Warehouses Against Cyber-Attack Risks

Giovanni Meggiato, Sirious Nterai, Etienne Skowronski, Ruodi Gao, Muhammad Atiqur Rahman
Postgraduate students in Logistics and Transportation Management
Department of Business Administration
University of Gothenburg
Gothenburg, Sweden
gusntesi@student.gu.se; gusmeggi@student.gu.se; gusrahmu@student.gu.se;
gusgaoru@student.gu.se; gusskoet@student.gu.se

Shahryar Sorooshian
Associate Professor in Business Administration
Department of Business Administration
University of Gothenburg
Gothenburg, Sweden

Abstract

Cyber-attacks are a tactic spreading in the last decades since the increased use of the internet has enabled offenders to achieve their goals. There are a plethora of protective measures against these attacks, but the most important step is making protection part of the company's strategy, by increasing prevention and investments in protective mechanisms. The aim of this paper is to explore the risk of hackers' attacks on warehouses and how companies deal with that risk. A number of solutions are provided via this qualitative research. Cyber-attacks are increasing alongside the use of the internet, shared information platforms, and the increased number of transactions, but companies are not unprotected, since there are solutions that companies can use to protect themselves.

Keywords
Cybercrime, Warehousing, Supply Chain Management, Risk

1. Introduction

An endless growing network, the internet offers individuals easy ways to access data that present an interest for them. This can be done from any electronic device that can connect to the internet. Part of living in the 'Internet Era' is understanding and accepting accessibility of information is convenient, but the safety of information is almost compromised for convenience, leaving companies and data vulnerable to digital disruption (Warehouse & Logistics News, 2019). Up until recently, cybersecurity was often not considered to be a top priority issue in supply chain management. Supply chain businesses such as third-party logistics (3PLs) providers rely on a rapid, continuous flow of data to operate properly (Choy et al., 2008).

3PLs and their clients also rely on daily access to enormous quantities of critical data, making them especially vulnerable and highly desirable targets. There are additional reasons for why supply chain and 3PLs businesses are at higher risk (ibid). By its very nature, the supply chain is a network of connected partners, often a vast array of businesses interconnected via shared information. Supply chain businesses tend to rely heavily on connectivity for mission critical operations but many still rely on old systems and outdated technologies. This makes supply chain and 3PL warehouses often more vulnerable to cyberattacks. Critical information such as buyer payment details, manufacturing specifications, order fulfillment, operational capabilities, and processes, patent data and other data can be held for ransom or stolen. Ignoring these risks can come at a steep price: major manufacturers such as Renault have lost valuable production time, equating to significant losses. (Datexcorp, 2021). As a result, the purpose of this

report will be to discuss some possible types of cyber-attacks and to present how logistics can be protected against them, with a focus on warehouse operations of logistics.

2. Theoretical Analysis

2.1 Introduction to Cyber Attacks

Cyber-attacks are a common phenomenon around the globe, and they are in the form of internet worms, automatic scans, or distributed denial of service (DDoS) (Koike et al., 2005). Generally, computer hackers gain access to a computer or to a similar device by exploiting a flaw in the computer's software or configuration, or by using stolen usernames and passwords. Once hackers have access, they can impersonate legitimate users for accessing data, as well as change files and configurations, or they can manipulate other devices connected to the compromised computer. Consequences of hacking can be serious, depending on which machines hackers have accessed and what level of access they have achieved (Melendez, 2019). According to Koike et al. (2005), these attacks can cause damage to economic activities and the widespread use of computers during the last decades has made businesses even more dependent on technology. This accelerated dependency though has increased the level of vulnerability towards attacks (Warren and Hutchinson, 2000). Therefore, companies need to assess the potential risks and manage them.

The rapid development of information technology is making possible the increased exchange of information among different business partners (Warren and Hutchinson, 2000) and the supply chain management systems do not fail to fall under the same exchange, as they are dependent on electronic systems. The more international and widespread the commercial exchanges of a company, the higher the risk of being attacked by hackers (Koike et al., 2005; Bunker, 2020). In other words, global interconnectivity led to an increase in cyberthreats (Huang and Chiang, 2021).

