



**ENHANCING CYBERSECURITY IN LOGISTICS
SERVICES: A STUDY OF THIRD-PARTY LOGISTICS
(3PL) SERVICE PROVIDERS**

BARIŞ CAN GENÇ

Thesis for the Master's Program in Logistics Management

Graduate School
Izmir University of Economics

Izmir

2025

**ENHANCING CYBERSECURITY IN LOGISTICS
SERVICES: A STUDY OF THIRD-PARTY LOGISTICS
(3PL) SERVICE PROVIDERS**

BARIŞ CAN GENÇ

THESIS ADVISOR: ASSOC. PROF. DR. AYSU GÖÇER

Master's Exam Jury Members
Prof. Dr. Bengü Sevil OFLAÇ
Assoc. Prof. Dr. Aysu GÖÇER
Asst. Prof. Dr. Tunca TABAKLAR

A Master's Thesis
Submitted to
the Graduate School of Izmir University of Economics
the Department of Logistics Management

Izmir
2025

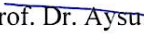
Approval of the Graduate School

Prof. Dr. Mehmet Efe BİRESSELİOĞLU

I certify that this thesis satisfies all the requirements as a thesis for a Master's degree.

 Prof. Dr. Özgür ÖZPEYNİRCİ

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for a Master's degree.

 Assoc. Prof. Dr. Aysu GÖÇER

Master's Exam Jury Members

Prof. Dr. Bengü Sevil OFLAÇ
Izmir University of Economics

Assoc. Prof. Dr. Aysu GÖÇER
Izmir University of Economics

Asst. Prof. Dr. Tunca TABAKLAR
Izmir Katip Celebi University

ETHICAL DECLARATION

I hereby declare that I am the sole author of this thesis and that I have conducted my work in accordance with academic rules and ethical behaviour at every stage from the planning of the thesis to its defence. I confirm that I have cited all ideas, information and findings that are not specific to my study, as required by the code of ethical behaviour, and that all statements not cited are my own.

Name, Surname: Barış Can GENÇ

Date: 10.06.2025

Signature:

ABSTRACT

ENHANCING CYBERSECURITY IN LOGISTICS SERVICES: A STUDY OF THIRD-PARTY (3PL) LOGISTICS SERVICE PROVIDERS

Genç, Barış Can

Master's Program in Logistics Management

Advisor: Assoc. Prof. Dr. Aysu GÖÇER

June, 2025

Supply chains consist of interconnected stakeholders that continuously exchange information and data to maintain operations. With the Industry 4.0 technologies, managing large volumes of critical data has become easier, significantly improving operational efficiency and transparency in logistics and supply chain sectors. However, they have also exposed supply chain networks to various cybersecurity threats. If one member of a supply chain lacks sufficient security, vulnerabilities can spread across the entire system due to its interconnected structure. As companies increasingly delegate logistics operations to 3PL providers, cybersecurity risks are inevitably transferred to these providers. This study aims to uncover the impacts of cyberattacks on 3PL service providers and examine the potential ripple effects on both individual stakeholders and the overall supply chain network, and to come up with mitigation strategies to mitigate these impacts and cyberattacks. Content analysis was used to examine the data collected from semi-structured interviews with eighteen key stakeholders and Systems Theory is used in the study. The findings reveal that

cyberattacks on 3PL service providers disrupt not only their operations but also the entire supply chain, affecting all stakeholders. These attacks cause short-term disruptions such as data compromise and operational delays, as well as long-term consequences such as loss of customer trust, disruption of relationships, and significant financial losses. In addition, it is seen that the ripple effects on all stakeholders can be prevented and reduced when the mitigation strategies we uncovered are implemented, and ultimately, the overall stability of the supply chain can be increased.

Keywords: Cybersecurity, Third-Party Logistics (3PL), Ripple Effects, Supply Chain Resilience, Systems Theory, Cyberattacks.



ÖZET

LOJİSTİK HİZMETLERİNDE SİBER GÜVENLİĞİN ARTIRILMASI: ÜÇÜNCÜ TARAF (3PL) LOJİSTİK HİZMET SAĞLAYICILARI ÜZERİNE BİR ÇALIŞMA

Genç, Barış Can

Lojistik Yönetimi Yüksek Lisans Programı

Tez Danışmanı: Doç. Dr. Aysu GÖÇER

Haziran, 2025

Tedarik zincirleri doğası gereği, operasyonların sürdürülebilirliğini sağlamak için sürekli olarak bilgi ve veri alışverişinde bulunan birbirine bağlı paydaşlardan oluşur. Endüstri 4.0 teknolojilerinin ortaya çıkmasıyla birlikte, büyük hacimli kritik verilerin yönetimi kolaylaşmış, bu da lojistik ve tedarik zinciri sektörlerinde operasyonel verimlilik ve şeffaflığı önemli ölçüde artırmıştır. Ancak, bu teknolojiler verimlilik sağlarken aynı zamanda tedarik zinciri ağlarını çeşitli siber güvenlik tehditlerine karşı savunmasız hale getirmiştir. Tedarik zincirinin bir üyesinin yeterli güvenliğe sahip olmaması, yapının birbirine bağlı doğası nedeniyle tüm sistemi etkileyebilecek açıkların ortaya çıkmasına yol açabilir. Şirketlerin lojistik operasyonlarını giderek daha fazla üçüncü taraf lojistik (3PL) hizmet sağlayıcılarına devretmesiyle birlikte, siber güvenlik riskleri kaçınılmaz olarak bu sağlayıcılara da aktarılmaktadır. Bu çalışma, 3PL hizmet sağlayıcılarına yönelik siber saldırıların etkilerini ortaya koymayı ve hem bireysel paydaşlar hem de genel tedarik zinciri ağı üzerindeki olası dalga etkilerini incelemeyi, ayrıca bu etkileri ve siber saldırıları azaltmaya yönelik etkili stratejiler geliştirmeyi amaçlamaktadır. Çalışmada, on sekiz kilit paydaşla yapılan yarı

yapılandırılmış görüşmelerden elde edilen veriler içerik analizi yöntemiyle incelenmiş ve araştırmanın kuramsal çerçevesi Sistem Teorisi ile oluşturulmuştur. Bulgular, 3PL hizmet sağlayıcılarına yönelik siber saldırıların yalnızca bu firmaların operasyonlarını değil, tüm tedarik zincirini ve tüm paydaşları etkilediğini ortaya koymaktadır. Bu saldırılar, veri ihlalleri ve operasyonel gecikmeler gibi kısa vadeli aksaklıkların yanı sıra, müşteri güveninin kaybı, ilişki bozulmaları ve önemli mali kayıplar gibi uzun vadeli sonuçlara da yol açmaktadır. Ayrıca, sektör uzmanlarının görüşleriyle ortaya konan önleyici stratejilerin uygulanması durumunda tüm paydaşlar üzerindeki olumsuz etkilerin önlenebileceği veya azaltılabileceği ve nihayetinde tedarik zincirinin genel istikrarının artırılabilceği görülmektedir.

Anahtar Kelimeler: Siber Güvenlik, Üçüncü Taraf Lojistik (3PL), Dalga Etkileri, Tedarik Zinciri Dayanıklılığı, Sistem Teorisi, Siber Saldırıları.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my thesis supervisor, Assoc. Prof. Dr. Aysu Göçer, for her invaluable guidance, support, and encouragement throughout this research. I am also thankful to all participants who contributed their time and insights during the interviews. Lastly, I would like to thank my family and friends for their endless support and motivation during this journey.



TABLE OF CONTENTS

ABSTRACT	iv
ÖZET.....	vi
ACKNOWLEDGEMENTS	viii
TABLE OF CONTENTS.....	ix
LIST OF TABLES	xii
LIST OF FIGURES.....	xiv
LIST OF ABBREVIATIONS	xv
CHAPTER 1: INTRODUCTION	1
1.1. Background	1
1.2. Problem Statement	3
1.3. Significance of the Thesis	6
1.4. Aims and Objectives of The Thesis	8
CHAPTER 2: LITERATURE REVIEW	10
2.1. Supply Chain and Technology Adoption.....	10
2.1.1. Supply Chain Security Issues related to Technology Adoption.....	13
2.1.1.1. Insider Threats	14
2.1.1.2. Blockchain Technology (BCT) and Threats.....	16
2.1.1.3. Artificial Intelligence (AI), Internet of Things (IoT) and Threats	18
2.2. Overview of Cybersecurity in Supply Chain and Logistics.....	21
2.2.1. Common Types of Cyberattacks Seen in Supply Chain and Logistics	24
2.2.1.1. Distributed Denial of Service (DDOS).....	24
2.2.1.2. Malware	25
2.2.1.3. Hardcoded Credentials.....	26
2.2.1.4. Phishing	26
2.3. The Role and Importance of 3PL Service Providers in Cybersecurity and Their Impact on Supply Chain Stakeholders	27

CHAPTER 3: THEORETICAL BACKGROUND OF THE STUDY	37
CHAPTER 4: METHODOLOGY	43
4.1. Semi-Structured Interview	43
4.1.1. Sample of Interviews.....	47
4.1.2. Content Analysis Method.....	53
CHAPTER 5. FINDINGS.....	56
5.1 Ripple Effects on Cyberattacks on 3PL	56
5.1.1. Employee Impacts	59
5.1.2. Financial Impacts	60
5.1.3. Information Security Impacts.....	64
5.1.4. Legal Impacts	66
5.1.5. Operational Impacts	67
5.1.6. Reputational Impacts.....	70
5.1.7. Industrial Impacts.....	72
5.1.8. Information Sharing Impacts.....	74
5.1.9 Societal Impacts	75
5.2. The Ripple Impacts of Cyberattacks on Key Stakeholders.....	77
5.3. Detailed Impacts by Stakeholder	78
5.3.1. Detailed Impacts on 3PLs	83
5.3.2. Detailed Impacts on Importer and Exporters	89
5.3.3. Detailed Impacts on Ports	96
5.3.4. Detailed Impacts on Customs.....	102
5.3.5. Detailed Impacts on Shipowners.....	105
5.3.6. Detailed Impacts on Retailers	106
5.4 Mitigating the Ripple Effects of Cybersecurity Issues Along a Supply Chain	107
5.4.1. Employee Related Mitigation Strategies to Reduce Employee Impacts	107
5.4.2. Industrial Mitigation Strategies.....	115
5.4.3. Information Security Strategies.....	123
5.4.4. Mitigation Strategies for Information Sharing Impacts	134
5.4.5. Legal Mitigation Strategies	144

5.4.6. Operational Mitigation Strategies	147
5.4.7. Reputational Mitigation Strategies.....	153
CHAPTER 6. CONCLUSION.....	156
6.1. Academic and Practical Implications.....	157
6.2. Limitations and Further Research	161
REFERENCES.....	163
APPENDICES.....	179



LIST OF TABLES

Table 1. Sample Size of Interviews.....	46
Table 2. Profile of the Interviewees.	48
Table 3. Short and Long Term Ripple Effects.	57
Table 4. Codes and Participant Responses of Employee Impacts.	60
Table 5. Codes and Participant Responses of Financial Impacts.....	61
Table 6. Codes and Participant Responses of Information Security Impacts.	64
Table 7. Codes and Participant Responses of Legal Impacts.....	67
Table 8. Codes and Participant Responses of Operational Impacts.....	67
Table 9. Codes and Participant Responses of Reputational Impacts.	71
Table 10. Codes and Participant Responses of Industrial Impacts.	73
Table 11. Codes and Participant Responses of Information Sharing Impacts.	74
Table 12. Codes and Participant Responses of Societal Impacts.....	76
Table 13. Impacts of Cyberattacks on Stakeholders.	77
Table 14. Detailed Impacts on Stakeholders.....	79
Table 15. Illustrative Quotes About Employee Impacts on 3PLs.....	83
Table 16. Illustrative Quotes About Financial Impacts on 3PLs.	84
Table 17. Illustrative Quotes About Industrial Impacts on 3PLs.....	86
Table 18. Illustrative Quotes About Information Sharing Impacts on 3PLs.....	87
Table 19. Illustrative Quotes About Operational Impacts on 3PLs.	88
Table 20. Illustrative Quotes About Reputational Impacts on 3PLs.....	89
Table 21. Illustrative Quotes About Employee Impacts on Importers and Exporters.	90
Table 22. Illustrative Quotes About Financial Impacts on Importers and Exporters.	90
Table 23. Illustrative Quotes About Industrial Impacts on Importers and Exporters.	91
Table 24. Illustrative Quotes About Information Security Impacts on Importers and Exporters.	92
Table 25. Illustrative Quotes About Information Sharing Impacts on Importers and Exporters.	94
Table 26. Illustrative Quotes About in Operational Impacts on Importers and Exporters.	94

Table 27. Illustrative Quotes About in Reputational Impacts on Importers and Exporters.	96
Table 28. Illustrative Quotes About Employee Impacts on Ports.	96
Table 29. Illustrative Quotes About Financial Impacts on Ports.	97
Table 30. Illustrative Quotes About Information Security Impacts on Ports.	98
Table 31. Illustrative Quotes About Information Sharing Impacts on Ports.	99
Table 32. Illustrative Quote About Legal Impacts on Ports.	99
Table 33. Illustrative Quotes About Operational Impacts on Ports.	100
Table 34. Illustrative Quotes About Reputational Impacts on Ports.	102
Table 35. Illustrative Quotes About Financial Impacts on Customs.	103
Table 36. Illustrative Quotes About Information Security Impacts on Customs.	103
Table 37. Illustrative Quotes About Operational Impacts on Customs.	104
Table 38. Illustrative Quotes About Reputational Impacts on Shipowners.	106
Table 39. Illustrative Quotes About Reputational Impacts on Retailers.	107
Table 40. Employee Related Mitigation Strategies and Illustrative Quotes Aimed at Preventing Ripple Effects on Employees.	110
Table 41. Mitigation Strategies and Illustrative Quotes to Mitigate Industrial Ripple Effects.	118
Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects.	128
Table 43. Mitigation Strategies and Illustrative Quotes to Mitigate Information Sharing Ripple Effects.	139
Table 44. Mitigation Strategies and Illustrative Quotes to Mitigate Legal Ripple Effects.	145
Table 45. Mitigation Strategies and Illustrative Quotes to Mitigate Operational Ripple Effects.	150
Table 46. Mitigation Strategies and Illustrative Quotes to Mitigate Reputational Ripple Effects.	155

