LogForum

> Scientific Journal of Logistics <

2021, 17 (1), 49-57

http://doi.org/10.17270/J.LOG.2021.555

http://www.logforum.net p-ISSN 1895-2038 e-ISSN 1734-459X

ORIGINAL PAPER

CYBER SECURITY IN SUPPLY CHAIN MANAGEMENT: A SYSTEMATIC REVIEW

Mohd Nasrulddin Abd Latif[1] Nurul Ashykin Abd Aziz[2], Nik Syuhailah Nik Hussin[2], Zuraimi Abdul Aziz[2]

1) Politeknik Mukah Sarawak, Sarawak, **Malaysia**, 2) Universiti Malaysia Kelantan, Kelantan, **Malaysia**

ABSTRACT. **Background:** Cyber security of supply chain is a part of its safety measure that focuses on the management of the required cyber security that includes information technology systems, software, and networks. Supply chain management has a high risk of being threatened by cyber terrorism, malware and data-theft. Common supply chain cyber security activities are done to minimize risks including sole-purchase from trusted vendors, and disconnection of critical machines from external networks.
Methods: The main data sources for this study are research articles published from 2010 to 2020 in a peer-reviewed journal in the Web of Science and Scopus database. This study uses a systematic survey approach that is guided by PRISMA Statement, where the current study shows the trend of cyber research security in supply chain management.
Results: The final screening shows 41 identified related articles that are related to cyber security in supply chain management. This study also examined the publishing trends related to cyber security in supply chain management for both WOS and Scopus databases. The analysis shows that the highest publishing value was in 2019, coming from the Scopus database. In addition, four elements are covered in this study namely: (i) network security; (ii) information security; (iii) web application security and (iv) internet of things (IoT).
Conclusions: In brief, some suggestions are proposed to provide guidance for future researchers to study deeper about cyber security in supply chain management.

Key words: systematic review, supply chain, cyber security, network security, information security.

INTRODUCTION

Today, supply chain is becoming more complex and global. It is now increasingly dependent on information technology to increase its efficiency and to support communication and coordination between network suppliers, manufacturers, distributors, and even transportation service providers. Simultaneously, if information technology is not appropriately secured, it will increase supply chain vulnerability to cyber attacks [Kirk, 2014]. Raghavan, Desai and Rajkumar [2017] claimed that cyber security is frequently debated in the business industry from various angles, as recent violations show that every sector is exposed.

Furthermore, supply chain management needs to be carefully planned to get the right product, in the right quantity, and in the right place at the right time to reach the customers, and necessarily at the right price as claimed by [Mangan, Lalwani 2016]. As such, organizations digitize their operations to improve process efficiency and cost optimization [Shivajee et al., 2019]. Additionally, Shivajee et al. [2019] explained that the application of effective information technology tools ensures the organization's continued growth. Prominently, it regulates a set of techniques used to increase the security

Citation: *Latif M.N.A., Aziz N.A.A., Hussin N.S.N., Aziz Z.A., 2020. Cyber security in supply chain management: a systematic review. LogForum 17 (1), 49-57, http://doi.org/10.17270/J.LOG.2021.555*
Received: 21.10.2020, Accepted: 30.11.2020, on-line: 12.01.2021.

and integrity of a programme, network, and data from unauthorized and harmful access. Likewise, it refers to the process and technological body [Seemma, Nandhini, Sowmiya, 2018].

According to Miorandi et al. [2012], the supply chain is now consolidated between organizations through digital communication links due to digitization. In the supply chain, all members become the weakest because of the information and security arrangements that are shared throughout the supply chain. Meanwhile, Li et al. [2015], through their analysis found that information exchange, agility, and visibility increase through digital technology. However, there are some threats and risks that arise in this supply chain.