A study conducted on hacker attacks in 2017 (Cukier, 2017) showed that every 39 seconds hackers are trying to attack computers with access to the internet. While in 2019 the cost of data breaches in the US only reached the value of $3.5 billion (Cobalt, 2021). Therefore, warehouses' systems should not be neglected. In the warehouse there is always a system that thrives the process more effectively and efficiently. That system is always at risk of being hacked and for this, cybersecurity is very important. Cybersecurity focuses on the management of information technology systems, software, and network for both a business and its third-party suppliers. It is designed to mitigate the threats of malware, cyber terrorism, and data theft.

2.2 Supply Chain Management and Its Risks

Mentzer et al. (2001) defined Supply Chain Management (SCM) as "the … coordination of the traditional business functions … within a particular company and across businesses within the supply chain, for the purposes of improving the long-term performance of the individual companies and the supply chain as a whole." That is why SCM cannot be seen from the perspective of a single company, but its partners become part of the picture as well. With the development of technology, SCM has become more popular, and companies have been able to better integrate their business partners' information (Moshood et al., 2021; Abideen et al., 2021).

The application of computers in SCM makes the task no longer a single linear operation. The SCM system consists of a widely distributed network. As digital tools continue to become more innovative, their applications are the incarnation of the fourth industrial revolution in manufacturing (e.g., artificial intelligence (AI), Internet of Things (IoT), machine learning, automation, sensors) (Moshood, 2021). These technologies are used for supply chain optimization. For example, the concrete manifestation of the IoT can be explained as people or things with biochips, which can connect to sensors embedded in cars to remind drivers of information security. It is a system of interconnected digital devices, computing machines, people, objects, and machines (Gillis, 2021). Companies can use the IoT to manage and control warehouse inventory (Trung et al., 2021). At the same time, however, that may falsify data transmitted between participants (such as ordering parties and manufacturers), resulting in supply disruptions or ineffective production and transportation (Torbacki, 2021).

Planning systems, warehouse inventory planning, delivery speed have improved, while costs are being reduced to improve a company's market value and competitiveness. Based on Boiko et al (2019) the future trend of SCM is its

development towards global e-commerce, with the communication between manufacturers, suppliers, contractors, transportation, and trading companies already being part of an online network.

At the same time, there are many uncertainties and network security risks under such a development trend. Where different vulnerabilities and weaknesses can make users vulnerable to hacker attacks and threats (Boiko et al., 2019). According to an Identity Theft Resource Centre (ITRC) survey in 2021, there was an increase of 42% in the first quarter of the year in supply chain hacking attacks in the US, which in turn strengthens the fear of cyber-attacks in the supply chain operations. Pandey et al. (2020) proposed that network security risks significantly impact supply chain performance, and the company's information and communication technology may be one of the reasons for vulnerabilities and exposure to security threats.

2.3 Warehousing and Its Risks

In the era of digitalization almost all businesses have an online presence, be that in social networks or through their official webpages. The reason behind it is so they can reach as many consumers as they can, but companies do not take into consideration the risks regarding security when they begin their online services (Warren and Hutchinson, 2000). Reaching the target market can be done either by having a physical or an online store. In both cases the need for a warehouse is undeniable.

Warehousing is one of the most critical subsystems in the SCM. Its implementation cost accounts for a large part of the logistics cost and provides material management conditions. The main functions of warehousing are the goods receival, storage, picking, shipment, and last the fulfillment of e-commerce orders (Dragomirov, 2019). According to Van den Berg and Zijm (1999) there are three different types of warehouses, the distribution, production, and contract warehouses. In all three types there is a movement of material, be them raw, semi-finished or finished products. In the modern market, logistics companies often reduce human resources and costs by automated warehousing (Boenzi et al., 2017). Changing the traditional working mode to ensure the effective operation of storing and retrieving products through industry 4.0. (Pandian, 2019). Li-mei (2018) shows that the future will realize full automation and intelligent warehouse management is no longer just an idea. Therefore, for the purposes of the present paper it is assumed that the warehouses mentioned are automated and their dependence on information exchange and technology is higher, aka the risks are higher.

In the Verizon data breach case, warehousing employees stored a large amount of customer data in a database without setting access rights. A web application attack on Verizon data was used to track individuals or businesses into giving them more detailed and sensitive information (Allais, 2021). As a result, apart from the direct financial losses, the company’s reputation got damaged, with a direct impact on market competitiveness and its customers’ loyalty decreased. In another case, hackers hacked HVAC bank to gain access to Target's system and accessed the bank card numbers of 100 million customers (W&Ln, 2019). This incident did not only cause huge losses for the company but also affected the customers who cooperated with the company.

