EPiC Series in Computing

Volume 97, 2024, Pages 9–19

Proceedings of 36th International Conference on Computer Applications in Industry and Engineering

Assessing the Implementation Challenges of Cybersecurity Solutions: An Enpirical Analysis

Le Vinh Quang [1,1*],Tran Huu Đuc[2,1†] and Narayan Chandra Debnath[3,1‡]

[1] Eastern International University, BinhDuong New City, Vietnam.

quang.le@eiu.edu.vn, duc.tran@eiu.edu.vn, narayan.debnath@eiu.edu.vn

Abstract

The implementation of cybersecurity measures in the manufacturing industry is crucial as organizations increasingly adopt digital technologies and face escalating cyber threats. This research paper aims to identify the challenges associated with implementing effective cyber security in the manufacturing industry and utilizes the Average Analytic Hierarchy Process (AHP) to evaluate and prioritize these challenges.

This research contributes to the existing knowledge by addressing the research gap regarding cyber security challenges in the manufacturing industry. The findings offer practical guidance for manufacturing organizations seeking to enhance their cyber security posture, enabling them to safeguard critical assets, ensure uninterrupted production processes, and protect sensitive information.

Keywords: Cybersecurity, Manufacturing industry, Average Analytic Hierarchy Process, AHP.

1 Introduction

The manufacturing industry has become increasingly reliant on digital technologies and interconnected systems, leading to unprecedented opportunities for growth and efficiency (da Costa Liberato et al., 2018). However, this digital transformation also introduces new vulnerabilities and risks, particularly in terms of cybersecurity (Bocayuva, 2021). As manufacturing organizations embrace Industry 4.0 technologies and digitize their operations, protecting critical assets, sensitive information, and ensuring uninterrupted production processes are critical concerns (Ahmed et al., 2023). The need

[*] Masterminded EasyChair and created the first stable version of this document

[†] Created the first draft of this document

[‡] Created the first draft of this document

to safeguard against cyber threats has never been more critical, given the potential consequences of successful attacks on the industry's infrastructure and operations (Kimani et al., 2019).

The rapidly evolving landscape of cyber threats presents an ongoing challenge for the manufacturing industry (Vaidya et al., 2018). As new technologies emerge and existing ones evolve, attackers continuously find novel ways to breach defenses (Zlomislić et al., 2017). This dynamic nature of cyber threats necessitates constant monitoring, updates, and adaptation of cybersecurity measures (Shetty et al., 2018), putting a strain on resources and requiring organizations to stay vigilant at all times.

Amidst the growing recognition of the significance of cybersecurity in the manufacturing sector (Ani et al., 2017), it is evident that there is a need for in-depth research that focuses specifically on the challenges faced in implementing effective cybersecurity solutions. While there is a burgeoning body of literature on cybersecurity, there is still a gap in research that delves into the unique context of the manufacturing industry and its distinct obstacles. Previous studies have often provided generalized approaches or overlooked the intricacies of securing industrial control systems, supply chains, and sensitive data in this sector (Cheung et al., 2021; Knowles et al., 2015; Raimundo & Rosário, 2022).

This research paper aims to address this critical gap by investigating the challenges of cybersecurity solutions implementation in the manufacturing industry. By leveraging the Average Analytic Hierarchy Process (AHP) as a decision-making method (Saaty, 2002), we intend to systematically evaluate and prioritize the identified challenges. The Average AHP approach allows for a quantitative analysis of the significance and impact of each challenge, providing valuable insights into the priorities for cybersecurity investments and mitigation strategies.

This study's primary contribution is to provide a comprehensive understanding of the obstacles manufacturers encounter while attempting to bolster their cybersecurity posture. By specifically focusing on the manufacturing sector, we aim to shed light on the nuances and complexities involved in securing digitalized operations and supply chains. Furthermore, the utilization of the Average AHP method enhances the rigor and objectivity of our analysis, enabling a more robust assessment of the challenges.

The remainder of this research paper is structured as follows. Section 2 provides a comprehensive review of the existing literature on cybersecurity challenges in the manufacturing industry. Section 3 outlines the research methodology, including data collection, identification of challenges, and the implementation of the Average AHP approach. Section 4 presents the findings and analysis of the identified challenges, highlighting their relative importance and implications. Section 5 discusses the implications of these challenges and provides recommendations for addressing them. Finally, Section 6 summarizes the key findings, contributions, and suggests avenues for future research in the field of cybersecurity in the manufacturing industry.