There are investigative reports made on data breaches where small organizations are often the target of cyber attacks due to their size in the supply chain. As such, larger companies are at risk of being exposed to specific threats, which have contracts with these small organizations to produce particular products [Verizon, 2014]. There is no denying that there is an increase in the number of attackers, but the tools available to the potential attackers are also becoming more sophisticated and active [Kizza, 2013; Koien, Oleshchuk, 2013]. Hence, Taneja [2013] highlighted that the use of the cyber medium and the internet could achieve its full potential if it thrives from cyber vulnerabilities and threats.

Yeboah-Ofori and Shareeful Islam [2019] described that cyber security within the supply chain provides organizations with secure network facilities to meet business objectives as a whole. Obviously, technological integration helps increase business processes, production productivity, and even reduce distribution costs. However, the increasing interdependence between the various supply chain stakeholders has created many challenges, including the lack of third-party audit mechanisms and cyber threats. This has also led to attacks such as design specification manipulation, changes, and manipulation during distribution activities. Hackers are also seen targeting web applications, as they have many networks. Thus, careful attention and monitoring can be done through firewalls and intrusion detection systems. In detail, the web application layer needs to be set up to ensure that it is safe from unauthorized users by developing high-quality security mechanisms for software development [Ge, Paige, Polack, Chivers, Brooke, 2006]. Web applications are an essential type of service provider and communication channel for their users. Vulnerability on the internet can have a detrimental effect and in turn, it affects all sensitive data.

The systematic literature review is an analysis of research questions formulated using systematic methods that aims to collect secondary data and efforts to identify, select and synthesize related studies to answer the research questions. To build a relevant systematic overview, the current article is guided by this key research question: "What is the focus field of cyber security in supply chain management?" This study's concentration is to explore areas that have been explored by previous studies in the context of cyber security in supply chain management, and this study also attempts to identify the trends of articles published in the last 10 years (2010-2020). Therefore, the focus of this study is to study this problem systematically.

METHODOLOGY

For the present study, the method used to obtain related articles of cyber security in supply chain management is discussed. Researchers have used key sources to search for associated articles from the Web of Science (WOS) and Scopus databases. Using the Preferred Reporting Items for Systematic Reviews and Meta-Analyzes (PRISMA) approach, the researchers conducted systematic reviews such as eligibility criteria and exclusions, process revision like introductory steps, examination and qualification. Next, it is followed by data abstraction and article analysis.

Research Design

Systematic literature review is outlined on the basis of important criteria from the

PRISMA checklists. Additionally, PRISMA's statement allows the search for terms related to cyber security in supply chain management. This is important to ensure that researchers have taken measures to reduce bias in design and revision response.

Sources of Data

For the present study, the researchers relied on two major journal databases: Web of Science (WoS) and Scopus. As claimed by Zhu [2020], WoS and Scopus are two of the world's leading and competing citation databases. The web-based Web of Science was launched in 1997, and the database was renamed as the "Web of Science Core Collection" in around 2014. Additionally, the Science Citation Index Expanded, Social Sciences Citation Index and Arts and Humanities Citation Index was originally developed in 1997 and its gradual coverage developed ever since [Liu, 2019; Rousseau et al., 2018]. According to Cision [2017], it was initially produced by the Institute of Scientific Information (ISI) and is now operated by Clarivate Analytics. Furthermore, the Web of Science's acceptable content is determined by the evaluation and selection process based on the following criteria: impact, influence, timelinessness, peer review, and geographical representation [Reuters, 2010].

Meanwhile, Scopus is an abstract database and a collection of Elsevier launched in 2004. All journals covered in the Scopus database, regardless of who they are published below, are reviewed annually to ensure that the high quality standards are maintained. Search in Scopus also incorporates patent database search. In addition, Scopus also provides four types of quality measurements for each title: h-Index, CiteScore, SCImago Journal Rank and Source Normalized Impact per Paper [Kulkarni, Aziz, Shams, Busse 2009].