LIST OF FIGURES

Figure 1. Taxonomy of cyberattacks for supply chain links (Hammi, Zeadally and Nebhen, 2023). Reproduced with permission from Hammi, Zeadally and Nebhen (2023). ©Association for Computing Machinery.	27
Figure 2. “Domino effect” impact of cybersecurity in supply chains (Levy and Gafni, 2021). Reproduced with permission from Levy and Gafni (2021). © 2020 Emerald Publishing Limited.	35
Figure 3. Generic Supply Chain Model (Caddy and Helou, 2007). Reproduced with permission from Caddy and Helou (2007). © 2007 Elsevier.....	39
Figure 4. Method descriptions for RQs.....	43
Figure 5. The ripple effects of cyberattacks on 3PL service providers.....	77

LIST OF ABBREVIATIONS

3PL: Third Party Logistics

AEO: Authorized Economic Operator

AI: Artificial Intelligence

BCT: Block Chain Technology

C-TPRM: Cyber Third Party Risk Management

CIMS: Computer Integrated Manufacturing Systems

CISA: Cybersecurity and Infrastructure Security Agency

CSCRM: Cyber Supply Chain Risk Management

CTPAT: Customs-Trade Partnership Against Terrorism

DDoS: Distributed Denial of Service

DSC: Digital Supply Chain

EDI: Electronic Data Interchange

ENISA: European Network and Information Security Agency

ERP: Enterprise Resource Planning

FMS: Flexible Manufacturing Systems

GNSS: Global Navigation Satellite Systems

ICT: Information Communication Technology

IDS: Intrusion Detection Systems

IoT: Internet of Things

IT: Information Technology

ITRC: Identity Theft Resource Center

JIT: Just In Time

ML: Machine Learning

NIST: National Institute of Standards and Technology

OBM: Original Brand Manufacturer

OR/MS: Operation Research/Management Science

PRISMA: Preferred Systematic Reviews and Meta-Analysis

RFID: Radio Frequency Identification

RQ: Research Question

SANS: SysAdmin, Audit, Network, and Security

SCD: Supply Chain Disruption

SCM: Supply Chain Management

SFTP: Secure File Transfer Protocols

SLR: Systematic Literature Review

TMS: Transportation Management Systems

VPN: Virtual Private Network

VR: Virtual Reality

WMS: Warehouse Management Systems

CHAPTER 1: INTRODUCTION

1.1. Background

In today's global business world, logistics and supply chain management (SCM) are the basic components that make up global trade. Therefore, the efficiency and reliability of the supply chain and the logistics systems involved are of critical importance in ensuring that goods and services are delivered to the end user at the right time, in the right condition and at the right cost. The use of third-party logistics (3PL) service providers within the supply chain ecosystem has increased and they have now begun to take on more strategic roles (Zacharia, Sanders and Nix, 2011). These providers facilitate the operations of companies in the supply chain, increase flexibility, and reduce costs by providing services such as storage, transportation, distribution and order fulfillment (Selviaridis and Spring, 2007). With the technologies that emerged with Industry 4.0, a recent revolution, the logistics industry has experienced significant improvements in terms of operational efficiency, transparency and overall performance increase. The integration of technologies such as digital platforms, cloud, internet of things (IoT), blockchain, artificial intelligence (AI), radio frequency identification (RFID) into operations has initiated a new phase in the logistics industry (Ugochukwu, Goyal and Arumugam, 2022). However, due to the increasing dependence on digital technologies and interconnected systems and the centralized database structures of these technologies, logistics and supply chain networks have been exposed to numerous cybersecurity threats (Ugochukwu, Goyal and Arumugam, 2022). Other reasons that cause the supply chain and logistics sector to become a target are: Logistics operations involve the sharing of private consumer information (name, address, phone number, and bank account information) and product information among logistics players (manufacturers, suppliers, transportation service providers, customs agencies, ports, exporters, importers and customers). And the involvement of so many logistics stakeholders raises privacy and security concerns about private information because customer information and product details are exchanged and shared across numerous logistics stakeholders during the logistics process (Ugochukwu, Goyal and Arumugam, 2022).

For the above reasons, the importance of increasing cybersecurity in logistics is undeniable. In this regard, 3PL service providers, who form the veins of the system by

acting as a bridge between networks in logistics operations within the supply chain, play a key role. Supply chain firms, such as 3PL providers, rely on a constant flow of data to operate effectively (Choy et al., 2008). 3PLs and their clients rely on daily access to massive amounts of crucial data, making them particularly vulnerable and attractive targets. There are other reasons why supply chain and 3PL organizations are at greater risk. The supply chain is, by definition, a network of connected partners, frequently a diverse group of enterprises linked together by common information. Supply chain firms rely largely on connection for mission-critical operations, yet many still use obsolete systems and technologies. This renders supply chains and 3PL service providers more exposed to hacks (Meggiato et al., 2022). To remain competitive, organizations are outsourcing their logistical activities to 3PL providers as the new global economic landscape emerges (Hsiao et al., 2010; Li et al., 2012). As more businesses outsource their logistics to 3PLs, supply chain risks and uncertainties are passed to these providers (Gkanatsas and Krikke, 2020). In another study, it was stated that although logistics activities are an inevitable reality in supply chains, cybersecurity in logistics is often ignored and the lack of studies on cybersecurity in the field of logistics is also mentioned (Cheung, Bell and Bhattacharjya, 2021). A statistic that reveals the importance of 3PL service providers states that more than 60% of cybersecurity breaches in supply chains originate from suppliers or 3PL (Simon and Omar, 2020). Cyberattacks were carried out via third-party suppliers or service providers against companies like Target, Home Depot, Fiat Chrysler, Costco, and Sam's Club (Simon and Omar, 2020). Cybercriminals exploited ransomware, malware, hacking, and computer viruses via third-party suppliers to enable illegal activity on IT hardware and software of supply chain organizations and obtain access to targeted business (Dhillon and Backhouse, 1996; Urciuoli and Hints, 2017).

In this context, the thesis aims to bridge this knowledge gap by investigating the potential ripple effects of cyberattacks on 3PL service providers throughout the supply chain. This study aims to highlight the importance of strong cybersecurity measures in ensuring the resilience and continuity of logistics services by examining how such attacks affect the supply chain and its stakeholders. Additionally, by identifying and implementing effective mitigation strategies, this research aims to protect critical infrastructure and thereby maintain the uninterrupted flow of goods and services vital to economic stability and growth.

1.2. Problem Statement

Meggiato et al (2022) stated that the supply chain management (SCM) system consists of a large size and distributed network. As digital technologies have become more innovative, applications of these technologies have represented the fourth industrial revolution (For example, AI, IoT, machine learning (ML), automation, and sensors) (Moshood et al., 2021). These technologies are used to optimize the supply chain. To improve the efficacy and efficiency of the supply chain, firms' systems physically link via trust networks and interfaces to share collaborative information such as inventory, sales data, and customer data (PWC, 2013). However, interconnection and interdependence may result in a domino effect of risk propagation, meaning that if one organization is breached by a threat agent, other participating players may also be exposed to data threats (Li and Xu, 2021). Simultaneously, there are numerous uncertainties and network security threats associated with this growing trend. Where various vulnerabilities and flaws might expose consumers to hacker attacks and threats (Boiko, Shendryk and Boiko, 2019). According to a 2021 Identity Theft Resource Centre (ITRC) questionnaire, supply chain hacking incidents increased by 42% in the first quarter of the year in the United States, heightening concerns about cyber-attacks on supply chain operations (Meggiato et al., 2022). Supply chains are frequently targeted because a weak link in an integrated system might allow hackers to access all of a company's data. In these circumstances, attacks are launched against the third-party firm, which is thought to have the weakest internal security measures in place (Creazza et al., 2022). When a single member's security standards are found to be inadequate, the vulnerability spreads to all supply chain partners (Momoh, 2016). In this context, third party logistics (3PL) services have proven to be critical in assisting many supply chain representatives with distribution tasks, allowing them to focus on their core competencies such as product development and production. However, there are many flaws in today's global supply chains that affect the operations of 3PL companies. For these reasons, most companies need digital transformation. This digitalization increases supply chain performance by increasing information sharing and therefore visibility; but it poses significant cybersecurity risks (Tiwari et al., 2023).

Cybercrime costs firms \$2.9 million per minute, according to RiskIQ data. Cybercrime will cost businesses globally an estimated \$10.5 trillion per year by 2025.

Furthermore, an IBM analysis shows that the average overall cost of a data breach will be \$4.3 million in 2022 (Sadeghi, Azadegan and Ojha, 2023). In addition to interrupting supply chains by approximately \$8 million, cyber-attacks on US firms have a detrimental impact on society by lowering job possibilities, with an estimated 10,000 jobs lost annually (Boyson, 2014). If we look at other statistics and numbers: According to cybersecurity firm Kaspersky, the average economic expenses connected with a supply chain attack on a business in 2021 were \$1.4 million USD, which was greater than all other forms of cyberattacks (Kshetri, 2022). In 2020, SolarWinds, a US-based IT monitoring and network management firm, had a supply chain hack that affected 18,000 customers. The cost of the attack was anticipated to reach \$100 billion USD (Kshetri, 2022). When the target is difficult to attack, it may be more appealing for an attacker to pursue a company that is part of the target's supply chain. According to the European Network and Information Security Agency (ENISA), supply chain hacks are expected to increase by 400% from 2020 to 2021 (Kshetri, 2022). According to a poll conducted by cybersecurity startup BlueVoyant, 97% of businesses have been harmed by a cybersecurity breach in their supply chain, and 93% have experienced a direct cybersecurity breach as a result of supply chain deficiencies. This strongly emphasizes the need to include suppliers, third-party providers such as 3PLs, in a company's cybersecurity understanding and plan (Kshetri, 2022). Additionally, BlueVoyant's research found that 38% of companies do not have a way to identify when or if a problem has arisen with a supply chain partner. Furthermore, BlueVoyant's survey discovered that 38% of firms had no method of identifying when or if a problem arises with a supply chain partner. Furthermore, according to BlueVoyant's survey, 31% of organizations would have a supply chain with more than 1000 entities by 2021. Any supply chain partner may be a source of risk for a firm (Kshetri, 2022). Particularly third parties. In this context, supply chain attacks are becoming increasingly popular among attackers since they allow them to access information from larger firms or many enterprises via a single, third-party (Hammi, Zeadally, and Nebhen, 2023). Real cybersecurity examples that support all the information given above and the chaos they create cannot be ignored. The NotPetya ransomware struck the massive Danish shipping company AP Moller-Maersk in June 2017, causing millions of dollars' worth of losses in its logistics division (Cheung, Bell, and Bhattacharjya, 2021). The attack caused serious damage to Maersk's corporate computer systems and networks. During a discussion at the World Economic

Forum in Davos, Maersk chairman Jim Hageman Snabe revealed the attack, which was determined to be notPetya. Maersk's computer operations were completely disrupted for at least 10 days at 76 ports globally as a result of this cyber intrusion. Large-scale cleanup activities encompassing 45,000 PCs, 4,000 servers, and more than 2,500 apps were required as a result of the aftermath. The event resulted in financial consequences exceeding \$300 million US, including lost revenue and expenses associated with cleaning (Conklin and Bronk, 2018). One of its subsidiaries, Svitzer Australia, experienced a data breach again 2017. Emails containing sensitive financial information were automatically sent to two external email accounts via hacked email accounts (Cheung and Bell, 2019). A Mailto-like ransomware attack occurred against Toll Group, an Australian 3PL, in January 2020 (Van Marle, 2020). Another ransomware, Nefilim attacked Toll four months later. The vulnerability of the logistics industry to hackers has been brought to light by these incidents (Lennane, 2020). The notPetya attack also targeted TNT Express, a subsidiary of Federal Express, causing significant hardship for this global transportation firm. All computers were blocked, which prevented the organization from exchanging data or accessing internally held information. It could thus no longer transport commodities. Businesses who depended on this organization to transport their goods encountered an unforeseen challenge and were forced to come up with other plans to minimize disruptions to their clients, such as missing deliveries and delays (Creazza et al., 2022). When the calendar showed September 2017, it was estimated that the damage caused by a conical flask could cost up to 300 million dollars (Bloomberg.com, 2017). When the calendar showed December 2021, the billion-dollar German logistics company Hellman Worldwide Logistics became a victim of ransomware. The incident highlights persistent and evolving threats in the context of cybersecurity, particularly in supply chains. Another example is SolarWinds. The 2020 SolarWinds hack was a supply chain attack that took use of SolarWinds' software update infrastructure to compromise the networks of over 18,000 companies (Keskin et al., 2021). Despite the fact that the full extent of the attack is yet unknown, Microsoft's president called it the "largest and most sophisticated attack" that has ever occurred (Whitaker, 2020). The attack was discovered in December 2020, despite having begun in March 2020 (Keskin et al., 2021). Hundreds of private organizations and facilities were affected by this attack. This really clever attack demonstrated how vulnerable all the third parties we rely on are to breaches with this kind of serious consequences (Keskin et al., 2021). Businesses

have many partners, and every program that a company uses might be a point of attack. For organizations, choosing a third party presents a difficult trade-off (Keskin et al., 2021). Partners that don't follow several cybersecurity best practices are already in danger. Although high-end companies are adept at cybersecurity, attackers are more interested in them since they may potentially expose all of their client businesses (Newman, 2021). The breach at SolarWinds is not unprecedented, and given its magnitude, it presents a significant risk to possible new attackers who may attempt to reproduce and enhance their capabilities (Newman, 2021).