2 Literature review

In today's digital era, cybersecurity implementation has become paramount for organizations across diverse industries. The rapid adoption of Industry 4.0 technologies, cloud computing, and the Internet of Things (IoT) offers numerous benefits for growth and efficiency in the manufacturing sector. However, it also exposes manufacturers to a wide range of cyber threats, including ransomware attacks, data breaches, and industrial espionage. Thus, understanding the specific challenges in implementing effective cybersecurity solutions in manufacturing is essential to safeguard critical infrastructure and intellectual property.

The complexity of modern IT infrastructures poses significant challenges. The coexistence of legacy systems and cutting-edge technologies in sectors like manufacturing can lead to integration issues and cybersecurity compatibility concerns (Khan et al., 2022). Furthermore, the shortage of skilled cybersecurity professionals exacerbates the challenges faced by organizations, affecting both large

enterprises and small to medium-sized businesses (Horváth & Szabó, 2019). Compliance with regulations and standards is another ongoing concern for organizations in various sectors. Meeting industry-specific regulations and cybersecurity standards can be resource-intensive and complex, necessitating a comprehensive compliance strategy (Topping et al., 2021). The interconnected nature of supply chains and business ecosystems presents additional cybersecurity challenges. As organizations rely on third-party vendors, partners, and suppliers, potential entry points for cyberattacks increase, emphasizing the need for robust vendor risk management practices (Roy Sarkar, 2010).

Several research studies have explored the challenges faced by organizations when implementing cybersecurity measures. Some studies have identified common attack ways, such as insider threats, supply chain vulnerabilities, and weak access controls (Roy Sarkar, 2010; Tufail et al., 2021; Yeboah-Ofori & Islam, 2019), others have focused on specific manufacturing technologies, such as supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), and their unique cybersecurity challenges (Bhamare et al., 2020). The impact of cyber-attacks on manufacturing operations, such as production disruptions and financial losses, has also been examined (Bhamare et al., 2020).

However, a comprehensive assessment of challenges in the implementation of cyber security still needs further supplementation across various aspects beyond technology focus. Therefore, this study aims to identify and comprehensively evaluate these challenges by utilizing the research framework proposed by (Kabra et al., 2023), previously employed in identifying challenges in digital technology implementation.

The Analytical Hierarchy Process (AHP) is a widely recognized decision-making method that provides a structured approach to evaluate complex problems with multiple criteria (Albayrak & Erensal, 2004). In the context of cyber security challenges in manufacturing, AHP offers a valuable framework for quantitatively assessing the relative importance of different challenges. By involving experts in the industry and applying AHP, researchers can establish a priority ranking of challenges, enabling manufacturers to allocate resources effectively to address the most critical concerns. AHP is particularly valuable in the context of evaluating challenges in Information and Communication Technology (ICT) applications, as it provides a structured and systematic approach to assess the relative importance of these challenges based on multiple criteria (Kabra et al., 2023). Nevertheless, there are still limitations when utilizing the Analytic Hierarchy Process (AHP) technique to evaluate the challenges in the execution of cyber security.

3 RESEARCH METHODOLOGY

This study will employ the literature review method to identify the challenges. To assess these challenges, Average Analytic Hierarchy Process (AAHP) method will be utilized. AAHP method enables an effective analysis of the relative importance of various criteria, providing valuable insights into the decision-making process. Through this approach, the research aims to quantitatively assess and prioritize the challenges associated with cybersecurity implementation in the manufacturing industry, contributing to enhanced cybersecurity strategies for organizations in this sector.

3.1 AHP and Average AHP

Analytic Hierarchy Process (AHP) is a Multi-criteria decision-making (MCDM) technique proposed by (Wind & Saaty, 1980), which involves pairwise comparisons of multiple criteria to determine their relative importance. The AHP approach comprises four main steps:

AHP consists of a series of four stages:

1. Establishing the hierarchical structure of the model.
2. Gathering data through pairwise comparisons and measurements.

3. Computing normalized weights for each factor and scrutinizing these weights.
4. Developing solutions to address the problem.

In this research, we suggested the percentage scale (from 1 to 9) for the pair-wise comparison shown in Figure 1.