Systematic Review Process

Based on Figure 1, four stages are involved in the systematic review process. The first stage is to identify the keywords used for the search process. Researchers refer to previous studies and the keywords "cyber security" and "supply chain" or "supply chain management" were used. The following are the requirements for the Scopus database: TITLE-ABS-KEY ("cyber security") AND TITLE-ABS-KEY ("supply chain" OR "supply chain management"). For the WoS database, the following terms are used: TS = ("cyber security") AND TS = ("supply chain" OR "supply chain management"). In the first stage of identification, after a careful screening, 33 duplicate articles were deleted. The second stage was screening; 153 articles were worth reviewing, and 82 articles were issued. The third level was eligibility, where the full articles were accessible. After careful examination, the amount of 74 articles was excluded for not focusing on cyber security in supply chain management, and they were not conceptual papers. They did not focus on the areas studied by the researchers. Next, the final stage that was surveys that showed 41 articles used for further analysis (Figure 1).

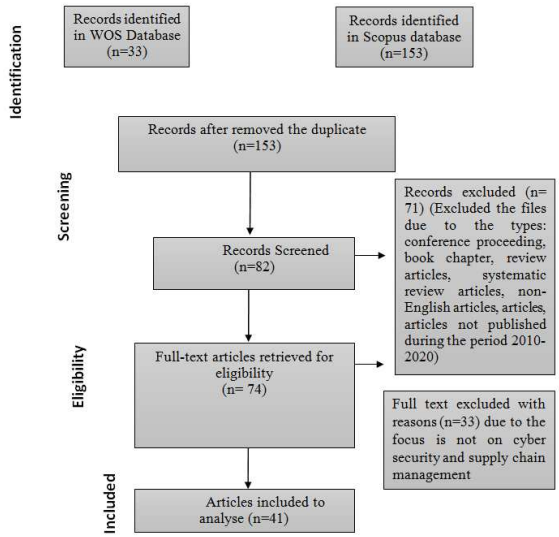

Fig. 1. Flow of the Systematic Review

Data Abstraction and Analysis

For data abstraction and analysis, the remaining articles were evaluated and analyzed by the researchers. The focus was on specific studies that could answer the research questions. The data was extracted using in-depth article reviews to obtain information related to the focus of each article.

Result and Discussion

The present study shows an overview of 41 articles that met the criteria set by the researchers for the purpose of the systematic review.

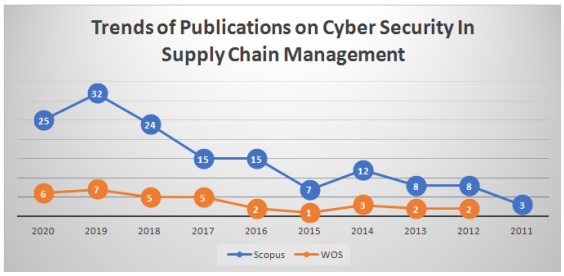

Fig. 2. Trend of Publications

The present study aims to systematically analyze the existing literatures on the outcomes of cyber security in supply chain management. The outcome should be entirely determined at the beginning of the supply chain management's activities to ensure that the outcomes were accessible. Referring to Figure 2, it was a trend of publication on cyber security in supply chain management. Compared to the two databases of Scopus and World of Science (WOS), the trend graph shows that most publications in the Scopus database were high. Next, 2019 shows the highest year data for published articles for these two databases where 32 articles were published in the Scopus database while 7 articles were published in the WOS database. Based on the researchers' observations, the trend of publications related to cyber security in supply chain management increased little by little every year starting in 2011, where there were only 3 publications in the Scopus database. In the following year, 2012 and so on, the number of publications increased unevenly, but related publications were still published. Overall, the publishing trend for this topic is growing and begins to be explored by researchers.

Analysis on Field of Study Covered in WOS and Scopus Databases

In the analysis of the entire final articles selected after screening, the researchers identified areas of studies related to cyber security in the context of supply chain management (Refer Figure 3). When most companies and businesses think about security, they often think about securing their digital networks, software, and assets from cyber attacks and data breaches. But, for the supply chains of whether traditional manufacturers or service providers, or data supply chains trusted by most large companies, they are also vulnerable to security risks. This is seen in many big data breaches through third parties. In practice, every company or business has a place in the supply chain, where the supply chain continues to grow on the flow of information such as the flow of goods and services. Therefore, it is not surprising that supply chain security is a very complex and continuously evolving function. Next, this shows that business executives pay more attention as the risks faced by information across the supply chain become increasingly apparent.