To sum up, the security of warehouse management development plays a crucial role in the whole SCM. In the competitive market of the whole supply chain, network security and risks coexist. The company needs to control risks well and keep up with the information technology innovation environment to improve the company's performance and market competitiveness (Sorooshian et al., 2020; Mun et al., 2020).

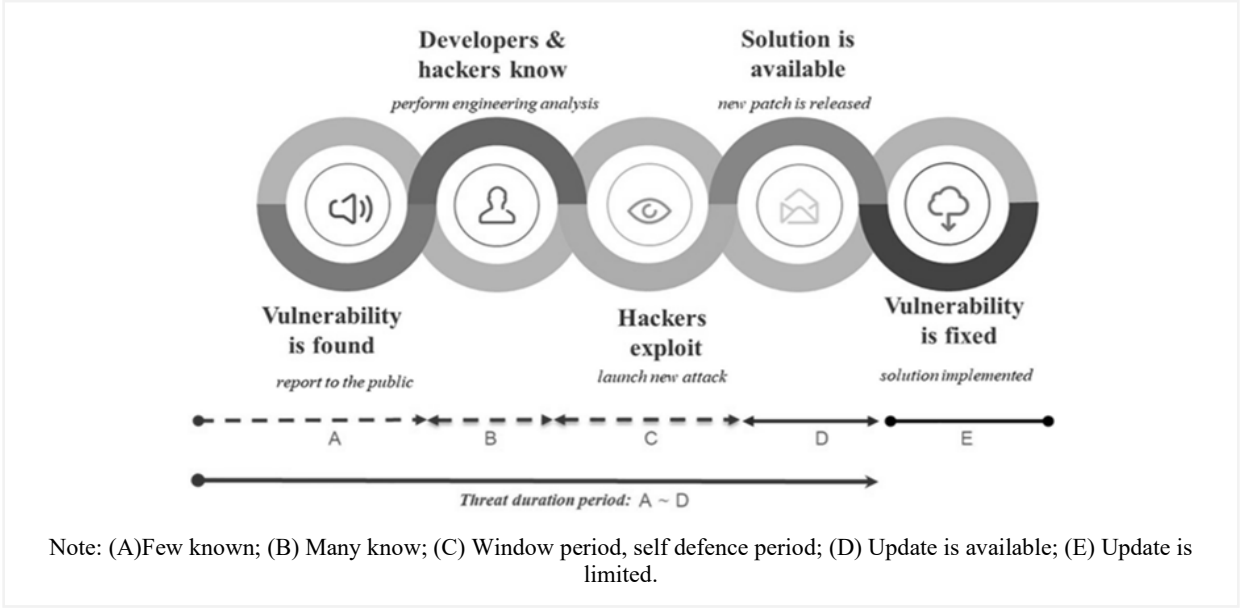
2.4 Warehousing and Steps Towards Protection

Preventing and managing risks can become easier when one knows what form it might take. Most often the attackers use a software with the purpose of cracking passwords, or they try to steal credit card information through various paths, called “spoofing attacks”, or they block the user’s ability to access various applications/destinations (Warren and Hutchinson, 2000). Of course, there are multiple ways of harming a business, but the focus remains on the preventing side.

Bunker (2020) supports that education about threat mitigation, precautions and investment in technology that is up to date and can offer protection against cyber-attacks, are the initial and most important steps for a business and its employees. While Warren and Hutchinson (2000) propose the use of encryption in accordance with security standards, access control points, proper training on computer security systems, and lastly raising awareness among employees

regarding potential risks. On the other hand, Shields (2015) pinpoints the recognition of weakness in one's system and the implementation of a pro-active model, as a risk protection measure.

Figure 1 depicts how the situation is in most of the companies in regard to their system's vulnerabilities (Huang and Chiang, 2021). When warehousing systems, and not only, are installed their vulnerabilities are not known. In this step, hackers have the upper hand because these are the security points, they take advantage. What the figure explains more is that there is another group of vulnerabilities that are known, but companies choose to ignore or do not repair. This comes as a lack of time or increased cost and complexity.



Note: (A)Few known; (B) Many know; (C) Window period, self defence period; (D) Update is available; (E) Update is limited.

Figure 1. Toward a Self-Adaptive Cyberdefense Framework in Organization, by Huang and Chiang (2021).