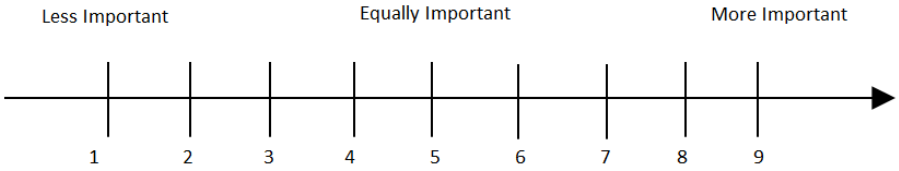

Figure 1: Figure 1 the percentage scale (from 1 to 9) for pair-wise comparisons

For each expert, AHP comparison tables are created to compute the relative weights of criteria, which are referred to as AHP values. If multiple experts (n experts) are involved, each expert's evaluation (AHPEi) is conducted, and the average AHP value of experts (A(AHP)) is calculated using the arithmetic mean, as represented in Equation 1.

$$A(AHP) = \frac{\sum_{i=1}^{n} AHPE_i}{n}$$

4 Results

4.1 Identifying challenges in Cyber security solutions implementation

In this study, we will build a multi-hierarchical structure of cyber security implementation challenges inspired by the technology adoption challenges identified by (Kabra et al., 2023). This structure will be further reinforced by incorporating insights from the most recent literature review on additive manufacturing adoption, along with input from 08 experts in the field including CEO, managers of IT Department of manufacturing companies, and ICT professors. The challenges related to cyber security implementation will be categorized into two levels, as presented in Table 1.

Main challenges	Sub challenges
Strategy (S)	Lack of policies to adopt technology
	Inadequate policy awareness and support from government
	Lack of management vision
	Lack of cross-organization development program
	Lack of supply chain understanding
Organisation (O)	Conflicting short-term focus goal-oriented culture
	Not inviting end-user input
	Lack of cyber security personnel
	Lack of pressure from other organizations
	Lack of transparency in the utilization of funds
Human (H)	Lack of education and training to the employees
	Lack of benchmarking about the knowledge of cybersecurity solutions
	Workforce resistance to change
	Lack of motivation to use cybersecurity solutions
	Lack of education and training to the employees
Finance (F)	Donors support
	Lack of funds for investment in technology
	High Cost
	Competition for funding
	Fundraising expenses
Technology (T)	Lack of awareness about exact technological solutions
	Lack of Cybersecurity solutions enabling infrastructure
	Lack of customization
	Frequent updates of technology
	Incompatibility in Cybersecurity facilities linked with different organizations

Table 1: Identification of challenge factors from the exisiting literature.

4.2 Prioritisation of Cyber security solutions challenges with A(AHP)

The A(AHP) questionnaire was designed to evaluate and prioritize the five key challenge factors and their related sub-factors. As previously stated, data was gathered using the A(AHP) questionnaire. The survey included the participation of eight cyber security specialists. The experts were instructed to use numerical scales ranging from 1 to 9 while making their choices to assess the priority of implementing cyber security. The questionnaire, which included a decision-making process and paired comparisons, took each participant between forty and fifty minutes to complete. Table 2 shows an example of paired choice criterion comparisons for a specific aim defined by expert No.1. Figure 1 depicts how significance was assigned on a scale of 1 to 9. As transverse values, the reciprocal values of these important ratings were employed (aij = 1/aji). Expert No. 1 came to the conclusion that Strategy was three times more significant than Organization, resulting in a transversal value of one-third. Similarly, Organization was regarded three times less significant than Strategy, resulting in an aij = 1/aji reciprocal ratio.

Criteria	S	O	H	F	T	S	O	H
S	1.00	3.00	9.00	7.00	5.00	1.00	3.00	9.00
O	0.33	1.00	7.00	5.00	3.00	0.33	1.00	7.00
H	0.11	0.14	1.00	0.33	0.20	0.11	0.14	1.00
F	0.14	0.20	3.00	1.00	1.00	0.14	0.20	3.00
T	0.20	0.33	5.00	1.00	1.00	0.20	0.33	5.00

Table 2: Pairwise comparison matrix of expert No. 1's decision criteria (challenge factors) with respect to the goals.

Table 3 shows how we built a pairwise comparison matrix of challenge factors by dividing each matrix member by the total of its corresponding columns. To compute 0.560 in the matrix, for example, we divided 1 (from Table 2) by the total of column values (1.00 + 0.33 + 0.11 + 0.14 + 0.20= 1.79) (from Table 2). By computing the row averages, we calculated the Eigenvectors or relative weights of the criteria (challenging factors) that fit with the purpose of Table 3. To demonstrate, the related weight of a strategic challenge was determined by dividing the total number of rows by the total number of rows. (0.560 + 0.642 + 0.360 + 0.488 + 0.490) in terms of the quantity of challenging factors/criteria (6), yielding a value of 0.508.