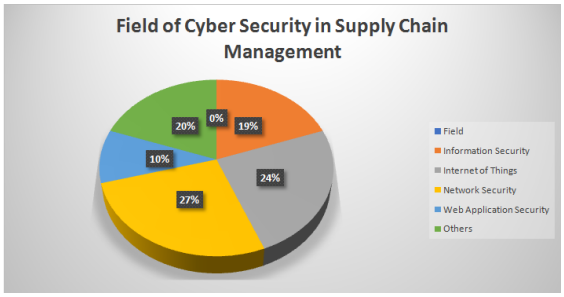

Fig. 3. Field of Study

Network Security

According to Figure 3, it shows that 27% of past studies were in network security (e.g. [Klos, Richardson, Corporation, 2013; Kshetri Voas, 2019; Pandey, Singh, Gunasekaran, Kaushik, 2020; Tamy, Belhadaoui, Rabbah, Rifi, 2020]. According to Gaigole and Kalyankar [2015], network security is an essential element for personal computer users as well as organizations. Besides, safety is the main concern due to the widespread use of the internet. There is no denying that the internet itself can pose some security threats. This can be explained when the intellectual property can be easily accessed through the internet, and there are many types of attacks that can be

transmitted over the network. There are differences in network security management for all types of situations, and it is necessary because the increased daily use of the internet includes home or office use, where it requires underlying security. However, large businesses require high maintenance, capable software, and sophisticated hardware to prevent hackers and scammers [SANS Technology Institute, 2020]. On the other hand, Gaigole and Kalyankar (2015) highlighted that network security should be a priority for the entire network, in order to stay awake and protected. Network security does not only focus on computer security at each end of the communication network, but it should also be monitored when sending data, as communication channels should not be vulnerable. This is because it will pose a greater threat. Hackers may intend to hack communication channels, obtain, manipulate data, and disseminate false information within the network.

Information Security

Next, Figure 3 shows that 19.5% of the past studies were in the field of information security [e.g. Boyson, 2014; Fernández-Caramés, Blanco-Novoa, Froiz-Míguez, Fraga-Lamas, 2019; Ram, Zhang, 2020]. Information security refers to a set of strategies for managing the tools, policies, and processes involved in detecting, preventing, and documenting. In addition, it is also to respond to threats to digital and non-digital information. The purpose of developing an information security programme is to protect the integrity, availability, and confidentiality of a business's data and information technology system. Among other things, it is also to ensure that sensitive information is disclosed only to the authorities, avoid manipulating invalid data, and confirm that the appropriate authorities can access the data when needed [Jain, Parashu, 2017]. The development of information security programmes aims to protect the integrity, availability, and confidentiality of business data systems and information technology.

Web Application Security

As reported in Figure 3, there were 9.8% previous studies in web applications [e.g. Osborn, Simpson, 2017, 2018; Polatidis, Pavlidis, Mouratidis, 2018]. Jain and Parashu [2017] explained that protection is required on any software used by the user. Each of these applications may contain holes or vulnerabilities in which an attacker can infiltrate user requests. Besides, application security includes software, hardware, and procedural methods to protect applications and avoid external threats. Among other things, aspects of application security also include actions taken during the development life cycle to protect applications from possible risks through vulnerabilities. It covers the design, development, use, upgrading, or maintenance of applications. Moreover, the security rules found in security forms and practices in the proper use of applications can minimize the risk of manipulating applications to steal data, hacking keywords to gain access, and controlling the data contained. Pandey and Singh [2020] classify cyber security risks into three categories: cyber security, supply risk, operational risk and demand risk. Cyber physical system has pushed global innovation into the daily operations of SC professionals. Web applications are an important type of service provider and communication channel for users. Vulnerability on the internet can create harmful effects and affect all sensitive data. Moreover, the main reason for this is that developers have limited programming skills and lack awareness of the importance of cyber security [Durai, Priyadharsini, 2014].