Cyberattacks are a potential and increasing risk for all types of industries. It is a phenomenon that globally occurs on a daily basis, but the collection of frequency data was not possible on how often it might occur on a supply chain management and specially on warehouse management. But being on the safe side is a better option than ending up being a victim. Before reacting to a threat, first it needs to be detected, next a risk assessment about the damage and the recovery tactics follows and last the creation of an immune system that in most of the cases is adaptive, since not all vulnerabilities and threads can be fought back (Huang and Chiang, 2021).

3. Analysis - Risk-Preventing Solutions

3.1. Making Full Use of Available Technology

There are different methods companies and warehouses can use to prevent themselves from being hacked. The range of possibilities is big and sometimes, implementing very simple measures can already reduce the risk of hackers entering informatics systems in warehouses.

- Updated Software

Probably the first important measure that is quite simple to realise is to constantly keep the systems of the warehouses up to date. This includes all software that is in use and the warehouse management system (WMS). Using outdated software more strongly exposes a company to the risk of being hacked, as the hackers use more and more advanced processes to enter an informatics system and an old version of a software might not be able to prevent it (American Warehouses, 2021). It might happen that cybercriminals are informed about an outdated software in a company and know exactly how to use this weakness and enter the system more easily. The speed of development of patches to solve weaknesses in the software is also important here and should play a role in the decision-making of warehouses

about which software to purchase (Farahni et. al., 2016). Software and WMS's are often the first door for hackers to a lot of data about the company and customers and should therefore not be breached (Parker Software, 2021).

- Back-Up Data

Besides securing the data with frequent software updates, a company should also back-up all its data frequently. Hackers can encrypt or remove valuable data, like customer information, therefore companies would be better off having saved their data externally (American Warehouses, 2021). The systematic back-up of data can be done automatically by using a software that does it consistently and is able to restore different versions of back-ups easily (Raam, 2019). According to Raam (2019), a company should also have a good "disaster recovery plan" in case some data is lost and needs to be recovered. He also advances the 3-2-1 rule that can be followed when securing data. According to this rule, the data should be saved three times, in two different mediums and one of the copies should be held outside the company's facilities. This last point might be more to protect the data from possible natural catastrophes than from hackers.

- Antivirus Software

The next step for a warehouse is to have a good antivirus software and effective firewalls. A firewall is a device that intercepts network traffic between the in-house system and external systems and checks it to identify potential dangers for the internal system of the company and block entering malware (Forcepoint, 2021). Antiviruses, as the name says, detect, block or remove viruses from a device. A warehouse can also use anti-ransomware protection, a ransomware being a form of a malware that locks data and is asking money to the company in exchange of the data (American Warehouses, 2021).
All of these measures represent costs for the warehouse, but it is worth investing enough money into cybersecurity as this improves the profit of a company in the long run and as a cyberattack can quite easily cause huge problems to a warehouse and thus to the whole company (Gibbons, 2020).

3.2. Employee's Role in Cybersecurity

On the other hand, the warehouse can put some responsibility on its employees to secure the facilities and the systems from external attacks. It is the humans that are actually the biggest threat for companies in that sense, or rather the human error. According to a study from IBM, 95% of successful cyberattacks on companies are mainly due to human errors (Ahola, 2021). A warehouse's workforce should therefore be aware of the risks that the usage of WMS, computers and other technologies brings to the company and should be trained to be able to respond to certain situations. This is important because the cause of human errors is often the gap between the employees' skills and knowledge and the actual functioning of a system (Liginlal et al., 2008).

It starts with simple skills, like that all employees should be able to recognize suspicious e-mails or dangerous links for example (Allais, 2021). Then, it has to be monitored how easy data can be accessed from the employees. As warehouses usually contain huge databases with very important information, the warehouse managers can restrict access to certain data to certain employees, by for example defining in which areas of the WMS every employee are able to log in. An employee could be restrained to the functions and data that it requires for its specific task, and not have access to the whole WMS for example (Allais, 2021).

Concerning passwords, employees should use complicated ones and be trustworthy to not spread them. Using a password management system can be a good solution for companies, as the system gives random complicated passwords that do not have to be remembered by employees (Ahola, 2021). Besides protecting access to software and databases, employees have to be cautious about access to hardware. Liginlal et al. (2008) suggest that computers or other connected devices, as well as documents falling into the hands of the wrong people can also be a huge threat for any company in terms of security. This involves rules like to not lose sight of an open computer or the restriction of bringing office devices home. Finally, there can be a restriction on the use of personal devices in the workplace to reduce risks.