We estimated consistency indices (C.I.) and consistency ratios (C.R.) using Saaty (2004) criteria to assess the consistency of the comparison matrix. The C.I. is calculated as C.I. = (max - n) / (n - 1), where max is the biggest eigenvalue of the pairwise comparison matrix. The C.R. is calculated by dividing the C.I. by the random consistency index (R.I.), as shown in Table 4. The proper R.I. value for a five-by-five matrix is 1.12. The assessment is considered satisfactory if the C.R. is less than or equal to 0.1. Otherwise, create a new pairwise comparison matrix until the C.R. is less than or equal to 0.1 (Saaty, 2004). Using the aforementioned technique, we calculated the C.R., which was 0.072348987, which did not exceed the 0.10 (10 percent) criterion. As a consequence, the experts' judgments were relatively consistent and might lead to an appropriate choice for these criteria.

n	1	2	3	4	5	6	7	8	9	10
R.I	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49
n	11	12	13	14	15					
R.I	1.51	1.48	1.56	1.57	1.58					

Table 4: Average random consistency index (R.I.).

The A(AHP) technique was used by eight experts to compare each adoption obstacle in Figure 2 to itself. The average score was used to determine the priority of each adoption challenge level, as shown in Table 5. The arithmetic mean of the experts' A(AHP) values was used to get the average AHP value A(AHP). To demonstrate, the average AHP of the strategic challenge in the table was calculated by adding the rows (0.508+ 0.508+ 0.529+ 0.264 + 0.035 + 0.070 + 0.508 + 0.260), yielding a result of

0.335 and placing second. Table 6 summarizes the outcomes of all challenge elements' priority, including the major and sub-challenges.

	Criteria weights									
	RES 1	RES 2	RES 3	RES 4	RES 5	RES 6	RES 7	RES 8	Averg	Rank
SC	0.508	0.508	0.529	0.264	0.035	0.070	0.508	0.260	0.335	2
OC	0.265	0.264	0.185	0.505	0.503	0.502	0.264	0.503	0.374	1
HC	0.035	0.070	0.038	0.137	0.068	0.039	0.070	0.035	0.061	5
FC	0.082	0.038	0.077	0.045	0.134	0.223	0.038	0.068	0.088	4
TC	0.110	0.120	0.170	0.049	0.260	0.166	0.120	0.134	0.141	3

Table 5: Average of the AHP values of the experts for major challenges.

Criteria	**Weights**	**Ranks**
Main Factors		
Strategic Challenges	0.335	2
Organisational Challenges	0.374	1
Human Challenges	0.061	5
Financial Challenges	0.088	4
Technological Challenges	0.141	3
Sub-Challenge Factors (Strategic)		
Lack of policies to adopt technology	0.162	4
Inadequate policy awareness and support from government	0.102	5
Lack of management vision	0.209	3
Lack of cross-organization development program	0.289	1
Lack of supply chain understanding	0.239	2
Sub-Challenge Factors (Organisational)		
Conflicting short-term focus goal-oriented culture	0.207	2
Not inviting end-user input	0.160	5
Lack of cybersecurity personnel	0.207	3
Lack of pressure from other organisations	0.237	1
Lack of transparency in the utilisation of funds	0.188	4
Sub-Challenge Factors (Human)		
Lack of skills to use cybersecurity	0.258	2
Lack of education and training to the employees	0.168	4
Lack of benchmarking about the knowledge of cybersecurity	0.188	3
Workforce resistance to change	0.272	1
Lack of motivation to use cybersecurity	0.115	5
Sub-Challenge Factors (Financial)		
Donors support	0.209	2
Lack of funds for investment in technology	0.339	1
High Cost	0.111	5
Competition for funding	0.162	4
Fundraising expenses	0.179	3

Sub-Challenge Factors (Tecnological)		
Lack of awareness about exact technological solutions	0.219	2
Lack of cybersecurity enabling infrastructure	0.175	4
Lack of customization	0.138	5
Frequent updates of technology	0.259	1
Incompatibility in cybersecurity facilities linked with different organisations	0.209	3

Table 6: Average of the AHP values of the experts for major challenges.

5 Conclusions and discussion

This study presented five main challenges and 25 sub-challenges by using adopting digital technology framework.

The most significant challenge in the process of implementing Cybersecurity solutions is the organizational challenges. This study shows that a lack of pressure from external organizations could reduce the deployment of cybersecurity solutions less urgent. Insufficient incentive from peer organizations may diminish the prioritization and significance of cybersecurity implementation. These findings are supported by Kabanda et al. (2018), who emphasize that external factors further reinforce the limited adoption of cybersecurity practices.

The findings of this study closely match with the earlier research conducted in small and medium-sized enterprises (SMEs) across developing countries. SMEs frequently operate with simpler systems, which might pose challenges in adopting rigorous cybersecurity protocols (Rawindaran et al., 2023). The absence of intricate business operations and outdated legacy systems is regarded as a favorable aspect in this scenario. The impact of the cybersecurity environment in developing nations on cybersecurity practices has been observed to demonstrate a strong and enduring influence.