Internet of Things

The internet of things shows 24.4% of the past studies focusing on this area [e.g. Ardito, Petruzzelli, Panniello, Garavelli, 2019; Cheung, Bell, 2019; Gajek, Lees, Jansen, 2020; Urquhart, McAuley, 2018]. According to de Vass, Shee, and Miah [2018], the Internet of Things (IoT) is the next generation in an embedded ICT system connected to the internet network in a digital environment to integrate the supply chain, and logistics process to run smoothly. Additionally, the emerging IoT integration into the current ICT system can be unique because of its ingenuity.

Their study also found that IoT can positively and significantly impact the integration of internal processes, customers, and suppliers, which affects supply chain and organization performance. Mostafa, Hamdy, and Alawady [2018] highlighted that IoT is a new technology that enables the connection of several objects by collecting real-time data and sharing it; the information generated can then be used to support automated decision-making. Phase and Mhetre [2018] described that IoT infrastructure operates by assembling, delivering information to track the position, quality, and timely delivery of goods. IoT today is used to track goods and predict the situation to help protect and reduce losses. Multifaceted algorithms happen due to the different supply chains. Lastly, 19.5% of the statistics showed about other fields.

RECOMMENDATIONS FOR FUTURE RESEARCH

Based on the 41 final articles screened in the present study, the researchers found that future studies can meet some constraints. First and foremost, cyber security is an essential factor in today's supply chain management, but most studies do not explain it further. Researchers suggest that future studies explore more about web security elements other than those discovered in this study, namely web application security, internet of things, network security, and information security. By exploring other elements in future studies, they can explain more about the importance of establishing cyber security in supply chain management. Secondly, most past studies relied on keyword searching. This technique is the most commonly used form of text search on the web. Most search engines query and retrieve their texts using keywords [Rahman, 2013]. Nevertheless, another searching method includes citation searching. As claimed by Fasco [2004], savvy searching means citation searching. This search technique has long been used for decades. Moreover, Wright, Golder and Rodriguez-Lopez [2014] claimed that citation searching is an additional search method for systematic review and it is useful to confirm findings in other reviews. Hence, future studies are proposed to use this technique to explore more search articles in the field of cyber security in supply chain management.

CONCLUSION

In brief, this study presents a systematic review of existing literatures on the results of cyber security in supply chain management by reviewing study publications in the last ten years. The reviews were sourced from two databases namely Scopus and WoS, that produced 41 articles related to the field. This survey provides scholars' views on the importance of cyber security in supply chain management. From the present study, it shows that the trend of cyber security research in supply chain management is increasing and getting more attention from scholars. This present study discovered four main elements in cyber security: i) network security; ii) web application security; iii) internet of things; and iv) information security. Lastly, the majority of the past studies focused on network security. Therefore, many studies related to cyber security are needed in the future to provide more understanding about the importance of cyber security for supply chain management in an organization or business.

ACKNOWLEDGMENTS AND FUNDING SOURCE DECLARATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Ardito L., Petruzzelli A. M., Panniello U., Garavelli A.C., 2019. Towards Industry 4.0: Mapping digital technologies for supply chain management-marketing integration. Business Process Management Journal, 25(2), 323–346. http://doi.org/10.1108/BPMJ-04-2017-0088

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

http://doi.org/10.1016/j.technovation.2014.02.001

Cheung K.F., Bell M.G.H., 2019. Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research. http://doi.org/10.1016/j.ejor.2019.10.019

de Vass T., Shee H., Miah S.J., 2018. The Effect of "Internet of Things" on Supply Chain Integration and Performance: An Organisational Capability Perspective. Australasian Journal of Information Systems, 22, 1–29. http://doi.org/10.3127/ajis.v22i0.1734

Durai K.N., Priyadharsini K., 2014. A Survey on Security Properties and Web Application Scanner. International Journal of Computer Science and Mobile Computing, 3(10), 517–527.