To sum up, the above-mentioned measures are some of the alternatives that warehouses can implement in order to reduce the risks of cyberattacks. The risk can never be completely eliminated, as especially a certain amount of human error is impossible to avoid. But implementing the mentioned steps, puts a warehouse on the safer side and can only be beneficial for the business, even if it involves high costs.

3.3. The Blockchain Technology

One of the possible (especially for the future) solutions against the virtual risks a supply chain can consider should be the blockchain technology (Wahab et al., 2020). Blockchain technology can be defined as a kind of virtual network, a safer and more developed one than those we are familiar with in our home or work environment.

The main concept is, as the word itself suggests, a chain consisting of blocks containing information. Each block has three main elements: data, the hash and the hash of the previous block. The hash is a string of numbers and letters identifying a block. When a new block is created, a new hash appears. The hash of the previous block is what generates the chain, connecting the blocks. The first block of the chain, the only one which cannot be connected to a previous one, is called genesis block. If a hacker tempered a block, the hash of that block would be modified and the following block would not be valid anymore, because it would not contain the same hash of the previous block. But the hash system is not enough. The second step that makes the blockchain safe is the proof of work, a request for supplemental calculations. The proof of work makes the creation of new blocks slower, contrasting the effort of the hacker. For instance, in the case of Bitcoin, a proof of work requires ten minutes, so the amount of time to sabotage the entire chain could be huge. (ibid)

Another feature, which makes this technology safer, is its decentralisation. The blockchain uses a peer-to-peer (P2P) network, which is almost similar to the kind of network people used in the 2000's, an example of which is eMule. The connected device to this P2P network becomes a node, a critical component of this technology in other words. The device can receive a complete copy of the blockchain, and to verify that everything is correct. When a new block is created, this will be sent to all the nodes of the network, letting them add it to their own copy of the blockchain. This impedes hackers: they should sabotage every single block of the chain, re-do the proof of work for each of them and take control of the majority of the network. (ibid, Nermin et al., 2021)

According to Min (2019) blockchain technology can improve the supply chain or warehouse operations. It can enable evolution from the conventional risk management to a BT-enabled risk management. If the first one is reactive, the second is preventive or proactive. If the first buffers and hedges, the second is about sharing risks and information. Then, conventional risk management detects tangible risk, while a blockchain can detect a lot of invisible risks, progressing to a multilayer protection from a simple damage control.

One of the supply chain vulnerabilities that a blockchain can improve is contract formation by proposing the ideal solution of a smart contract. A smart contract is a contract converted to computer codes that automatically enforces obligations, being self-executing and self-verifying, mitigating risk and giving the firm more efficiency. Another use of blockchain is asset tracking: it is possible to register the entire journey of goods along the supply chain, reducing - for example - "the risk of loss and damage during transit", "simplifying global trade with added trust and transparency" (Min, 2019). This aspect can be crucial in the food industry, for instance, Walmart asked IBM to take part in an experiment about food safety. They developed a blockchain that made it possible to reduce the time for a normal tracing food process from seven days to 2.2 seconds (Miller, 2018).

Moreover, a blockchain can help with secure and error-free order fulfilments, especially in those steps of order fulfillment such as checking customer credit history and processing the order, checking, and allocating on-hand inventory, notifying customers of order/shipment status, confirming order delivery receipt, checking missed delivery on some orders and record the order history. For Min (2019), the last destination of a blockchain is the fight against cybercrime. He states that antivirus software is not enough to abate the risk and "the use of BT can remove the risk of a single point of failure with its end-to-end encryption, visibility and privacy". Blockchain can store data to exchange them in a secure way among players of the supply chain that do not trust each other (Fernández-Caramés et al., 2019). Some researchers proposed an interesting communication architecture for the warehouse of the future, where blockchain technology has a part in it. They suggested an Unmanned Aerial Vehicle (UAV) incorporating a Single-Board Computer (SBC) and a tag reader. The SBC is that board that processes information from the tag reader and sends it to a so-called ground station. BT appears in this step, when the ground station can send data to a blockchain, instead of centralised solutions like databases and cloud-based services, "to provide enhanced cybersecurity". In this way the system can join smart contracts and let the SBC store data more safely. So, with a warehouse like this, the enterprise can take advantage of interesting BT's features, such as transparency, data authenticity, data security and operational efficiency. (Fernández-Caramés et al., 2019)

To conclude, Min (2019) supports that it is too early to adopt this technology, because of factors such as future legal and regulatory compliance, actual computing power, lack of expertise and organizational resistance. Indeed, at the moment, what Min called the focal company for the blockchain is a large multinational firm, such as one of Fortune 500 companies, because of their big staff and IT infrastructure.

