes beyond preventing theft from the threat of terrorism and requires the integration of security with many other units. And so on (Closs and McGarrell, 2004), the internal threat is the innermost part.

In November 2003 at Michigan State University, several companies held a workshop, which was talking about supply chain security. From this axis, many companies announced that they would use a multi-functional team consisting of taxes, customs, security, government relations, production control, logistics, procurement, internal controls, and human resources.

Because companies are now not only concerned with security measures in their own operations and those of first-class suppliers, but also rely on security measures throughout the supply chain. (Closs and McGarrell, 2004).

2.1 Secure the digital supply chain

A significant thing is to know how to assess the security status of the institution, and we also know the importance of digital security and that it is well known to the executive heads and management teams, but not only to make it an organizational priority and also to learn how to assess the security situation of the institution, then take adequate measures to identify and mitigate the risks.

Here we will provide examples of companies that have been breached prominently, such as Sony Pictures, so the problem cannot be completely solved, and we have another example also for the American retailer TARGET, the pirates concern on corporate vulnerabilities. Each time, they had the option to get to key IT systems remotely and take what they needed. On account of Target, that was customer credit card information and other individual details; on account of Sony Pictures, almost everything was. (Boyes, 2015).

IJSER

The goal nowadays is the intentional damage to a business violation - meaning damage caused by things like intellectual property theft, the impact of reputation, business disruption, and possibly - the use of unlawful access to material damage to infrastructure and vital equipment. Unfortunately, very few companies are concerned about these violations. (Boyes, 2015).

So, the focus will be on chief executives and manufacturing and logistics chain managers to focus on insurance. They also secure ERP and other central administrative systems.

We can now answer this question. What can companies do to reduce the risk of cyber-attacks on their supply chain?

Checking for bugs in Sony Company and other notable achievements will be a useful start. If you use strong and private passwords, do not store them on the server, and do not make the data that you are supposed to protect, in an unencrypted folder marked "Password". This inevitably reduces the risk of cyber-attacks on the supply chain.

Here, we also note that the ultra-sensitive data must be stored separately, away from the central ERP system and the broad user base, to avoid compromising the rights to access transaction data prompting to serious breaches. (Boyes, 2015).

2.2 securing IoT supply chain systems

IoT is one of the most important technologies used in the deployment and developing of cyber supply chain systems. IoT is used in tracking goods and assets and more over in exchanging data between the main players in supply chain systems (suppliers, retailers, and customers).

Security of IoT plays a significant role in the assurance of the security of the role supply chain system. In contrast to conventional systems, the interconnection between networks and devices in IoT supply chain systems allows for more severe attacks. In fact, these systems are incredibly complex, internationally distributed, and deeply interconnected. Which is make the impact of incidents practically hard to measure. However, IoT remains a largely unregulated technology when it comes to security policies and standards. (Farooq and Zhu, 2019).

Therefore, risk analysis and management in IoT supply chain systems is a very challenging task. Risk analysis provides the stakeholders and all the parties involved in an IoT supply chain system with a clear conception of all the involved financial and legal liabilities.

1. Safeguarding Transportation and Shipping

3.1 Extensive Backgroud

Logistics is one of the important sectors that has evolved recently, it focuses on management the transportation, and merchandise storage, dealing with such things as internal and external freight, reverse freight, communications during transportation, and warehouse storage. The logistics handle cargo delivery, freight forwarding, and coordination between both external and internal third-party transportation companies. (Lun, et al., 2016)

With the new development in the field of technology, many activities of logistics have been automated and digitized. As it is known the digitalization and automation that can be done online requires having a security system to secure all information that is archived and stored in their system. Recently the frequency and severity of cyber-attacks and data breaches have increased significantly. (Foote, 2017).

In logistics, cyber threats continue to evolve, many companies have started to take many measures to face the ever-increasing risks in cyberspace. The range and sophistication of cyber-attacks are increasing. These companies cannot afford to remain stationary in the face of these risks without taking the importance of cyber security seriously. The logistic companies still run their business based on the Internet, they must realize that their websites, ports, applications, and digital connections can be easily targeted and vulnerable to cyber-attacks and intrusions unless they are up to date according to cyber security practices and procedures. (Lomotko, et al., 2018).

IJSER

2. Research gap and challenges

4.1 Threats to sensitive data and information.

The growing industry of logistics including the shipping field has always been hesitant to embrace the new technologies. The digital transformation and adoption process will, however, simplify routine activities, enhance ship capabilities and protection, enhance productivity and create opportunities for collaboration and cooperation. In this dynamic ambitious market, more shipping companies see technical advances as a key for success. Yet new possibilities often lead to new obstacles: opening up the network to remote controls or data transfer raises the possibility of invading cyber threats. Electronic attacks often focus specifically on the marine industry, attacking and compromising the ship's GPS programs, GPS impersonation, GPS jamming, port container terminals, physical security alarms, electronic recognition certificates, cargo monitoring and record-keeping systems. Not only military ships, containers and oil tankers are targeted, but marine ships are under great risk as well. Safe sailing, navigation, and crew operations are essential elements that must be protected.