These real-life examples highlight the critical importance of addressing cybersecurity risks in supply chains. The far-reaching consequences of such attacks not only lead to significant financial losses but also disrupt global operations, impacting all stakeholders in the supply chain and highlighting the urgent need for robust cybersecurity measures across sectors (Creazza et al., 2022).

There is a dearth of thorough study on the particular vulnerabilities of 3PL providers and the wider effects of cyberattacks on the supply chain, despite the crucial role of cybersecurity in logistics (Cheung et al., 2021). Studies to date tend to focus on supply chain risks in general or cybersecurity in specific cases, leaving a large knowledge gap about the specific challenges faced by 3PL providers (Gkanatsas and Krikke, 2020; Cheung et al., 2021). This thesis seeks to address this gap by investigating how cyberattacks on 3PL providers impact the entire supply chain and its stakeholders.

Therefore, the main problem addressed in this thesis is that 3PL providers are in a binding position between stakeholders in the supply chain, and an attack on a 3PL affects everyone from the manufacturer, supplier to the end user, and as a result, the risks that arise for the entire supply chain.

1.3. Significance of the Thesis

The significance of this study lies in the comprehensive examination of cybersecurity in the context of 3PL providers and its broad implications. Supply chains are stated as a chain consisting of intertwined rings that include stakeholders such as manufacturers, suppliers, transporters, etc. (Boiko, Shendryk and Boiko, 2019). 3PLs are indispensable parts of transportation, storage and distribution in this chain. In this era where digital transformation has an important place for operational efficiency, the

increasing frequency and complexity of cyberattacks pose serious threats to the logistics and supply chain. In this chain, large businesses may have a small cybersecurity footprint, while small businesses and third-party providers may have a large cybersecurity footprint even if they are small in size (Gafni and Levy, 2023). This puts them in a more targetable position. For example, in a network where there are suppliers-manufacturers-logistics service providers and customers, attackers do not want to target the manufacturer because it is relatively difficult to hijack the system since they are a relatively larger and more developed business. Likewise, although suppliers are sometimes the main target as the examples mentioned in the previous sections, attacking here is not enough to take over the entire chain. To continue, since customers are the last link in the chain, an attack here cannot target the previous links in the chain. At this point, a successful attack on a 3PL service provider may first spread to the manufacturer's information, and from this information to both the supplier and customer sides, and thus to the entire chain.

A study conducted in 2019 found that employees are increasingly being used for malicious cyberattacks day by day (Colicchia, Creazza and Menachof, 2019). This finding reveals that suppliers in the supply chain underestimate the vulnerability risks of third-party personnel in the corporate network, cloud, software used and other technologies (Boiko, Shendryk and Boiko, 2019). In this context, while data sharing continues throughout the supply chain consisting of business partners, suppliers, manufacturers and logistics providers, it is of great importance for managers to take into account the consequences of security vulnerabilities (Mutek and Irwin, 2018). Because information security risks are so high, supply managers must understand security vulnerabilities in order to establish acceptable ethical security strategies that promote, protect, and avoid harm to customers, partners, and other stakeholders (Norman et al., 2020).

In the problem statement section, the serious financial effects of cyberattacks were mentioned with statistics and real-life examples. In addition to these financial effects, these cyberattacks on third parties negatively affect buyer and supplier relationships, the risks are very destructive and negatively affect the competitiveness of companies (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Moreover, it causes the company, personal, etc. information of the stakeholders in the entire supply chain to fall into the hands of attackers.

When we look at it academically, there is a significant gap in the existing literature on cybersecurity for 3PL providers. Existing research addresses some parts of managing cyber risks, but a significant gap in the literature remains (Simon and Omar, 2020). In their article "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era", Creazza et al. state that Logistics Service Providers are the organizers of the Cyber Supply Chain Risk Management (CSCRM) process towards a more "supply chain-focused" response to cyber threats and risk events. revealed that it can play an important role. 3PL firms are frequently hired by businesses to handle their logistics (Gkanatsas and Krikke, 2020). When businesses delegate responsibility for cybersecurity risk management in connection with logistics to their 3PL partners, it fosters a sense of security (Gkanatsas and Krikke, 2020). This emphasizes the necessity of conducting scholarly research on the topic.

As a result, when all the information given above is considered, it is revealed how important the subject is academically and practically.

1.4. Aims and Objectives of The Thesis

The primary aim of thesis is to this knowledge gap by investigating the potential ripple effects of cyberattacks on 3PL service providers throughout the supply chain. By examining how such attacks can compromise the security of the entire supply chain, from manufacturers to end consumers, we aim to highlight the significant risks posed by vulnerabilities in 3PL services. Moreover, by highlighting the severe consequences of cyberattacks on the broader supply chains, we aim to reinforce the need for robust cybersecurity improvements within logistics and supply chain operations. We also aim to contribute to the creation of a safe and uninterrupted supply chain for all stakeholders by introducing effective mitigation strategies for these attacks.

The thesis includes a comprehensive review of the literature on cybersecurity in logistics operations, including the harms of cyberattacks, privacy, security, and impacts on multiple stakeholders, as well as surveys and interviews with logistics professionals to collect data on their experiences with cybersecurity systems in logistics operations.

This thesis aims to answer the following research questions (RQ):

RQ1: How do cyberattacks on 3PL service providers generate a ripple effect throughout the supply chain, impacting its stakeholders?

RQ2: What are the mitigation strategies for a cyberattack on 3PL service providers?

With the first RQ, we aim to identify the ripple effects of cyberattacks on 3PL service providers, examining how these attacks spread to supply chain stakeholders such as 3PL firms, ports, importers, exporters, and customs agencies. A semi-structured interview will be used to address this RQ (Flick, 2014). This method was chosen as it allows the collection of detailed and detailed data from a wide range of participants, including key stakeholders in the supply chain such as exporters, importers, customs agents, ports and 3PL service providers (Megaldi and Berler, 2020). The semi-structured format allows participants to provide in-depth information while ensuring that the data collected is comparable across different participants (Wilson, 2013). Moreover, this method was chosen for its suitability for investigating complex issues and capturing the diverse perspectives of stakeholders affected by cyberattacks (Megaldi and Berler, 2020).

With the second RQ, we aim to identify effective mitigation strategies to prevent or minimize the impact of cyberattacks targeting 3PL service providers. Additionally, we seek to contribute to the development of a secure and uninterrupted supply chain for all stakeholders through in depth examination of participants' perspectives on mitigation strategies for cyberattacks against 3PL providers. In that respect, interviews accommodate the diversity of experiences and insights of industry stakeholders, which is crucial for identifying nuanced and context-specific strategies (Megaldi and Berler, 2020). The open ended nature of the interviews will provide a comprehensive perspective on real world practices and challenges (Wilson, 2013).

The use of semi-structured interviews was designed to comprehensively address the RQs and achieve the overall objectives of the thesis. This method was carefully selected for its ability to provide detailed stakeholder perspectives on the effects of cyberattacks on the supply chain, capturing a wide range of experiences and insights. Semi-structured interviews contributed to the thesis by offering industry experts' opinions and real-world practices, enabling the identification and evaluation of effective cybersecurity mitigation strategies. This approach allowed for a deeper exploration of cybersecurity challenges and their impact on supply chain resilience, particularly for 3PL providers (Wilson, 2013).

CHAPTER 2: LITERATURE REVIEW

The integration of technology in SCM has revolutionized logistics operations, driving unprecedented levels of efficiency and connectivity. However, this technological advancement also introduces new challenges, particularly in the realm of cybersecurity. As supply chains become increasingly digital, they are more vulnerable to cyber threats that can disrupt operations, compromise sensitive data, and undermine stakeholder trust. This literature review explores the adoption of technology in supply chains, the specific cybersecurity threats faced by logistics services, and the crucial role of 3PL service providers. This chapter aims to highlight the current state of cybersecurity in logistics by examining existing research, examine the existing information in the literature, identify gaps in the literature, and emphasize the importance of third parties, especially 3PL service providers, on the subject.

2.1. Supply Chain and Technology Adoption

Supply Chain has been defined as a global network that delivers raw materials, products and services to end users through a designed flow of information, physical distribution and money (Hammi, Zeadally and Nebhen, 2023). It includes suppliers, logistics service providers, manufacturers, distributors, retailers and end users. In another definition, the supply chain is a network of manufacturers, suppliers, distributors, retailers, logistics service providers, information and other logistics management services providers that are involved in shipping products to customers (Chow and Heaven, 1999).

The Internet has revolutionized people's lives and is now used in almost every aspect of life. In this context, it is an inevitable fact that technologies will become widespread and used in supply chains (Hammi, Zeadally and Nebhen, 2023). It has also been stated that supply chains are the backbone of developing technological ecosystems (Ghadge et al., 2020). The application of information, digital and electronic technologies to every aspect of the supply chain, from the first link of the chain to the last link, has resulted in the definition of Digital Supply Chain (DSC) (Hammi, Zeadally and Nebhen, 2023). DSC systems, which have started to be used with developing technology, are systems used to improve and digitalize transaction and cooperation processes with supply chain partners (Xue et al., 2013). These technologies are radically transforming supply chain structures in different industries,

resulting in many benefits such as maximizing profit and minimizing loss, optimizing supply chain lead times, enabling demand-driven supply chain, improved collaboration between different stakeholders, improved cash flows, cost management, real-time tracking, predictive analytics, automated decision-making processes etc. (Heizer, Render and Munson, 2017). In addition, Industry 4.0 concepts such as the IoT, additive manufacturing, virtual reality (VR), AI, ML and blockchain help reflect, expand, change and renew relationships between supply chain partners (Ghadge et al., 2020). For instance, IoT devices can monitor the condition of goods in transit, providing real-time data on temperature, humidity, and location, which helps in maintaining product quality and ensuring timely deliveries. Blockchain technology (BCT) offers an immutable ledger of transactions that enhances transparency and traceability, thereby reducing fraud and improving accountability across the supply chain. AI and ML algorithms analyze vast amounts of data to forecast demand, optimize inventory levels, and streamline logistics operations, leading to cost savings and better resource utilization.

Moreover, with globalization and developing technologies (such as industry 4.0 and industry 5.0), organizations today increasingly rely on suppliers and third parties to carry out their critical operations. As a result, the rate of outsourcing of critical services and functions has increased. All organizations rely on purchasing items and services, and the majority of organizations also sell things and services to other organizations. In the area of Information Communication Technology (ICT), the supply chain consists of a variety of resources (hardware and software), storage (cloud or local), distribution channels (web apps, online stores), and management software (Nygård and Katsikas, 2022).

A common point of all this technological development, apart from improving supply chains and logistics operations and increasing operational efficiency, is that all these technologies create a security vulnerability and are vulnerable to cyber risks. Hammi, Zeadally and Nebhen (2023) argue that DSCs are vulnerable to a wide range of cyberattacks, from a simple information theft to a complete shutdown of factory operations, and that supply chains are a collaboration of many different technologies and techniques such as the IoT, cloud computing, networks and telecommunications and many more. Therefore, they stated that it is vulnerable to different cyber risks. Another study claimed that advances in cybersecurity interventions have lagged

behind these advances in the digitalization of supply chains, and that supply chains are unintentionally expanding their vulnerability by imprudently collaborating with many different partners (Boone, 2017). In this context, according to the global risk research conducted by various consultancy and insurance companies in 2018, cybersecurity and data breaches emerged as the biggest corporate risk, which reveals the seriousness of the issue (Ghadge et al., 2020).

Bechtsis et al (2021) drew attention to the need for risk management in order to increase the security, durability and sustainability faced by supply chains with developing technology. In the study, the impact of security on supply chain operations and gaps in flexibility strategies and practices were determined. The researchers then proposed a framework that was validated through a case study. This framework highlights the need for data-driven digital technologies that enable effective data processing for data collection and management, secure storage, and data monetization for supply chain security. In another study Kumar and Mallipeddi (2022) pointed out the cybersecurity risks that come with Industry 4.0 and Industry 5.0. To address the issue, the study discussed possible future research directions that production and operations management researchers could undertake to help organizations and supply chains develop robust strategies to reduce the number and impact of attacks on organizations and supply chains. The authors stated that production and operations management should be addressed in global operations strategy, healthcare sector, public, technology management, disruptive technologies and supply chain. They also added that cybersecurity research is critical to overcoming the challenges of cybersecurity risks for industry and society.

Nygård and Katsikas (2022) systematized security threats and challenges in DSCs and related cybersecurity measures. The authors discuss the necessary knowledge and skills that cybersecurity experts must have to ensure effective management of cyber risks in the DSC and systematize the areas where research is needed. Also, Hammi, Zeadally, and Nebhen (2023) presented a holistic survey on supply chain security. In the study, different security problems and attacks targeting different supply chain technologies were discussed. Then, various countermeasures and security solutions proposed by academic and industry researchers to mitigate the identified threats are discussed. As a result of their analysis, the researchers found that previously proposed supply chain security solutions did not take into account the

different security challenges and problems they addressed. Therefore, the authors draw attention to the need for a comprehensive and holistic approach that ensures the security of the end-to-end supply chain. Additionally, they stated that blockchain and AI can be key solutions that can increase the security of the supply chain. In another study, Ivanov, Dolgui and Sokolov (2019) examined the impact of Digitalization and Industry 4.0 on the ripple effect and disruption risk control analytics in the supply chain. With the research framework, the authors combine results from two isolated areas: the impact of digitalization on SCM, and the impact of SCM on ripple effect control. With this framework, the authors touched on 3 issues. The first is what the relationships are between big data analytics, Industry 4.0, additive manufacturing, advanced track and trace systems, and supply chain disruption (SCD) risks. The second is how digitalization can contribute to improving ripple effect control, and the last is which digital technology-based extensions can trigger developments in supply chain risk analytics.