4. Conclusion and Suggestions for Future Research

Throughout the paper it has been presented the real existence of cyber-attacks towards supply chain operations and warehouses, followed by measures companies can take to prevent attacks on their systems. Hacking is a great threat and the current development towards a more and more connected world makes any individual and company more vulnerable against cyber-attacks. The supply chains of companies are no exception to that, and the wish for optimized processes makes supply chain planners rely on information technologies and automation to operate their supply network. The risk of cyberattacks is thus huge for the various companies involved. To narrow the discussion a bit, the focus of this report has been cyber-security inside warehouses.

Warehouses are crucial components of most of the supply chains and manage a lot of important tasks like sorting, storage, and the shipment of goods. Their vulnerability against hackers is growing, as the current trend goes towards developing fully automated warehouses managed by a fully intelligent warehouse management system that relies on digital information exchange. This thread represents a huge challenge for the companies. Moreover, potential risk-preventing actions and technologies have been presented. Several simple measures that warehouses can consider minimizing risks have been detailed. These measures focus on technology but also on the human's responsibility in cybersecurity.

Finally, trying to take the research a step further, a ground-breaking option such as blockchain was presented. An alternative that has a great potential to thrive, even though it is in its beginning and companies are skeptical. But looking back into human history, was not every technology worth trying, fought against at its beginning? So far, this information sharing technology presents a high safety level that is extremely difficult to hack, while offering more effectiveness inside the supply chain. This solution also shows another reason for developing the concept of cooperation within supply chain networks, connecting vendors and buyers with long-term strategic partnerships in a deeper way, compatible with that one suggested by just-in-time (JIT) manufacturing and related logistical models, such as those suggested by Sarkar and Giri (2020) and connected to the ordering cost reduction alongside the process quality improvement on an integrated vendor–buyer inventory system. So, this technology has a huge potential and could make supply chain and warehousing enter a whole new era of safe information sharing and operating, but only the future will tell.

References

Abideen, A.Z., Pyeman, J., Sundram, V.P.K., Tseng, M.-L., Sorooshian, S. Leveraging Capabilities of Technology into a Circular Supply Chain to Build Circular Business Models: A State-of-the-Art Systematic Review. *Sustainability*, 13, 8997, 2021.

Ahola, M. The Role of Human Error in Successful Cyber Security Breaches. *Usecure*; 2021

Allais, E. Best practices for keeping your warehouse cyber secure Industrial distribution, 2021

Boenzi, F., Digiesi, S., Facchini, F., Mossa, G., & Mummolo, G. A Nonlinear Integer Programming Model for Warehousing Sustainable Logistics. *Engineering Systems and Networks,* pp. 99-107, 2017.

Boiko, A., Shendryk, V., & Boiko, O. Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia computer science*, 149, pp.65-70, 2019.

Bunker, G. (2020). Targeted cyber-attacks: how to mitigate the increasing risk. Network Security, 2020(1), 17-19.

Choy, K. L., Chow, H. K., Tan, K. H., Chan, C. K., Mok, E. C., & Wang, Q. Leveraging the supply chain flexibility of third party logistics–Hybrid knowledge-based system approach. *Expert Systems with Applications*, 35(4), pp. 1998-2016, 2008.

Fox, J. Cobalt. Business Cost of Cybercrime (Feb 11, 2021). https://cobalt.io/blog/business-cost-of-cybercrime [Accessed 20th December 2021]

Cukier, M. (2007). Hackers Attack Every 39 Seconds. Available at: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds[Accessed 6 December 2021].

Dragomirov, N. Warehousing in logistics–main review of Bulgarian research contribution. In Conference proceedings *5-th International Scientific Conference ERAZ-Knowledge Based Sustainable Development Budapest*, Hungary, pp. 107-111, 2019.