Compared to studies focusing on technology application in manufacturing, one of the significant implementation challenges pertains to financial or strategic considerations (Kabra et al., 2023). However, this present study reveals that financial challenge ranks only fourth. This implies that the market offers a considerable array of cybersecurity solutions, suggesting that financial constraints may not be a major hindrance for businesses in adopting these solutions.

Building upon the insights gained from this study, several avenues for future research in the realm of cybersecurity implementation and organizational challenges can be explored: Investigate further the role of external pressures from organizations and stakeholders in driving the urgency of cybersecurity solutions implementation. Delve into the specific mechanisms through which such external influences impact the decision-making processes and prioritization of cybersecurity initiatives within enterprises. Explore holistic approaches that address both organizational challenges and external influences in tandem. Investigate strategies for fostering collaboration among peer organizations to collectively elevate the importance of cybersecurity implementation and to share best practices.

Acknowledgments – This research is financially supported by Eastern International University, Binh Duong Province, Vietnam

References

Ahmed, S. F., Alam, M. S. Bin, Hoque, M., Lameesa, A., Afrin, S., Farah, T., Kabir, M., Shafiullah, G. M., & Muyeen, S. M. (2023). Industrial Internet of Things enabled technologies, challenges, and future directions. *Computers and Electrical Engineering*, *110*(July), 108847. https://doi.org/10.1016/j.compeleceng.2023.108847

Albayrak, E., & Erensal, Y. C. (2004). Using analytic hierarchy process (AHP) to improve human performance: An application of multiple criteria decision making problem. *Journal of Intelligent Manufacturing*, *15*(4), 491–503. https://doi.org/10.1023/B:JIMS.0000034112.00652.4c

Ani, U. P. D., He, H. (Mary), & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers and Security*, *89*(November). https://doi.org/10.1016/j.cose.2019.101677

Bocayuva, M. (2021). Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *WMU Journal of Maritime Affairs*, *20*(2), 173–192. https://doi.org/10.1007/s13437-021-00240-4

Cheung, K. F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*(July 2020), 102217. https://doi.org/10.1016/j.tre.2020.102217

da Costa Liberato, P. M., Alén-González, E., & de Azevedo Liberato, D. F. V. (2018). Digital Technology in a Smart Tourist Destination: The Case of Porto. *Journal of Urban Technology*, *25*(1), 75–97. https://doi.org/10.1080/10630732.2017.1413228

Horváth, D., & Szabó, R. Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? *Technological Forecasting and Social Change*, *146*(March), 119–132. https://doi.org/10.1016/j.techfore.2019.05.021

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kabra, G., Ramesh, A., Jain, V., & Akhtar, P. (2023). Barriers to information and digital technology adoption in humanitarian supply chain management: a fuzzy AHP approach. *Journal of Enterprise Information Management*, *36*(2), 505–527. https://doi.org/10.1108/JEIM-10-2021-0456

Khan, B. S., Jangsher, S., Ahmed, A., & Al-Dweik, A. (2022). URLLC and eMBB in 5G Industrial IoT: A Survey. *IEEE Open Journal of the Communications Society*, *3*(July), 1134–1163. https://doi.org/10.1109/OJCOMS.2022.3189013

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. *Applied Sciences (Switzerland)*, *12*(3). https://doi.org/10.3390/app12031598

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights*, *3*(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, *15*(3), 112–133. https://doi.org/10.1016/j.istr.2010.11.002

Saaty, T. L. (2002). Decision making with the Analytic Hierarchy Process. *Scientia Iranica*, *9*(3), 215–229. https://doi.org/10.1504/ijssci.2008.017590

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management†. *Geneva Papers on Risk and Insurance: Issues and Practice*, *43*(2), 224–238. https://doi.org/10.1057/s41288-018-0078-3

Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers and Security*, *108*. https://doi.org/10.1016/j.cose.2021.102324

Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies*, *14*(18), 1–22. https://doi.org/10.3390/en14185894

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 - A Glimpse. *Procedia Manufacturing*, *20*, 233–238. https://doi.org/10.1016/j.promfg.2018.02.034

Wind, Y., & Saaty, T. L. (1980). 8002_Marketing_Applications_of_the_Analytic.pdf. In *Management Science* (Vol. 26, Issue 7, pp. 641–658).

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future Internet*, *11*(3). https://doi.org/10.3390/fi11030063

Zlomislić, V., Fertalj, K., & Sruk, V. (2017). Denial of service attacks, defences and research challenges. *Cluster Computing*, *20*(1), 661–671. https://doi.org/10.1007/s10586-017-0730-x