Sobb, Turnbull, and Moustafa (2020) discuss existing and emerging meaningful models regarding standardization, improvement, and security assurance issues for military products chains 4.0 of new technologies.

Enache (2023) discussed the basic cybersecurity concerns and feasible ways to reduce risks affecting the logistics sector, which is increasing with technologies such as big data, cloud computing and IoT.

In general, although the benefits of technology adoption in supply chains are significant, companies should not ignore potential risks and focus on them.

2.1.1. Supply Chain Security Issues related to Technology Adoption

As supply chains increasingly adopt advanced technologies to enhance efficiency and competitiveness, they concurrently face a myriad of security issues that can undermine these benefits. The biggest problem that arises in this context is the increased risk of cyberattacks.

A supply chain attack is a powerful cyberattack that can breach even the most sophisticated security defenses through third parties. These attacks have been a security concern for many years, but with increasing digitalization day by day, their number has been increasing since early 2020 (Nygård and Katsikas, 2022). When a third party is compromised in a cyberattack, its customers' systems are often

compromised as well. Because third parties store sensitive data for many customers, a single supply chain attack allows attackers to access sensitive data of many organizations across many industries (Nygård and Katsikas, 2022). A cyberattack on a supplier or 3PL service provider can create major delays in production schedules and supply, as well as delays in shipping and delivery throughout supply chains (Williams, 2014). Cyber breaches by third-parties can also have an influence on an organization's overall financial performance and shareholder value (Modi, Wiles, and Mishra, 2015). Such attacks do not have to be directed at the company itself; they might occur anywhere along the supply chain (Simon and Omar, 2020). The main reason for this is that while interconnected systems provide significant operational benefits, they also expand the attack surface, making it easier for hackers to exploit vulnerabilities in one part of the network to access other areas.

Hackers may intend to hack communication channels, obtain, manipulate data, and disseminate false information within the network (Latif et al., 2021). Additionally, cyberattacks often have some type of direct monetary consequence, such as ransomware; or they are carried out as industrial espionage (O'hara, 2010). One example might be the WannaCry attacks of 2017. Data was encrypted throughout the attack to prevent users from accessing it; the data could only be accessed once the ransom was paid (Mohurle and Patil, 2017).

Similar unidentified cyberattack surfaces exist for robotic systems, drones, and other remotely operated systems. Future warehouses will be mostly automated and manned by robotics, actuators, and sensors. In theory, a cyberattack on a logistics system may affect operations, reroute vital equipment while it's in transit, send equipment via untrusted channels, or even stop all logistical movement and disturb system functions (Sobb, Turnbull and Moustapha., 2020). Since supply chains consist of interconnected nodes, an attack on one node reaches the entire chain with a domino effect.

2.1.1.1. Insider Threats

Insider threats are people who work for a company and may purposefully or inadvertently jeopardize the security of data and systems. Insider attacks might originate from staff members who have malevolent intent or inadvertently make blunders and get access to confidential logistics data. Unauthorized access, data

breaches, and delays in logistical operations can all result from insider threats. Although inadvertent errors might lead to unintentional data breaches, malicious insiders can deliberately breach systems (Odimarha, Ayodeji and Abaku, 2024).

According to Kunnathur (2015), employees carry the most important risk in the context of cybersecurity in companies. Stephens and Valverde (2013) emphasize that employees do not attach importance to password confidentiality, and Venter (2014) emphasizes that passwords are written down by employees so that they can be remembered, but the notes are not confidential. Moreover, sensitive information is inadvertently disclosed in employee communications within the company, and companies must be aware of this (Kunnathur, 2015). Alongside these careless actions, instances of employees purposefully misusing or even sabotaging a company's information are also documented in the literature (Ghadge, Caldwell and Wilding, 2020). Examples of these include data misuse and data sharing due to personal revenge against the employer (Deane et al., 2009; Sharma and Routroy, 2016).

An organization's cyber risk and the possibility of disruption in information technology (IT) system operations are increased in a supply chain where a large number of workers are committed to innovation in order to get a competitive edge (Boyson, 2014). Colicchia, Creazza, and Menachof (2019) discovered that workers are being utilized more and more as tools in harmful attacks and they divided insider threats into two parts: malicious. These are current employees and former employees. They divided natural and unintentional insider threats into four sections. These are current employees, former employees, power outages and technical problems.

The human component can be the greatest and most unpredictable danger to a company's cybersecurity, both in the careless and deliberate modes. Because they may have easy access to facilities or goods, employees may serve as insiders and assist criminals in continuing their illicit activities, or they may commit a crime on their own (Urciuoli, 2015).

According to the Cybersecurity and Infrastructure Security Agency (CISA), an insider threat is the possibility that an insider may utilize his or her permitted access or understanding of an organization to do harm to it. This damage can be willful or inadvertent behaviors that negatively impact the integrity, confidentiality, and availability of the organization's resources (Zeadally et al., 2012). 95% of successful

cyberattacks on businesses, according to IBM research, are mostly the result of human mistake (Ahola, 2021). The number of cyberattack incidents caused by insiders has increased by 47% since 2018 (Ponemon Institute, 2021). Moreover, according to the European Union Cybersecurity Agency, 88% of organizations agree that insider threats are a cause of problems (ENISA, 2020). Therefore, a security issue caused by an insider should be considered a serious problem for companies and can reach all supply chain links (CyberEdge Group, 2021). In an example that happened to Amazon, a former employee bypassed the firewall and accessed the account and credit card information of millions of customers. At Tesla, an insider shared confidential and sensitive data with unknown third parties (Hammi, Zeadally and Nebhen, 2023).

2.1.1.2. Blockchain Technology (BCT) and Threats

According to Kshetri (2017), BCT is a "data structure that makes it possible to create a tamper-proof digital ledger of transactions and share them". According to Meggiato et al. (2022) BCT is a type of virtual network that is safer and more advanced than the ones we are accustomed to at home or at work. Blockchain is essentially a distributed ledger for transactions that is maintained by synchronized states using digital signatures and cryptographic hash algorithms. Peer-to-peer networks are used to distribute and decentralize ledger material, and records are subjected to encryption with private keys serving as digital signatures (Park and Park, 2017). BCT has a particular set of properties. These include a decentralized structure, a distributed recording and storing mechanism, a consensus method, smart contracts, and asymmetric encryption, which provide network security, clarity, and visibility. BCT offers limitless potential to improve supply chain operations, including supply chain provenance, business process reengineering, and security enhancement (Dutta et al., 2020; Raj, Choi and Kumar, 2021; Chang et al., 2021).

While BCTs are most recognized for their usage in cryptocurrencies, such as Bitcoin, they may also be used to a range of systems and activities, including supply chains (Park and Park, 2017). Some of the reasons for its adoption include its ability to assure uniformity and encourage honesty in logistics operations (Choi et al., 2022). It may be used in conjunction with IoT to improve component tracking and traceability across the supply chain. Implementations in the supply chain can improve security and resistance to cyber-attacks by identifying insecure or possibly exploitable components at all levels of the supply chain (Kshetri, 2017). One suggested use of blockchain in

supply chains was the use of UAVs to gather track and trace data from RFID tags on industrial objects (Fernández et al., 2018).

The system also generally updates itself in real time, eliminating the need for a third-party validator or human intervention, making it more efficient. BCT has already begun to have an influence on corporate governance, thanks in part to its ability to protect the interchange of data while it is spread. A BCT-supported supply chain offers reduced operational risk than a standard supply chain (Tiwari et al., 2023). Additionally, BCT is the technological solution that can support the upkeep of systems safe and reliable (Lu et al., 2019; Mangla et al., 2021), which is essential for businesses looking to improve supply chain transparency (Luo and Choi, 2022; Shen, Dong and Minner, 2021; Xu et al., 2022).

Tiwari et al. (2023) drew attention to 3PL service providers and conducted a study on these providers and blockchain. They mentioned the increasing information sharing that comes with digitalization and stated that this may create cybersecurity risks. In this case, they stated that the features of BCT, such as being secure and decentralized, can help in cybersecurity. In their study, they examined the 3PL and blockchain literature and determined the difficulties and how to use blockchain. Then, interviews were held with industry executives to indicate the adoption status and obstacles of blockchain in 3PL service providers. Finally, a roadmap and framework for the implementation of blockchain is proposed, and they point out that the most important contribution of the study is this roadmap and framework. It has also been stated that a 3PL logistics chain enabled by BCT increases transparency and visibility while providing a high level of trust and information sharing.

Wahab et al (2020) argued that BCT is a potential defense tool against cyber threats that a supply chain may face.

BCT may enhance warehouse and supply chain operations (Min, 2019). It can facilitate the transition from traditional risk management to risk management supported by BT. While traditional risk management only finds apparent risk, a blockchain may identify many unseen dangers and go from basic damage control to layered protection. According to Min (2019), the battle against cybercrime is a blockchain's final objective. According to him, using BT can eliminate the possibility

of a single point of failure because of its end-to-end encryption, visibility, and privacy. Antivirus software alone is insufficient to reduce the danger.

Narwane et al (2023) suggested that the use of BCT with big data will have a positive impact on the management of supply chain risks. In the study addressing the Indian supply chain, 16 risk factors were identified in line with expert opinions. For the relationships between factors, the gray DEMATEL method was applied. The results are that the applied method can help managers, suppliers, service providers adapt blockchain and big data to their operations.

In another study, Martínez, Marin-Tordera, and Masip-Bruin (2021) suggested an authentication/access method for weaker elements in a supply chain, i.e., IoT devices, employing blockchain as the baseline technology. Their suggestion considers the production of temporal tickets to have higher access control.

Despite its benefits and usability, BCT is still not a completely reliable technology. The use of BCT is not without its difficulties. These include concerns about data privacy, operational resilience, and system governance. Not every use-case can benefit from blockchain due to its decentralized structure and operational expense. Furthermore, blockchain's ability to fend against some harmful attempts does not shield it from others. Cyberattacks like the "51% Attack," identity theft, and computer code hacking all put the integrity of blockchain operations at danger (Alkadi, Moustafa and Turnbull, 2020). Additionally, Tiwari et al. (2023) stated that BCT is quite expensive when implemented throughout the supply chain and includes software, hardware, training and transition costs. It has been revealed in the literature that it is difficult for companies in underdeveloped and developing countries to access these technologies due to these costs, and that third parties in the chain and small and medium-level companies may have financial difficulties in using technology.

2.1.1.3. Artificial Intelligence (AI), Internet of Things (IoT) and Threats

In general, AI refers to systems that function in autonomous, asynchronous, and goal-oriented contexts and have traits that mimic human behavior (Tecuci, 2012). AI in the context of supply chains frequently helps to resolve the industrial issues that these systems have, such as those involving distribution, cooperation, and operation synchronization (Sobb, Turnbull, and Moustafa, 2020). The term "Internet of Things" describes the network of computers connected online that use sensors and other

observational data to gather knowledge about the physical environment (Ashton, 2009). IoT essentially integrates compute and internet activity into already-existing devices, enabling large-scale communication across heterogeneous networking components (Sobb, Turnbull, and Moustafa, 2020).

In today's changing corporate climate, SCM may greatly benefit from the integration of AI technology to improve security and efficiency (Chukwu et al., 2024). According to Charles, Emrouznejad, and Gherman (2023), it may greatly improve supply chain security by enabling proactive risk mitigation techniques and offering sophisticated threat detection capabilities. Elluru et al. (2019) state that AI supported surveillance systems can analyze large amounts of data in real time, detect anomalies and potential security breaches before they escalate, and ML algorithms can help organizations prevent or minimize damage by identifying patterns that indicate fraudulent activities or malicious intent. Dubey et al. (2021) stated that AI can increase cybersecurity by constantly monitoring network traffic, identifying potential security vulnerabilities and responding autonomously to cyber threats, thus reducing the risk of data breach and cyberattack. Collins et al (2021) suggested that AI-supported security systems can improve threat detection and risk mitigation capabilities. Furthermore, Clement et al. (2024) pointed out that contemporary AI algorithms are capable of analyzing massive amounts of data from several sources, such as sensor data, transaction logs, and security films, in order to find patterns that point to abnormalities or security risks. Furthermore, AI-powered surveillance systems can identify illegal access, suspicious activity, or departures from normal behavior by continuously monitoring several aspects of the supply chain, including warehouse operations, transportation routes, and inventory movements (Chukwu et al., 2024).

Technology has played a big role in expediting processes in the face of many activities; one of these essential fields of technology is IoT technologies and AI, which now play an important role in the industry (Nozari, Szmelter-Jarosz and Ghahremani-Nahr, 2022). These technologies, which contribute to the supply chain and logistics in many areas, including security, also bring new security problems. There are vulnerabilities in ML systems used to validate and audit supply chain networks. Obtaining complicated AI systems raises trust concerns when consumers do not completely comprehend the program (Lee and See, 2004). Radanliev et al. (2020) stated that the integration of technologies such as AI, ML and data analytics in the

supply chain will create cybersecurity risks resulting from the integration of less secure systems. They also added that the integration of cyber elements into production will naturally attract cyberattacks.