Jasmin Farahani, Natalie M. Scala, Ph.D, LTC Paul Goethals, Ph.D, Adam Tagert, Ph.D, (2016) Best practices in cybersecurity: Processes and metrics. Baltimore business review: A Maryland journal, Available at: <https://www.cfasociety.org/baltimore/Documents/2016%20Baltimore%20Business%20Review%20copy.pdf#page=16> [Accessed 5 December 2021]

Fernández-Caramés, T., Blanco-Novoa, O., Froiz-Míguez, I. and Fraga-Lamas, P. Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applications in Big Data-Driven Supply Chain Management. Sensors, [online] 19(10), p.2394, 2019. Available at: <https://www.mdpi.com/1424-8220/19/10/2394> [Accessed 4 December 2021].

Gibbons, S. Why Investing In Cybersecurity Makes Sense Right Now. *2021 Forbes Media LLC*. 2020

Gillis, A. (2021). What is the internet of things (LoT). Available online at:https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Accessed 17 December 2021].

Huang, K., & Chiang, K. Toward a Self-Adaptive Cyberdefense Framework in Organization. SAGE Open, 11(1), *SAGE open*, 2021-01, 11 (1), 2021.

Koike, H., Ohno, K., & Koizumi, K. Visualizing cyber-attacks using IP matrix. *IEEE Workshop on Visualization for Computer Security*, pp. 91-98, 2005.

Li-Mei, D. U. A. N. Path Planning for Batch Picking of Warehousing and Logistics Robots Based on Modified A* Algorithm. *Academic Journal of Manufacturing Engineering*, 16(2), 2018

Liginlal, D., Sim, I., Khansa, L., How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Elsevier Ltd*. 2008

Melendez, Steven (2019), The Effects of Computer Hacking on an Organization, https://smallbusiness.chron.com/effects-computer-hacking-organization-17975.html [Accessed 6 December 2021]

Mentzer, J.T., DeWitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D. and Zacharia, Z.G. Defining supply chain management. *Journal of Business logistics*, 22(2), pp.1-25, 2001.

Miller, R., 2018. Walmart is betting on the blockchain to improve food safety. [online] TechCrunch. Available at: <https://techcrunch.com/2018/09/24/walmart-is-betting-on-the-blockchain-to-improve-food-safety/?guccounter=2> [Accessed 4 December 2021].

Min, H. Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 62(1), pp.35-45, 2019.

Mun, S. Y., Sorooshian, S. Prioritization of risk factors affecting information technology (IT) projects in malaysia. *Quality - Access to Success*, 21(176), pp.153-158, 2020.

Moshood, T. D., Sorooshian, S. The physical internet: A means towards achieving global logistics sustainability. *Open Engineering*, 11(1), pp. 815-829, 202.

Moshood, T. D., Nawanir, G., Sorooshian, S., Okfalisa, O. Digital twins driven supply chain visibility within logistics: A new paradigm for future logistics. *Applied System Innovation*, 4(2), 2021.

Nermin B, Sorooshian S, Motives for the new disruptive technologies: focus on the Blockchain technology, *Disruptive Technology and Digital Transformation for Business and Government*, IGI Global, 2021

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, 2020.

Pandian, A. P. Artificial intelligence application in smart warehousing environment for automated logistics. *Journal of Artificial Intelligence*, 1(02), pp. 63-72, 2019.

Raam, G, Six reasons why data backups are crucial for your business. ManageEngine Blog. 2021 Zoho Corporation Pvt. Ltd, 2019

S. Sarkar & B. C. Giri: *Stochastic supply chain model with imperfect production and controllable defective rate, International Journal of Systems Science:* Operations & Logistics, 7:2, pp. 133-146, 2020

Shields, K. Cybersecurity: Recognizing the risk and protecting against attacks. *NC Banking Inst.*, 19, 345,2015.

Sorooshian, S., Mun, S. Y. Literature review: Critical risk factors affecting information-technology projects. *Quality - Access to Success*, 21(175), pp.157-161, 2020.

Trung, N. D., Huy, D. T. N., & Le, T. H. IoTs, Machine Learning (ML), AI and Digital Transformation Affects Various Industries-Principles and Cybersecurity Risks Solutions. *Management*, 2021.

Torbacki, W. A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. *Sustainability*, 13(16), 8833, 2021.

Un. (American warehouse) (2021) Cyber security measures every warehouse should take. American warehouses. Available at: <https://www.americanwarehouses.com/blog/cyber-security-measures-every-warehouse-should-take>[Accessed 5 December 2021].