The number of cyber-attacks on ships across the world has steadily risen in recent years: security attacks and ransom operations in the logistics industry have been breached. Besides, commercial cruise ships suffer from DDoS attacks on ticketing services and theft of credentials. Moreover, cybercriminals can access steering ships in autopilot mode, manipulating cruise plans and radar signals or simply lock computers. (Foote, 2017). Therefore, the companies' work in the field of transportation and shipping has faced recently many cyber-threats that require to find the proper solutions to protect all sensitive data and information .

4.2 Decentralization (hard to provide full control over the whole supply chain).

Based on the previously discussed security aspects of the IoT supply chain systems, the most serious obstruction here is the decentralization. Which makes it hard to provide full control over the whole supply chain, as well as the lack of international regulations and standards. Some other logistical constrains discussed in (Farooq and Zhu, 2019) include the difficulty to find documentation of information about the supply chain due to privacy issues and competitiveness, and the lack of formalized best practices since they are highly depending on the nature of the industry. On other hand there is no centralized repository of documented and reported vulnerabilities and attacks to direct the risk analysis process for better detection of threats and potential attacks**.**

3. Recommended Solution

The recommended solution for logistics companies regarding information or cyber-attackers is to create International Cyber Agency that specializes in auditing systems and cyber logistics systems. Including two-stage security business models; security management guarantees that through implementing security controls, cybersecurity threats are sufficiently reduced, while security governance efficiently ties public security policies to key business goals and fundamental regulations. There is also ri**sk** management which involves identifying information assets that can be compromised by cyber-attacks. In addition to the auditing that focus on assessing enterprise compliance with cybersecurity regulatory guidelines (Utriculi, et al., 2013).

The companies can create an innovative platform to detect post-penetration with proactive capture of hidden threats, using forensic case analysis to demonstrate concessions. (Kardakova, et al., 2018**).**

4. Conclusion and Future work

This paper discussed the representation of cybersecurity in the supply chain and logistics for transportation and shipping protection.

Also, it emphasized the role of supply chain management and the threats and security of transportation and shipping businesses.

In this study we concluded that the most serious threats to the logistics and shipping sector are those which compromise the confidentiality of sensitive data and information of all the parties involved in the logistics business. As well as the decentralization of the cyber supply chain systems which makes it hard to provide full

IJSER

control and management over the whole supply chain risks.

For future work more research should be done to come up with more formalized standards and best practices on IoT supply chain systems that will guide the process of risk analysis to provide companies with the information they need to make their decisions upon the selection of the most appropriate IoT system to enforce their supply chain with. (Omitola and Wills, 2018).

References

Urciuoli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security–potential threats. Information & Security: An International Journal, 29(1).

Boyson, S., Corsi, T., & Rossman, H. (2009). Building a cyber supply chain assurance reference model. Science Applications International Corporation (SAIC).

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

Hintsa, J., Gutierrez, X., Wieser, P., & Hameri, A. P. (2009). Supply chain security management: an overview. International Journal of Logistics Systems and Management, 5(3), 344.

Closs, D. J., & McGarrell, E. F. (2004). Enhancing security throughout the supply chain (pp. 1-52). Washington, DC: IBM Center for the Business of Government.

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. Technology Innovation Management Review, 5(4), 28.

FAROOQ, M. J. & ZHU, Q. 2019. IoT Supply Chain Security: Overview, Challenges, and the Road Ahead.

Kardakova, M., Shipunov, I., Nyrkov, A. and Knysh, T., 2018, December. Cyber Security on Sea Transport. In Energy Management of Municipal Transportation Facilities and Transport (pp. 481-490). Springer, Cham.

Lun, V.Y., Lai, K.H. and Cheng, T.E., 2006. Shipping and transport logistics. Singapore: McGraw-Hill Education (Asia).

Foote, R. (2017). Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities, and Vessels Safe from Cyber Threats," Vol. 8: Iss. 2, Article 3. Available at: https://open.mitchellhamline.edu/cybaris/vol8/iss2/3

Lomotko, D.V., Kovalov, A.O., Kovalova, O.V. and Shuldiner, J.V., 2018. Safeguarding of Goods During Railway Shipping. International Journal of Engineering & Technology, 7(4.3), pp.246-250.

OMITOLA, T. & WILLS, G. 2018. Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain. Procedia Computer Science, 126, 441-450.

IJSER