In their study, Nozari, Szmelter-Jarosz and Ghahremani-Nahr (2022) examined the difficulties in IoT and AI in the supply chain, which is one of the most important parts of production organizations. The researchers conducted a systematic literature review (SLR) to uncover these challenges. Then, by applying the Delphi method, 29 difficulties were revealed within the framework of expert opinions. These challenges were then presented to twenty-five experts in the field of supply chain and IT and fifteen experts from the university in this field. A survey and Likert scale application resulted in a list of nine main challenges. According to the findings, cybersecurity is at the top of the list. Some of the other major challenges are: lack of trust in AI and the IoT, lack of appropriate infrastructure, lack of professionals and smart waste (Nozari, Szmelter-Jarosz and Ghahremani-Nahr, 2022). In another study, Younis, Sundarakani, and Alsharair (2021) investigated how AI and ML can be applied in supply chains. In their findings, they found that AI and ML applications are still in their infancy and the opportunity to improve supply chain performance is very high. They also found that some researchers claim that AI and ML are currently adding value, but many other researchers are of the opinion that they are still not fully utilized, and their tools and techniques can increase the overall value of the supply chain. Finally, research has discovered that the adoption of AI and ML has the ability to reduce the bullwhip effect, further supporting supply chain efficiency and responsiveness performance.

When considering IoT and AI-based supply chains, it is critical to provide effective resource allocation and secure data transfer between edge devices and the cloud (Pirbhulal et al., 2022). Exposing private data to hostile parties can lead to network intrusions and significant financial losses for enterprises (Da Costa et al., 2019). Consequently, it is crucial for enterprises to implement strong data transfer methods (Da Cruz et al., 2018).

All things considered, the successful application of AI technologies in supply chain operations demands careful planning, financial investments in personnel and

technology infrastructure, and a commitment to addressing organizational, ethical, environmental, and technical concerns (Chukwu et al., 2024).

2.2. Overview of Cybersecurity in Supply Chain and Logistics

Cybersecurity is described as the sum of tools, policies, security concepts, security measures, guidelines, risk management techniques, activities, training, best practices, assurance, and technology that may be utilized to safeguard the cyber environment, the organization, and the user's assets (ITU, 2009).

Cybersecurity can also be defined as the collection of tools, procedures, software, intervention strategies, and mitigation techniques created to guard computers, networks, programs, and data against damage, intrusion, and attacks in order to maintain availability, confidentiality, and integrity (Public-Safety Canada, 2014).

Cybersecurity, as it relates to supply chain and logistics security, is the process to defend the part of the chain that interacts with IT systems, networks, and software. Cybersecurity is required to stop sensitive data from being stolen and to make sure that spyware and other malicious software doesn't damage the system or the chain as a whole (Hassija et al., 2020).

In today's world, IT systems provide a continuous flow of data in the background across large parts of the supply chain; Therefore, cybersecurity is one of the most critical issues. Over-dependence on an interconnected IT system means that with an error that can come from a single point in the chain, the entire chain faces a security problem. A successful attack on just one of the systems can lead to access to all other secure parts (Hassija et al., 2020). Supply chains are also seen as potential targets by attackers because they contain thousands of employees, companies, customers and, in this context, thousands of private information that must be kept confidential. Logistics, on the other hand, carries risks because it is an important part of the supply chain and can be a weak link in the system. On the subject, Hassija et al. (2020) stated that supply chain stakeholders, especially third-party service providers, do not have the same security standards as other organizations in the chain. Trudgian (2016) stated that the systems that ensure the functioning of the supply chain carry a lot of information, including customers' credit card information, and drew attention to the need to protect this data.

Cheung, Bell, and Bhattachariya, (2021) point out in the findings of their study that there are a very limited number of studies that adopt quantitative research approaches to examine cybersecurity in logistics and SCM.

Ugochukwu, Goyal and Arumugam (2022) discussed cybersecurity for the logistics sector in their study. In the study, they proposed a Blockchain-based IoT-enabled system framework for safe and efficient logistics management in which logistics data can be captured with the use of IoT sensors. They also designed a diagram for secure communication between logistics stakeholders through a smart contract. As a result, they concluded that BCT, with its basic features, can provide security to logistics data and increase operational efficiency.

Colicchia, Creazza, and Menachof (2019) investigated how companies look at the management of cyber and information risks in their supply chains, what initiatives they adopt for this purpose, and to what extent they address them throughout the supply chain and presented a complete list of cyber supply chain risk management initiatives. The research topic is discussed in terms of cyber supply chain risk management. In this context, the main purpose of the study is to support companies to draw attention to and improve the CSCRM process and cyber resilience in their supply chains. The study is based on a comparative case study analysis involving five large international companies. The results of the study emphasize the importance of companies that can establish their own defense walls to shift their focus to the entire supply chain rather than to the IT infrastructure. The authors emphasize the importance of involving supply chain partners in the fight against cybersecurity. Additionally, the empirical results of the study show that companies focus only on the response and recovery phases rather than a multi-phase approach such as preparation, response, recovery and sustainment in the context of cybersecurity.

Odimarha, Ayodeji, and Abaku, (2024) highlight the urgent need for robust cybersecurity measures in the logistics and transportation sector, where supply chains are vulnerable to numerous cyber threats. By providing actionable recommendations and insights from real-world case studies, the study aims to strengthen logistics and transportation companies' cybersecurity defenses, protect critical assets, and maintain trust in the DSC ecosystem. The authors explore specific challenges faced by logistics companies, including the interconnectedness of global supply chains, dependence on

digital technologies for operations, and the high value of goods transported, and also address cyber risks, including threats such as ransomware, phishing attacks, data breaches, and SCDs. Additionally, cybersecurity measures such as robust authentication, access controls, encryption of sensitive data, establishment of secure communication channels, regular vulnerability assessments, and penetration testing are described.

Simon and Omar (2020) stated that individual nodes in a supply chain bear the entire cost of their own cybersecurity investments, but other nodes can also benefit from some of the benefits of the investments. For this reason, they discussed the differences between coordinated and uncoordinated cybersecurity investments and the differences arising from strategic and non-strategic attackers. They found that a lack of coordination in supply chains can lead to under- or over-investment in a strategic attacker, depending on how greater the indirect damages from attacks are relative to the direct damages.

Crosignani, Macchiavelli and Silva (2023) examined the effects of the most damaging cyberattack ever on the supply chain. Burrell et al., (2020) stated that protecting logistics and supply chain organizations from cyber and data security risks is not only the duty of IT employees but also the responsibility of the entire supply chain employee. They also investigated open door systems approaches to reduce data security and cybersecurity risk. Deyannis et al., (2022) presented a low-cost, reconfigurable intrusion detection system (IDS) application that can be easily integrated into supply chain networks and increases security levels to detect malicious activities in the context of cybersecurity in supply chains. Wang (2021) discussed the problem of supply chain attacks and the challenges of defending against software supply chain attacks. The author proposed an information flow-based detection approach that allows end users to detect many software supply chain attacks without dealing with any of the underlying software vendors. Ghadge, Caldwell, and Wilding (2020) explored cyber risk management in supply chain contexts and also developed a conceptual model that demonstrates a strong link between IT, organizational, and supply chain security systems.

Sadeghi, Azadegan, and Ojha (2023) discussed cyber resilience in supply chains. Their study examined the effects of visibility on cyber resilience during a data

breach. The study found that dominant suppliers are reluctant to share information about visibility, and supply chain and operations managers can prevent, sustain, and recover from disruptions when real-time information is available.

In the study of Martinez, Marin-Tordera and Masip-Bruin (2021), it was stated that insecure supply chains encourage well-known cyberattacks. Additionally, statistics are given that 80% of all cyber breaches occur in the supply chain, and moreover, 72% of companies do not have full visibility into their supply chains.

2.2.1. Common Types of Cyberattacks Seen in Supply Chain and Logistics

Below, the most common types of cyberattacks seen in supply chain and logistics will be explained. Additionally, the classification of cyberattacks on supply chain links is given in Figure 1.

2.2.1.1. Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack occurs when an extremely large number of packets are transmitted from many attack sites to a victim's site. These packets are sent in extreme numbers and the victim's resources such as bandwidth buffering and CPU begin to slow down and become exhausted (Hammi, Zeadally and Khatoun, 2019). DDOS is simply an attacker's attempt to disrupt the use of a service. According to Liu, Wang and Tang (2020), DDOS is a cyberattack that allows the attacker to infiltrate organizations' networks and overload the bandwidth of the network. The prevalence of DDOS is due to its ability to be very effective against all kinds of services (Hammi, Zeadally and Nebhen, 2023).

When it comes to the supply chain, DDOS allows attackers to infiltrate devices in the supply chain and can be part of a botnet that can launch a cyberattack through the internet network. In this case, supply chain machines cannot operate at their full performance and are targeted as the source of attacks, which has a negative impact on the company's brand value and reputation. Another scenario is when a stakeholder in the supply chain is subjected to a DDOS attack. In this case, the attack creates a domino effect between all supply chain steps, making the supply chain inoperable from start to finish (Hammi, Zeadally and Nebhen, 2023).

Small third parties, such as suppliers and service providers, represent the weakest link in the supply chain. Therefore, attackers target these weak links when performing a DDOS attack. In the supply chain, logistics and distribution are handled

by one or more third parties. Like parent companies, these logistics companies have computing and network infrastructure and can be obvious targets. As a result, operations may stop and even if the manufacturer can provide the product, its connection with the seller remains out of the system. It has been proven that the most common attack on service providers is the DDOS attack. According to 2019 data, DDOS accounts for 77% of attacks (Hammi, Zeadally and Nebhen, 2023). For example, the largest DDOS attack in history was carried out on Amazon company in 2020 (Tony et al., 2020).

Statistically, when comparing the first quarters of 2019 and 2020, there was an increase of 278%. According to Nexusguard, the increase in the third quarters in the same years is 542% (Tony et al., 2020). According to Sonatype, there is a 430% increase in attacks on open source software in the supply chain (Sonatype, 2020).

DDoS attacks against consumers have less damage than attacks on other stakeholders because they cannot reach the entire chain (Hammi, Zeadally and Nebhen, 2023).

2.2.1.2. Malware

Malware is a significant threat when it comes to supply chain security. Malware includes viruses and ransomware (Cleary et al., 2018). The most suitable example of this type of attack is the Wannacry attack. The attack spread to the infrastructures of more than 150 countries and caused material damage of \$4 billion (Berr, 2017).

Malware seriously affects logistics and distribution in the supply chain. If we look at past examples, large companies such as FedEx, Wannacry and Maersk have fallen victim to ransomware called NotPetya. These 3 companies suffered a total of approximately 970 million dollars in financial damage (Hammi, Zeadally and Nebhen, 2023). Another ransomware attack was made on the 8850 Km Colonial Pipeline, one of the largest oil pipelines in the USA, in May 2021.

Ferdous et al. (2023) aimed to comprehensively review the development of malware from past to present and current attack trends in order to determine effective defense mechanisms. In the study, they comprehensively examined the malware environment and analyzed malware types, operational mechanisms and vulnerabilities in depth, and researched new defense strategies. The researchers' findings highlighted rising trends in cryptojacking, IoT, supply chain attacks, and malicious attacks on

networks. Researchers highlight the critical need for robust, multi-layered security measures to combat evolving malware. The researchers additionally point out gaps in existing studies, particularly the lack of comprehensive studies that cover the full picture of malware evolution, contemporary attack trends, and defensive solutions. In another study, Shukla et al. (2023) revealed a unified learning approach that uses heterogeneous models for malware detection in IoT networks. The findings showed 13% better results than traditional federated learning in terms of accuracy and reduced the number of false positives by 63.99%. Sanjay et al. (2018) introduced a method that uses memory forensics-based analysis to detect fileless malware based on opcode sequences.

Statistically, according to security research company Cybersecurity Ventures, businesses become victims of a ransomware attack every 11 seconds, and the cost of global ransomware damage is approximately \$20 billion (Morgan, 2019).

2.2.1.3. Hardcoded Credentials

Hardcoded credentials are one of the most common security concerns in various systems such as IoT and ICS, and they can lead to security issues across the supply chain. These features, which make the work of employees and users easier, might be abused by attackers or inexperienced users. To provide access control, the utilized credentials must be kept secret (Hammi, Zeadally and Nebhen, 2023).

Considering the devices used in the supply chain, when users purchase an IoT device they are set up with hard-coded usernames and passwords. This information is also available on the sellers' websites. This situation leads to situations such as data identity theft through different cyberattacks and also facilitates unauthorized access to systems (Verma and Chandavarkar, 2019).

2.2.1.4. Phishing

Phishing is a type of cyberattack in which attackers attempt to gain access to systems by sending fake emails to employees for them to click (Kumar and Mallipeddi, 2022). Phishing attacks entail the use of counterfeit emails, messages, or websites to deceive people into divulging private information, such as bank account information or login passwords (Alkhalil et al., 2021). Phishing has been reported to be the most common source of cyberattacks, accounting for over 80% of attacks (Cisco, 2021). Given the wide range of parties engaged in logistics, including employees, suppliers,

and partners, phishing attacks are a substantial concern. Successful phishing attempts can result in unauthorized access to vital systems, the theft of sensitive information, and interruptions to supply chain activities (Okoye et al., 2024).

A phishing attack on Target Corporation in 2013 exposed the personal and credit card data of more than 100 million customers and caused Target an economic loss of more than \$200 million (Reuters, 2017). Attackers gained access to Target's systems via phishing and installed malware on many of its point-of-sale systems (Kumar and Mallipeddi, 2022). Figure 1 below provides the taxonomy of cyberattacks for supply chain links.