Fasco P., 2004. Citation Searching. Online Information Review, 28(6), 454–460.

Fernández-Caramés T.M., Blanco-Novoa O., Froiz-Míguez I., Fraga-Lamas P., 2019. 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 (Basel, Switzerland), 19(10). http://doi.org/10.3390/s19102394

Gaigole M.S., Kalyankar M., 2015. The Study of Network Security With Its Penetrating Attacks and Possible Security Mechanisms. International Journal of Computer Science and Mobile Computing, 4(5), 728–735.

Gajek S., Lees M., Jansen C., 2020. IIoT and cyber-resilience: Could blockchain have thwarted the Stuxnet attack? AI and Society, (0123456789). http://doi.org/10.1007/s00146-020-01023-w

Ge X., Paige R., Polack F., Chivers H., Brooke P., 2006. Agile Development of Secure Web Applications. In The 6th International Conference on Web Engineering, 305–312. Palo Alto.

Jain J., Parashu R.P., 2017. A Recent Study over Cyber Security and its Elements. International Journal of Advanced Research in Computer Science, 8(3), 791–793.

Kizza J., 2013. Guide to Computer Network Security. Springer.

Klos S., Richardson J., Corporation S., 2013. Support Better Cyber Security.

Koien G., Oleshchuk V., 2013. Aspects of Persona Privacy in Communications-Problems, Technology and Solutions. River Publishers.

Kshetri N., Voas J., 2019. Supply chain trust. IT Professional, 21(2), 6–10. https://doi.org/10.1109/MITP.2019.2895423

Mostafa N.A., Hamdy W., Alawady H., 2018. Impacts of Internet of Things on Supply Chains: A Framework for Warehousing. Social Sciences (Special Industry 4.0 Implication for Economy and Society), 84, 1–10. http://doi.org/10.3390/socsci8030084

Osborn E., Simpson A., 2017. On small-scale IT users' system architectures and cyber security: A UK case study. Computers and Security, 70, 27–50. http://doi.org/10.1016/j.cose.2017.05.001

Osborn E., Simpson A., 2018. Risk and the Small-Scale Cyber Security Decision Making Dialogue - A UK Case Study. Computer Journal, 61(4), 472–495. http://doi.org/10.1093/comjnl/bxx093

Pandey S., Singh R.K., 2020. Cyber Security Risks In Globalized Supply Chains: Conceptual Framework. Cyber Security Risks. http://doi.org/10.1108/JGOSS-05-2019-0042

Pandey S., Singh R.K., Gunasekaran A., Kaushik A., 2020. Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103–128. http://doi.org/10.1108/JGOSS-05-2019-0042

Phase A., Mhetre N., 2018. Using IoT in Supply Chain Management. International Journal Pf Engineering and Techniques, 4(2), 973–979.

Polatidis N., Pavlidis M., Mouratidis H., 2018. Cyber-attack path discovery in a dynamic supply chain maritime risk management

system. Computer Standards and Interfaces, 56, 74–82. http://doi.org/10.1016/j.csi.2017.09.006

Rahman M., 2013. Search Engines Going Beyond Keyword Search: A Survey. International Journal Pf Computer Applications, 75, 1–8.

Ram J., Zhang Z., 2020. Belt and road initiative (BRI) supply chain risks: propositions and model development. International Journal of Logistics Management. http://doi.org/10.1108/IJLM-12-2019-0366

SANS Technology Instirute. (2020). Predictions and Trends for Information, Computer and Network Security. Retrieved from https://www.sans.edu/cyber-research

Seemma P. ., Nandhini S., Sowmiya M., 2018. Overview of Cyber Security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125–128. http://doi.org/10.17148/IJARCCE.2018.71127

Tamy S., Belhadaoui H., Rabbah N., Rifi M., 2020. Cyber security based machine learning algorithms applied to industry 4.0 application case: Development of network intrusion detection system using hybrid method. Journal of Theoretical and Applied Information Technology, 98(12), 2078–2091.