Un. (Datexcorp, 2021) 11 Tips to Help Prevent Cyber Attacks against Your 3PL Warehouse. Available at: <https://www.datexcorp.com/11-tips-to-help-prevent-cyber-attacks-against-your-3pl-warehouse/> [Accessed 17 December 2021].
Un. (Forcepoint) (2021) What is a Firewall? Forecpoint 2021. Available at: <https://www.forcepoint.com/cyber-edu/firewall> [Accessed 5 December 2021].
Un. (Parker software) (2021) The security risks of outdated software. ParkerSoftware.com. Available at: <https://www.parkersoftware.com/blog/the-security-risks-of-outdated-software/> [Accessed 5 December 2021].
Un. (Warehouse & Logistics News) (2019) Cyber Security in Supply Chain. Available at: < https://warehousenews.co.uk/2019/11/cyber-security-in-supply-chain/> [Accessed 17 December 2021].
Van den Berg, J. P., & Zijm, W. H. Models for warehouse management: Classification and examples. *International journal of production economics*, 59(1-3), pp.519-528, 1999.
Wahab, S. N., Loo, Y. M., & Say, C. S. Antecedents of blockchain technology application among Malaysian warehouse industry. *International Journal of Logistics Systems and Management*, 37(3), pp.427-444, 2020.
Warren, M., & Hutchinson, W. Cyber-attacks against supply chain management systems: a short note. International *Journal of Physical Distribution & Logistics Management*, 2000.

Biographies

Giovanni Meggiato. is currently a postgraduate student at the program of Logistics and Transport management at the university of Gothenburg. In 2021 he received a BSc in Economics and Business at Ca' Foscari University of Venice. His interest in Logistics rose during this programme, which included the course in Economics and Management of Port Activities (in collaboration with North Adriatic Sea Port Authority). He has been a selected student for the 2021 Green Week Academy: the Green Week consisted of a tour around the north-eastern Italy through firms characterized by their investments on sustainability. The tour was followed by a weekend of conferences, promoted by Corriere della Sera, with a focus on logistics, one of them with Enrico Giovannini: Minister of Sustainable Infrastructures and Mobility. Born in Treviso, Italy, he lives in Gothenburg, Sweden. He was among the first five authors who contributed equally to this work.

Sirious Nterai. is currently a postgraduate student at the program of Logistics and Transport management at the university of Gothenburg and received a BSc in Business Administration at the university of Piraeus. Has an interest in Supply chain and industry 4.0. The last 2 years has been working in Retail and holding the position of Operations specialist and has been working with inventory and stock management. She was among the first five authors who have contributed equally to this work.

Etienne Skowronski. is currently a postgraduate student at the program of Logistics and Transport management at the university of Gothenburg. Born and raised in Munich from a French mother and a German father, he completed school with both German and French graduations and went on to do a Bachelor in Business Administration at the University of Mannheim. During this time, he spent one exchange semester at the Universidad del Desarrollo in Santiago de Chile. He graduated in Mannheim in Summer 2020. In the year 2020/2021, he collected practical experience doing an internship in the management team of a Decathlon warehouse in Dortmund, Germany. He started his Master's degree in Gothenburg in September 2021. He was among the first five authors who contributed equally to this work. This report was part of an assignment in their Supply chain Management course.

Ruodi Gao. is currently a postgraduate student at the program of Logistics and Transport management at the university of Gothenburg. She received her Degree of Bachelor of Science in Business and Economics with a major in Economics in Jönköping University, Sweden. Born in China. Has an interest in Supply chain and industry 4.0; who among the first five authors contributed equally to this work. This report was part of an assignment in their Supply chain Management course.

Muhammad Atiqur Rahman. is currently a postgraduate student at the program of Logistics and Transport management at the university of Gothenburg. Has an interest in Supply chain and industry 4.0; who among the first five authors contributed equally to this work. This report was part of an assignment in their Supply chain Management course.

Shahryar Sorooshian. Received his BSc, MSc, and PhD in industrial engineering plus an MBA in business analytics. He is a certified professional in engineering management, a graduate technologist, and an accredited management consultant. With more than 10 year experience, he now serves in the business school, University of Gothenburg as an associate professor. His field of interest is business Engineering, Industrial management, and Engineering management. He was lecturer of the course where the students team wrote this project under his mentorship.
.