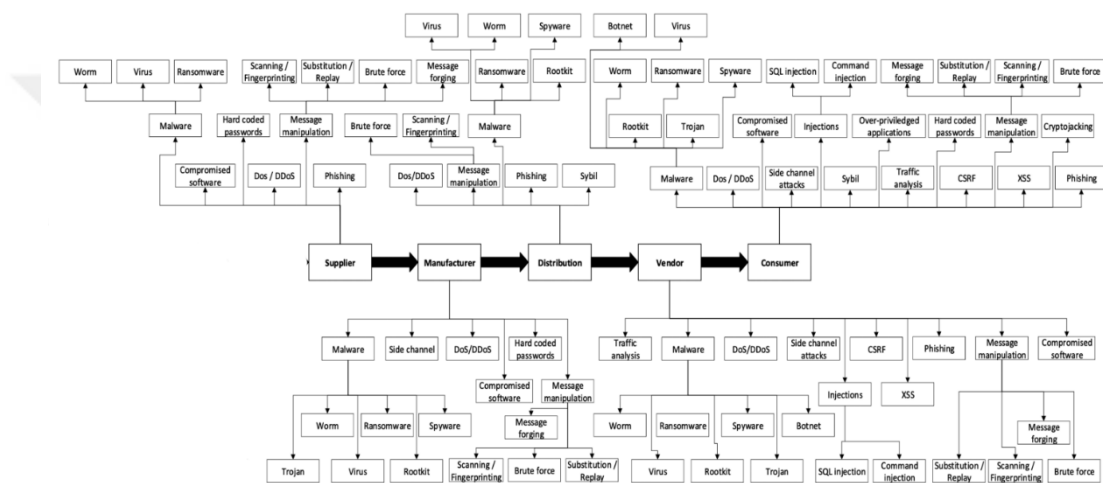


Figure 1. Taxonomy of cyberattacks for supply chain links (Source: Hammi, Zeadally and Nebhen, 2023). Reproduced with permission from Hammi, Zeadally and Nebhen (2023). ©Association for Computing Machinery.

2.3. The Role and Importance of 3PL Service Providers in Cybersecurity and Their Impact on Supply Chain Stakeholders

3PL service providers can be defined as external parties that perform logistics services between nodes in the supply chain (Alkhatib, Darlington, and Nguyen, 2015; Tezuka, 2011). Transactions of 3PL service providers include outsourcing services such as storage, transportation, distribution, and even financial transactions (Karrapan et al. 2017; Niemann, Hall, and Oliver 2017).

The rise of 3PL in tandem with increasing competitiveness in supply chains has encouraged manufacturers to outsource the logistics function. 3PL service providers

have also added services such as customs clearance, order processing, packaging and labeling, after-sales support and reverse logistics. (Tiwari et al., 2023).

Although 3PL services contribute greatly to business operations, they have increased the complexity of the supply chain by adding external stakeholders to the system; this leads to an increase in the number of interfaces, the number of intercompany transactions, and more information data flows across connections (Klockner et al., 2022). This data flow and sharing of information with other partners brings with it many risks and creates trust issues (Rao et al., 2021).

3PLs and companies that work with 3PLs rely on daily access to vast amounts of critical data, making them particularly vulnerable and a potential target for attackers. Supply chains are a network of interconnected nodes and are formed by multiple firms connected through shared information. The large number of devices connected to the same network and the high amounts of private data traffic that often accumulates in cloud solutions means that data protection and information security are critical issues in the context of supply chains and 3PLs. Moreover, real-time information acquisition among customers is increasing day by day, which puts more pressure on access security to invalidate attack attempts or unauthorized access and cyberattacks (Da Silva, Frederico, and Garza-Reyes, (2023). Third parties in the supply chain rely heavily on connectivity for critical operations, but many of these third parties still operate legacy systems and outdated technology. Therefore, supply chains and 3PLs are becoming more vulnerable to cyberattacks. Critical information such as customer personal information (such as bank accounts, payment information, identity information), production information, order fulfillment, operational capabilities and processes, patent information and other data are open and encouraging to cyberattacks (Meggiato et al., 2022).

3PL service providers are in a very important position under the heading of cybersecurity due to the thousands of data they have and the technologies they use. 3PL warehouses also have an important place in this process because 3PL warehouses use systems that improve the operation process. These systems always carry the risk of hacking, so it is very necessary to focus on cybersecurity in 3PLs (Meggiato et al., 2022). Software and warehouse management systems (WMS) are just some of the potential attack areas in 3PLs, where hackers can often access a lot of data about the

company and customers (Parker Software, 2021). Another risky system is electronic data interchange (EDI). As the use of EDI systems in supply chains increases, some negative aspects of these technologies have been discovered. (Calza and Passaro, 1997; Wong et al., 2012). EDIs managed by 3PL service providers have lower visibility and thus pose trust issues (Tiwari et al., 2023).

Boyes (2015) drew attention to problems with electronic data and software embedded in products. He stated that counterfeit digital products and software, especially in the supply chain, would create a cybersecurity breach. He defined the technologies that third parties should pay attention to as navigation devices, global data processing devices, storage devices, networking, communication infrastructure and cloud technologies. He added that security breaches in 3PLs have serious impacts on the security of goods in transit, fraud, cyber risks and supply chain integrity. Moreover, the widespread use of global navigation satellite systems (GNSS) is underestimated by many transport and fleet operators. While it is very useful from a logistics perspective, signals are vulnerable to attacks that can seriously disrupt navigation, and disruptions in satellite transmissions have a serious impact on the cyber resilience of many supply chains.

Kshetri (2022) mentioned that attackers can use stakeholders in the supply chain, such as a hardware manufacturer, supplier, logistics service providers, to infiltrate an organization's computer network. He also drew attention to spellings used by third parties. For example, in 2017, cyberattackers discovered and attacked a vulnerability in Apache Strus, an open-source Java framework. Attackers can also inject malicious code, viruses and similar things into third-party software, and supply chain members using them may also be affected (Kshetri, 2022). For example, in July 2021, an attack was made on Kaseya, a company that provides cloud-based IT management and security solutions for third parties in the supply chain. As a result, all supply chain third parties using Kaseya's systems were also affected. Numerically, it has been reported that 800 to 1500 companies were affected by the attack. Attackers performed a fake software update on an IT system used to remotely monitor servers and demanded a \$70 million ransom from companies to get their data back (Kshetri, 2022).

The reliance on 3PL in operations has also shifted supply chain risks and uncertainties to 3PLs (Gkanatsas and Krikke, 2020). Digital transformation initiated by 3PLs has led to the creation of new cybersecurity risks that affect the cyber resilience of the supply chain (Boyes, 2015). The proliferation of systems such as cloud-based systems, IoT, block chain, EDI, Enterprise Resource Planning (ERP), AI, WMS, ICS has increased these risks. In these attacks, where digital data transfer is interrupted, critical data, especially in supply chains, will no longer be usable and will cause serious damage (Gkanatsas and Krikke, 2020). These attacks on digital systems lead to disruption of operations, loss of important data that must be kept confidential, and even damage to the company's reputation. The logistics industry is particularly vulnerable to cyberattacks due to the vast amounts of sensitive information transferred between many stakeholders, including customers, suppliers and logistics providers. (Siegfried and Al-Sobaihi, 2022). The NotPetya malware attack that damaged Maersk's IT systems in 2017 resulted in the company having to shut down some of its operations for a very long period of time. As a result, Maersk had to deal with difficulties such as shipping delays and material damage, SCDs, and Maersk customers suffered serious financial losses. The attack also damaged Maersk's brand value and reputation. Customers began to worry about the security of their personal information and the products they purchased. This example shows how cyberattacks may have significant and far-reaching effects on logistics companies, underscoring the necessity of taking preventative measures to lessen the risks associated with them (Maersk, 2020). The same attack also targeted another 3PL service provider, FedEx and TNT, causing serious financial damage and disruption of operations. More recently, Toll Group, part of Japan Post, and German logistics giant Hellman Worldwide Logistics suffered a ransomware attack and were forced to disable some of their systems as a result; this led to delays, untracked packages, and missed deliveries affecting their customers' supply chains (Gkanatsas and Krikke, 2020). As carriers of goods between supply chain nodes, 3PLs need to work with upstream and downstream supply chain partners to coordinate and align supply chains when responding to SCDs like the examples above. It is not a problem of a single organization and spreads to all links in the chain (Andrés and Poler, 2015; Revilla and Sáenz, 2013).

Supply chain attacks are a powerful cyberattack that can breach even the most sophisticated security defenses through third-party connection (Nygård and Katsikas,

2022). The systems of the companies physically interact with one another via trust networks and interfaces to exchange collaborative information, such as inventory, sales data, and customer data, in order to increase efficacy and efficiency, particularly in the supply chain (PwC, 2013). The phenomenon of risk propagation known as the "domino effect" could result from interdependency and connectivity. This means that if a threat agent breaches one firm, it could expose other supply chain stakeholders to additional data risks (Kunreuther and Heal, 2003; Anderson and Moore, 2006; Huang, Hu, and Behara, 2008; Amin, Schwartz, and Sastry, 2013). Thanks to shared information and security arrangements across the supply chain, the cybersecurity of any organization within the chain is potentially only as strong as that of the weakest member of the supply chain. The attacker will exploit this by identifying the organization with the weakest cybersecurity in the supply chain and using those vulnerabilities present in their systems to gain access to other members of the supply chain. The weakest links seen by attackers are third parties and small and medium-sized businesses (Melnik et al., 2022).

Anderson and Moore (2006) also stated that due to the interconnectedness of systems, the risks of a weak link affect not only itself but also all other supply chain members. However, it has been stated that companies in an interdependent network do not invest in security and rely on the security systems of other companies in the network (Kunreuther and Heal, 2003). Therefore, it is important that security is not only within the organization but also from third parties (Wong et al., 2022).

A cyberattack on one system can have a domino effect on other systems used by stakeholders in the supply chain. A third-party weak link can increase vulnerability to attacks and cause operational disruptions (Afenyo and Caesar, 2023). Since a safety net is only as strong as its weakest link, it is critical to identify, evaluate, and reorganize the degree of exposure of weak third-party members in the supply chain in order to lower the detected risks (Zheng and Albert, 2019). Working with a weak third party on a network makes everyone more vulnerable to potential cyberattacks (Afenyo and Caesar, 2023).

All stakeholders of the supply chain are safe only if the entire chain is secure. The consequences of a successful attack rarely affect a limited stakeholder, often the

entire supply chain is affected. That's why supply chain organizations must be careful about over-reliance on third parties (Lees, Crawford, and Jansen, 2018).

Keskin et al., (2021) stated that since modern companies are dependent on third parties, strengthening the security of a company's internal network will not be sufficient and these dependencies will lead to new cyberattacks. Additionally, even if companies have the best cybersecurity practices in place, their data, customers, and reputation may be at risk from a third party. It has been explained that companies need effective and efficient methods to assess the cybersecurity risks of their partners. For this reason, in the study, existing methods for C-TPRM developed by companies were investigated and compared in order to find the indicators and criteria used in risk assessments.

Based on the literature, Gkanatsas and Krikke, (2020) pointed out that there are very few studies on building resilience in 3PL for the supply chain network. As seen in the literature, current cyberattacks on the supply chain are starting to target third-party service providers, and the effects of these attacks are evident with real examples, so companies need to evaluate the cybersecurity maturity of the third parties they work with (Pérez-Moron, 2020).

Below we list the research gaps we found through our literature review:

Colicchia, Creazza, and Menachof (2019) investigated the approaches of companies in supply chains to cybersecurity and information risk management. Research gaps have identified the need for what companies in the supply chain should do and implement to achieve cyber resilience in the entire supply chain by going beyond the binary in the context of cyber supply chain risk management processes, as well as what factors can facilitate the elimination of cybersecurity barriers.

Cheung, Bell and Bhattacharjya (2023) stated that although precautions are taken by companies in the supply chain to protect critical data and increase cybersecurity, attackers can bypass these measures. In this context, they state that there is a serious research gap regarding real-time recovery and subsequent precautions. The authors found that the literature mostly consists of precautionary measures, but real-time rescue efforts are quite limited. The need to investigate the design of a flexible backbone network that combines information sharing strategies among supply chain partners is also emphasized.

Melnyk et al (2022) argued that SMEs pose more threats in the supply chain than large companies and argued that there is a research gap in the need to address SMEs in the context of cybersecurity and the literature on this is quite insufficient.

Kshetri (2022) suggested that conducting due diligence on supply chain stakeholders and ensuring that they comply with a high standard of cybersecurity should be explored and is a key component of organizations' cybersecurity strategy.

Afenyo and Caesar (2023) drew attention to the maritime logistics side in cybersecurity and stated three research gaps. First, there is a need for research using methods such as interviewing experts to understand the key factors driving maritime cyber risks and attacks in companies' supply chains. Second, risk and resilience tools must be implemented to mitigate cyber threats. The final gap is the need for contextualized studies covering maritime cyberattacks on supply chains for companies in emerging markets.

Li and Xu (2020) suggested that attackers evaluate the security level of organizations and select targets according to the systems they can quickly invade without being detected, small companies are more vulnerable, and therefore strategic attacks may be a research gap in research. They also stated that studies generally use a two-tiered supply chain and that three-tiered supply chains should be examined in the future. Finally, examining solutions to manage third-party risks, such as appropriate security auditing or MSSs, is given as a research gap.

Tiwari et al (2023) emphasized that relevant information in the supply chain is shared in applications for all stakeholders and that further research is needed to understand the scope and type of data that can be shared between partners.