Taneja M., 2013. An Analytics Framework to Detect Compromised IOT Devices Using Mobility Behaviour. In ICT Convergence (ICTC) on. IEEE, 38–43.

Urquhart L., McAuley D., 2018. Avoiding the internet of insecure industrial things. Computer Law and Security Review, 34(3), 450–466. http://doi.org/10.1016/j.clsr.2017.12.004

Wright K., Golder S., Rodriguez-Lopez R., 2014. Citation Searching: A Systematic Review Case Study of Multiple Risk Behaviour Interventions. Medical Research Methodology, 14(73), 1–8.

Zhu J., 2020. A Tale of Two Databases: The Use of Web of Science and Scopus in Academic Papers. Forthcoming in Scientometrics.

BEZPIECZEŃSTWO CYBERNETYCZNE W ZARZĄDZANIU ŁAŃCUCHEM DOSTAW

STRESZCZENIE. **Wstęp:** Bezpieczeństwo cybernetyczne łańcucha dostaw jest częścią postępowania mającego na celu zapewnienie bezpieczeństwa, które skupia się na zarządzaniu bezpieczeństwem systemów technologicznych, oprogramowania i sieci. Zarządzanie łańcuchem dostaw jest zagrożone cyberatakami terrorystycznymi, złośliwym oprogramowaniem oraz kradzieżą danych. Działania obejmujące bezpieczeństwo cybernetyczne mają na celu minimalizację ryzyk, między innymi zakup tylko do zaufanych dostawców czy niepodłączanie krytycznych urządzeń od zewnętrznych sieci.
Metody: Praca oparta jest na przeglądzie publikacji naukowych z latach 2010-2020 w podlegających recenzji czasopismach z baz Web of Science i Scopus. Zastosowano metodo liczne podejście zgodne z zasadami PRISMA, ukazując trendy w dziedzinie bezpieczeństwa cybernetycznego w zarządzaniu łańcuchem dostaw.
Wyniki: Wyselekcjonowano 41 publikacji, których tematyka obejmuje bezpieczeństwo cybernetyczne w zarządzaniu łańcuchem dostaw. Przeanalizowano trendy w dziedzinie bezpieczeństwa cybernetycznego w zarządzaniu łańcuchem dostaw. Przeprowadzona analiza wykazała, że najwięcej publikacji ukazało się w 2019 w bazie Scopus. Dodatkowo, wyodrębniono cztery główne elementy badań: bezpieczeństwo sieci, bezpieczeństwo informacji, bezpieczeństwo aplikacji sieciowych oraz Internet rzeczy.

Wnioski: Sformułowano kilka sugestii, które mogą być wskazówkami do dalszych badań nad bezpieczeństwem cybernetycznym w zarządzaniu łańcuchem dostaw.

Słowa kluczowe: przegląd danych, łańcuch dostaw, bezpieczeństwo cybernetyczne, bezpieczeństwo sieci, bezpieczeństwo informacji

Mohd Nasrulddin Abd Latif
Department of Information Technology and Communication,
Politeknik Mukah Sarawak Km 7.5, Jalan Oya, 96400,
Mukah, Sarawak, **Malaysia**
email: nasrulddin@pmu.edu.my

Nurul Ashykin Abd Aziz
Universiti Malaysia Kelantan, Malaysia
Faculty of Entrepreneurship and Business
Locked Bag 36, Pengkalan Chepa,
16100, Kota Bahru, Kelantan, **Malaysia**
e-mail: ashykin.a@umk.edu.my

Nik Syuhailah Nik Hussin
Universiti Malaysia Kelantan, Malaysia
Faculty of Entrepreneurship and Business
Locked Bag 36, Pengkalan Chepa,
16100, Kota Bahru, Kelantan, **Malaysia**
e-mail: niksyuhailah@umk.edu.my

Zuraimi Abdul Aziz
Universiti Malaysia Kelantan, Malaysia
Faculty of Entrepreneurship and Business
Locked Bag 36, Pengkalan Chepa,
16100, Kota Bahru, Kelantan, **Malaysia**
e-mail: zuraimi@umk.edu.my