Kumar and Mallipedi (2022) revealed the research gaps in the context of cybersecurity and supply chain by preparing RQs for future research. The questions are as follows:

- How will cybersecurity risks affect existing supply chain strategies to recover from a disruption?
- How to design the supply chain networks to recover from disruptions caused by a cyberattack?

- How to design and exercise option contracts to hedge against disruption in cloud services?
- What supply chain factors strengthen or diminish the consequences of cybersecurity breaches?
- How to design and integrate Industry 4.0 and Industry 5.0 enabled supplychains to reduce the likelihood of cyberattacks?
- How will centralizing ICT infrastructure through cloud technologies aggravate or mitigate the cybersecurity supply chain risks?

Ghadge, Caldwell, and Wilding (2020) revealed the need for increased risk awareness, standardized policies, collaborative strategies, and research based on empirical models to build supply chain cyber resilience.

We wanted to conduct a study in this area due to the following findings we found in the literature review:

In their research, Creazza et.al (2022) revealed that Logistics Service Providers can play an important role in the cyber supply chain risk management process towards a more “supply chain-focused” response to cyber threats and risks. Moreover, their results showed that Logistics Service Providers can play a critical role in promoting not only collaboration but also compliance for a consistent approach to CSCRM throughout the supply chain, ultimately contributing to coordinated investments in information security in a networked environment. Moreover, they emphasize that Logistics Service Providers' protection initiatives are potential tools to guide supply chain actions. According to the literature, Logistics Service Providers can enable joint decisions and better coordination in investments in terms of cybersecurity (Li and Xu, 2020). Additionally, the need to delve more deeply into the mechanisms that Logistics Service Providers can put in place as “regulators” to encourage the adoption of a supply chain perspective on CSCRM throughout the supply chain is highlighted.

Levy and Gafni (2021) also highlighted the concept of cybersecurity footprint, argued how critical the cybersecurity footprint (that is, digital data in some way) is in terms of security in interconnected systems, and stated that an attack on third parties will spread to other stakeholders with a domino effect. Figure 2 below illustrates this domino effect.

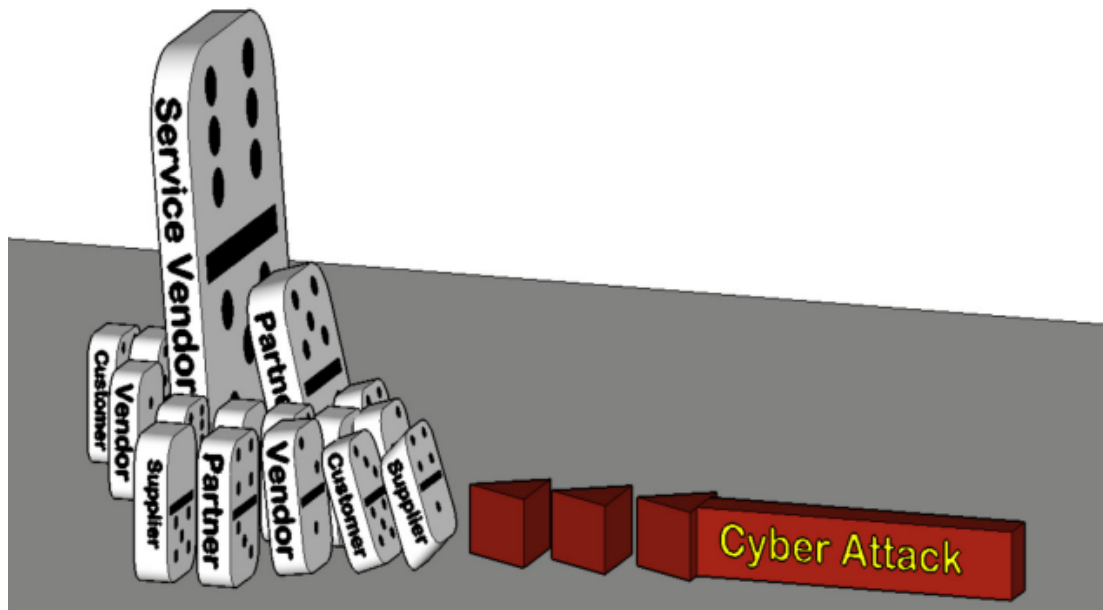


Figure 2. “Domino effect” impact of cybersecurity in supply chains (Source: Levy and Gafni, 2021). Reproduced with permission from Levy and Gafni (2021). © 2020 Emerald Publishing Limited.

Meggiato et al. (2022) are other authors who treat 3PLs as the focus. In the article, the existence of cyberattacks on supply chain operations and warehouses and the measures that can be taken to prevent these attacks are mentioned. Focusing especially on 3PL warehouses, the authors stated that the risks of cyberattacks are quite high for such companies and that research on the subject is needed.

Cheung, Bell and Bhattachariya (2021) stated in one of their studies that companies prefer 3PLs in their operations and that they may be important in the context of cybersecurity. In addition, the authors pointed out that there are few academic studies in the field of cybersecurity in this context and argued that more research should be done.

Gkanatsas and Krikke (2020) pointed out that the dynamic and changing market environment increases the importance of addressing operational risks in supply chain networks, and with these changes, a concept such as cyber risk develops and continues as a problem, and that this is a supply chain problem. They also particularly emphasized that with the increasing use of 3PLs, the risks and uncertainties existing in the supply chain spread to 3PLs. In the study, the authors studied and reviewed the literature on the development of resilient 3PL supply chain network designs through the use of operations research/management science (OR/MS). The authors emphasized

that the issue should be addressed in the context of 3PL and that there are few academic studies.

Simon and Omar (2020) suggested that a cyberattack on a single node affects multiple nodes in the supply chain, and that a network of many nodes rather than a single supply chain with a strategic attacker is a gap that needs to be investigated.

Perez-Moron (2020) mentioned that the latest cyberattacks are always carried out through 3PL companies, and therefore 3PLs are in the target position and at an important point in the context of cybersecurity.

Due to the studies carried out above and the issues emphasized, we determined our research target as working on supply chains and 3PL companies.



CHAPTER 3: THEORETICAL BACKGROUND OF THE STUDY

The systems theory has been chosen as the main theory for this research. Systems theory first emerged in 1951 thanks to Ludwig von Bertalanffy (Bertalanffy, 1951). Systems theory provides a good framework for understanding organizations as complex, open systems that are always in the process of interacting and communicating with their external environments (Katz and Kahn, 1978). It has been stated that systems theory is particularly effective in examining supply chains consisting of interconnected nodes that ensure the physical flow of materials (Towill et al., 1992). Systems theory in its current form is an intuitive and widely used theoretical foundation in the supply chain literature (Frankel et al., 2008; Manuj and Mentzer, 2008; Skipper et al., 2008).

According to the typology of systems, supply chains are social and human activity systems made up of the acts of both people and groups of persons, or companies (Checkland, 1981). The elements that make up a supply chain are people, organizations, technological infrastructure, information flows, physical goods flows, and flows of intangible services. Supply chains are designed with the intention of benefiting all parties involved by facilitating the better exchange of products, services, and information between various organizations. The argument presented here suggests that supply chains function as systems (Caddy and Helou, 2007). Supply chains are networks of economic entities, such as businesses, that voluntarily collaborate to manufacture and provide goods and services. According to Rouse (2005), supply chains are "systems of systems," and businesses are inherently systems.

Supply chains are inherently complex systems that work with multiple interconnected nodes and processes such as purchasing, supply, transportation, production, and sales (Shi, Dong and Ruan, 2009). Instead of considering the nodes in the system separately, the supply chain aims to optimize the performance of the nodes as a whole and ensure the flow of goods, information and resources without interruption. As open systems, supply chains rely on a continuous flow of inputs from their links to maintain operations, reflecting systems theory's concept of negentropy, that is, the self-maintenance of the organization through environmental inputs (Deeter-Schmelz, 1997; Zsidisin and Ellram, 2003; Bertalanffy, 1956). Disruptions in the supply chain flow, defined as unplanned and unpredictable events that disrupt the standard flow of goods, materials, and information in this system, significantly affect

the functioning of the system (Craighead et al., 2007; Svensson, 2000; Kleindorfer and Saad, 2005).

In line with the information provided by the above authors, the principles of systems theory appear to be interconnectedness, holism, dynamic interaction and feedback. Also, White (2015) determined the principles of system theory as holism, transformation, variety, feedback, control, autopoiesis, and nearly decomposable systems. Three key findings emerged from Ackoff's (1981) analysis of system dynamics and theory: (a) systems interact and are influenced by their environment and by other systems; (b) the functioning of each system component affects the functioning of the system as a whole; and (c) the functioning of each system component is interdependent. The model below reflects Ackoff's (1981) views about what constitutes a system. Regarding the third conclusion, for example, each of the three supply chain elements depicted in Fig. 6 below is significant in and of itself, but it does not offer a whole and full understanding of what a supply chain is and how to manage it. According to Ackoff's (1981) second conclusion, each component makes a distinct as well as a connected conjoint contribution. Once more, they are justifications for the claim that supply chains are systems. Figure 3 below, through the interactions of the components indicated by the arrows, confirms Ackoff (1981) and others' conclusion that systems are dynamic.

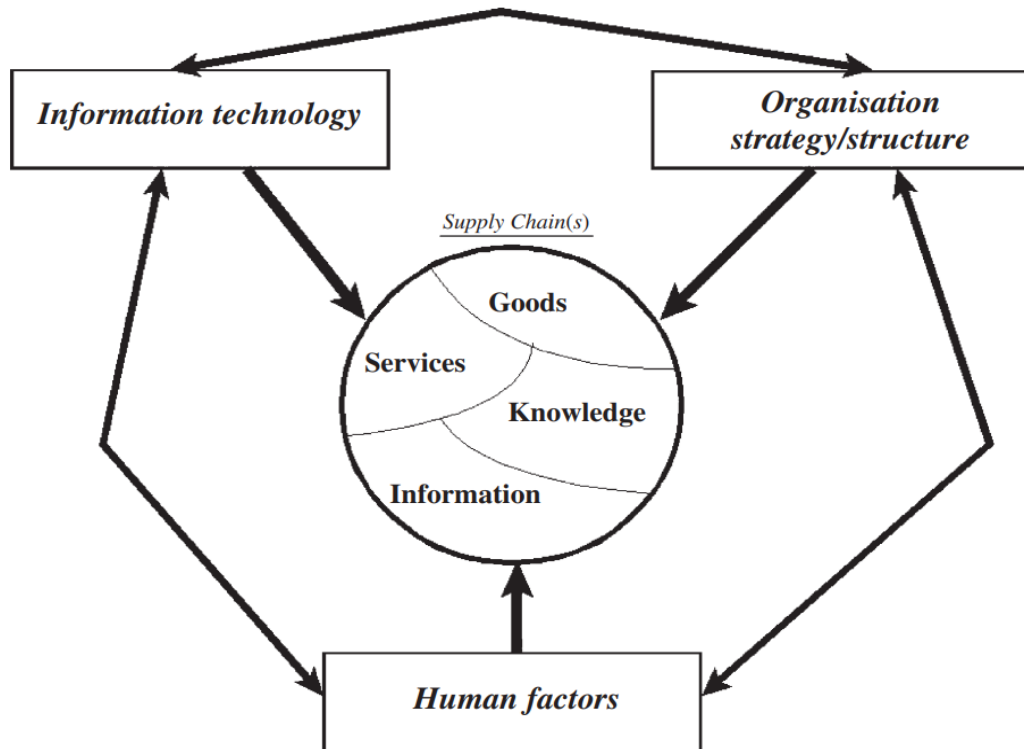


Figure 3. Generic Supply Chain Model (Source: Caddy and Helou, 2007). Reproduced with permission from Caddy and Helou (2007). © 2007 Elsevier.

Like Germain and Droge (1998), Burkhardt and Brass (1990) also argue that systems are affected by technological change. In particular, researchers suggest that a change in technology is or should be followed by a change in structure. That is, a change in the level or type of technology used in the supply chain will affect the way both organizations and their employees interact with the supply chain (Caddy and Helou, 2007). This information emphasizes that cybersecurity in 3PLs, which is the subject of our thesis, is a system problem and that it should be addressed with system theory.

In the context of our thesis, system theory assumes that the elements within the system are interconnected, which reveals the principle of interconnectedness. In the context of 3PL and supply chain, organizations in the chain (stakeholders such as suppliers, customs agents, retailers, sellers and logistics service providers) are interconnected through activities such as information, material flows and financial transactions. Therefore, in the context of system theory, in a cyberattack, it is not necessary to attack a specifically specified customer or stakeholder in order to capture

the information of a customer or any stakeholder in the supply chain, that is, the negative effects of a cyberattack on 3PLs will not only harm the 3PL company. It spreads to the supplier, manufacturer, customer and all stakeholders that are part of the chain and affects each of them.

Systems theory also suggests that the parts of the system should be understood not separately, that is, as a sum of parts, but as a whole, which gives rise to the principle of holism. This means taking into account the entire logistics network and all supply chain interactions when assessing vulnerabilities and working on ways to mitigate them to ensure cybersecurity in the 3PL. Therefore, a security measure or an improvement in cybersecurity in the 3PL not only secures the 3PL company but also affects the entire supply chain and provides a security perspective for the entire chain.

In addition, systems are dynamic and constantly evolving with technology and new trends and trying to adapt themselves to these developments. This clarifies the dynamic interactions principles of systems theory. It is seen that companies in the logistics sector, especially 3PLs, are constantly trying to adapt themselves to technological developments, new trends and changes in the market, and these reveal new supply chain risks such as cybersecurity, therefore cybersecurity measures must be dynamic, applicable and throughout the network in the context of the supply chain. It must be adaptable.

Systems operate through feedback mechanisms, where outputs of a system are fed back into the system as inputs. This explains the feedback principle. Effective cybersecurity measures in 3PL should include continuous monitoring and feedback to promptly identify and respond to threats.

Systems theory has implications for appreciating and managing sources of risk associated with supply chains. A perspective on synergy and entropy is relevant in this respect. Synergy within supply chains means the combined performance of interconnected nodes is greater than the sum of the individual performance realizations; this results in better global efficiency and competitiveness (New and Westbrook, 2004). On the other hand, entropy describes how feedback and adjustments work to keep the degradation of the system at a minimum (New and Westbrook, 2004). Taking a systems perspective in terms of supply chain, research, and practice helps in recognizing and managing the risks so that operations are made

much more robust and more flexible to variations under uncertainty. Therefore, the resilient supply chain should have solid interdependencies and channels of communication helpful in maintaining the robustness of the supply chain.

The design and operation of supply networks benefit greatly from the structuralist approach of systems theory. According to Hassan (2006), supply chain design may be improved methodically by applying the concepts of systems engineering, which can also increase supply chain dependability and effectiveness. In a similar vein, systems thinking may help ensure the robust functioning of supply chain activities and structures by supporting their methodical construction (Vrijhoef and Ridder, 2007).

Systems theory is further demonstrated in SCM by the incorporation of sophisticated production techniques and management models, such as computer integrated manufacturing systems (CIMS), flexible manufacturing systems (FMS), and ERP (Shi, Dong and Ruan, 2009). The efficient movement of money, information, and logistics is made possible by these technologies, which raises the supply chain's overall competitiveness. For example, developments such as ERP systems have improved data flow and real-time decision-making in the supply chain, facilitating the flow of information and data between different nodes (Shi, Dong, and Ruan, 2009). However, this interconnectedness of these technological systems carries the risk that a possible disruption in one area can spread to the entire chain and affect other stakeholders (Craighead et al., 2007)

We will use systems theory in this thesis because of the above-described information of systems theory, its compatibility with the supply chain, its principles, and the fact that a comprehensive framework for evaluating and improving supply chain operations is provided by systems theory. Moreover, because we view the supply chain as a dynamic and multi-linked system, we chose systems theory to identify how cybersecurity risks permeate the entire system throughout the network and affect overall system performance. Cybersecurity in 3PL must consider the overall logistic network with its interactions to add dynamism to the measures to counter the ever-growing threat environment. According to the literature, systems theory offers versatile approaches to address and improve the structure of the supply chain. The theory also emphasizes that all stakeholders in the chain are interconnected and

constantly interact. In this context, systems theory provides insights into optimizing performance, managing outages and risks, and increasing overall system resilience.



CHAPTER 4: METHODOLOGY

This thesis employs a qualitative research design using semi-structured interviews (Flick, 2014) to comprehensively address the RQs related to cybersecurity in 3PL service providers and to address the ripple effects of 3PL-centric cyberattacks on all stakeholders, namely the supply chain in general. Figure 7 shows the RQs, and the research method used for the RQs. The use of semi-structured interviews is crucial for capturing the complex and multifaceted nature of cybersecurity challenges in 3PL service providers and their ripple effects across the supply chain. Moreover, semi-structured interviews provide in-depth qualitative insights by allowing industry experts to share their experiences with cyberattacks and discuss the challenges they have faced. This method is particularly valuable in identifying the most effective mitigation strategies, as it enables participants to detail the cybersecurity measures, they have implemented and offer expert opinions on best practices (Wilson, 2013). Additionally, by gathering perspectives from various supply chain stakeholders, this approach enhances the validity and reliability of the findings, ensuring a comprehensive understanding of the RQs. Figure 4 below shows the methods used for the research questions.

Research Question	Method
RQ1: How do cyberattacks on 3PL service providers generate a ripple effect throughout the supply chain, impacting its stakeholders?	Semi-Structured Interview
RQ2: What are the mitigation strategies for a cyber attack on third-party logistics service providers?	Semi-Structured Interview

Figure 4. Method descriptions for RQs.

4.1. *Semi-Structured Interview*

The semi-structured interview method was chosen to explore how cyberattacks on 3PL service providers impact the overall efficiency and resilience of the supply chain and explore the strategies to mitigate the ripple effects of cyberattack on 3PLs. The overall purpose of a semi-structured interview is to collect systematic information about a handful of primary subjects while also allowing for some exploration when new issues or topics arise (Wilson, 2013). Semi-structured interviews are a prominent research approach in the social sciences (Ruslin et al., 2022). According to Hyman et al. (1954), interviewing is a universal method of inquiry in the social sciences. Magaldi and Berler (2020) describe a semi-structured interview as an experimental one. They

go on to say that the semi-structured interview is normally guided and focused on the main issue, which gives a broad pattern. Furthermore, Megaldi and Berler (2020) suggest that the semi-structured interview, despite the thematic paths offered prior to the session, allows a researcher to go deeper for a finding. Semi-structured interviews are seen to be appropriate for gathering information that is more likely to be expressed in an openly planned setting (Flick, 2014).

Semi-structured interviews provide a good perspective for gathering complex situations, emerging problems, facts, attitudes and opinions on them, and create the opportunity to raise new issues with open-ended questions. It is used to collect data that cannot be directly observed due to timing, privacy, dangers, etc. (Wilson, 2013).

One of the main advantages is that the semi-structured interview method has been found to be successful in enabling reciprocity between the interviewer and participant (Galletta and Cross, 2013), enabling the interviewer to improvise follow-up questions based on participants' responses (Hardon, Hodgkin and Fresle, 2004; Rubin and Rubin, 2005; Polit and Beck, 2010) and allowing space for participants' individual verbal expressions (RWJF (Robert Wood Johnson Foundation), 2008). Moreover, unlike structured interviews, it can reveal unknown issues and provides flexibility to the researcher. The use of semi-structured interviews requires a certain level of previous study in the research topic area (Wengraf, 2001; RWJF, 2008; Kelly, 2010) because the interview questions are based on previous knowledge. It is ethically dubious to collect data that is not completely necessary for the research (Gibbs et al., 2007). Therefore, while determining the RQs, cybersecurity has been researched for a long time with a literature review in the context of supply chain and logistics and the necessary preliminary infrastructure has been provided. Semi-structured interview questions were also prepared within the framework of this literature review.

Cyber attacks, a relatively new concept with evolving technologies, their complex and multifaceted nature and their impact on supply chains require a method that can obtain detailed, nuanced insights from participants. Semi-structured interviews allow for the exploration of specific themes and topics, while also providing the flexibility to delve more deeply into specific areas of interest or importance that arise during the conversation (Wilson, 2013). This ensures that interviews can adapt to the expertise and experiences of each participant and capture the rich, qualitative

data necessary to understand the complex dynamics at play (Wilson, 2013). Additionally, this method balances the need for consistency across interviews with the flexibility to explore individual perspectives in depth (Wilson, 2013). A predefined set of questions ensures that all relevant topics are covered, which helps in systematically comparing responses between different participants (Wilson, 2013). At the same time, the open-ended nature of the questions encourages participants to detail their experiences and insights, revealing aspects of the topic that were not anticipated by the researcher (Adeoye-Olatunde and Olenik, 2021). Moreover, the method is well-suited for the participation of professionals with first-hand experience of cybersecurity in supply chain and logistics (3PL providers). These individuals can provide detailed descriptions of specific events, explain immediate and long-term impacts on supply chain operations, and provide insights into measures taken to mitigate these impacts. Their perspectives are invaluable in understanding the real-world impacts of cyber threats and the resilience strategies used in the industry.

In light of the semi-structured interview literature described above, the semi-structured interview method was chosen due to its ability to provide context-rich data that can in-depth reveal the complexity of cyberattacks against 3PL providers and their ripple effects on supply chains. According to the literature, the method's flexibility and depth of inquiry have made it the most likely choice for exploring the nuanced and multifaceted nature of the RQs.

When it is necessary to evaluate a newly designed or already existing issue, the evaluator should collect information about the issue from more than one person during this process (Gugiu and Rodríguez-Campos, 2007). In this context, in a semi-structured interview, determining the information sources to be interviewed is an important process (Gugiu and Rodríguez-Campos, 2007). When we consider that the supply chain consists of stakeholders connected to each other in the network structure, the problems that a cyberattack in the 3PL sector will create will not only affect the 3PL company but also other stakeholders in the supply chain. For this reason, while creating the interviews, we included participants mainly from 3PL companies, in addition to these, Customs Consultancy Companies, Ports and Manufacturers. The RQs were written based on the literature review.

An interview questionnaire was prepared containing 22 main questions and 13 sub-questions related to the 3PL sector, cybersecurity in the 3PL sector, technology use and data transfer between stakeholders, the effects of cybersecurity on the 3PL company and supply chain, current measures and strategies used, and a total of 35 open-ended questions. Before the question phase, each interviewee was given a detailed information form so that they could have better information about the research.

During the interview, we noticed that some participants had difficulty understanding the questions and giving the answers we expected, so we tried to elaborate on the way we asked questions by giving examples and to open the participant's horizons and to ensure that they gave more detailed answers, and this method worked. The interview durations varied completely from participant to participant. For example, interviews were held for 105 minutes, 60 minutes, 40 minutes, and 35 minutes. During the interviews, additional questions were asked according to the participant's situation in order to make the participant more active and to elaborate on the topics. In that way, the participants were able to give more examples and make more explanations.

In this master's thesis, a group of interviewees who are experienced in the sector and have expertise in these subjects, mainly from 3PL companies and supply chain stakeholders connected to these companies, were determined and semi-structured interviews were conducted with them. Table 1 shows the sample size of the interviews. The sample group includes 4 different types of actors, 16 companies and 18 interviewees.

Table 1. Sample Size of Interviews.

Supply Chain Member	Interviews	
	#N (company)	#N (people)
3PL Company	10	12
Customs Consultancy	2	2
Importers/Exporters (OBM)	2	2
Port	2	2
Total	16	18

Then the information obtained through the semi-structured interview was analyzed using content analysis and the responses of the participants were examined and analyzed, and the results were explained.

4.1.1. Sample of Interviews

In this study, in-depth information was obtained on cybersecurity, data management and the effects of cybersecurity on the supply chain in the logistics sector through semi-structured interviews. A purposive sampling method was employed in selecting the participants (Campbell et al., 2020; Eisenhardt, 1989). Participants were strategically selected from global 3PL companies in İzmir, Türkiye. Recognizing the interconnected nature of supply chains, the interview sample also included collaborating ports, customs agencies, and manufacturing firms (importers/exporters) to provide a holistic view. Global 3PL companies operating in İzmir, Turkey, were chosen, with a particular focus on firms that had experienced cybersecurity incidents in the past. We contacted many 3PLs other than the ones we selected during the sample selection phase, but we eliminated these 3PLs because we thought that companies with experience on the subject would provide more accurate results. In total, eighteen participants from sixteen different companies, all operating within the same supply chain network were interviewed. This diversity made it possible to comprehensively address the views and experiences of actors at different stages of the supply chain on cybersecurity and data management.

The interviewed companies are leading companies in this sector and have global operations. The participant profiles were selected to provide a broad perspective on the operational processes of the logistics sector, SCM and interactions with external stakeholders, and the connections of all these with cybersecurity. The interviewees included professionals in different positions such as operations managers, IT specialists, customs brokers, company founders and supply chain managers. This diversity enabled the evaluation of cybersecurity measures in a wide range from the implementation level to strategic decision-making processes. With this sample, it is aimed to reveal the effects of cyberattacks on the supply chain in 3PL companies and the industry from different stakeholder perspectives. Table 2 provides detailed profiles of the participants.

Table 2. Profile of the Interviewees.

SAMPLE TABLE							
Interviewee	Role	Experience	Medium	Company	Company Info	Education	Duration
3PL1	Business Development Manager	8 years	Teams Meeting	3PLA	Number of Employee: 6800 Scope: International Services: Transportation, Warehousing, Distribution, Freight Forwarding, Supply Chain Management	BD	01:42:15
3PL2	Customer Service Support	3 years	Teams Meeting	3PLB	Number of Employee: 16600 Scope: International Services: Transportation, Freight Forwarding	BD	00:50:36
3PL3	National Customs and Trade Manager	33 years	In Person	3PLC	Number of Employee: 81000 Scope: International Services: Transportation, Warehousing, Supply Chain Management	MD	00:21:23

Table 2. Profile of the Interviewees (Continued).

3PL4	Business Development Manager	10+ years	Teams Meeting	3PLD	Number of Employee: 1000+ Scope: International Services: Transportation, Distribution, Freight Forwarding	BD	00:45:31
3PL5	Senior IT Specialist	6 years	Teams Meeting	3PLE	Number of Employee: 100000+ Scope: International Services: Transportation, Warehousing, Distribution, Freight Forwarding, Supply Chain Management	BD	00:30:36
3PL6	Sales Account Manager	6 years	Teams Meeting	3PLE	Number of Employee: 100000+ Scope: International Services: Transportation, Warehousing, Distribution, Freight Forwarding, Supply Chain Management	BD	00:44:20

Table 2. Profile of the Interviewees (Continued).

3PL7	General Manager of Information Systems Department	10+ years	Teams Meeting	3PLF	Number of Employee: 501- 1000 Scope: International Services: Transportation, Warehousing, Distribution, Supply Chain Management	BD	00:31:00
3PL8	Pricing Manager	10+ years	In Person	3PLF	Number of Employee: 501- 1000 Scope: International Services: Transportation, Warehousing, Distribution, Supply Chain Management	HS	00:18:54
3PL9	Information Security Department Manager	10+ years	Teams Meeting	3PLG	Number of Employee: 7500+ Scope: International Services: Transportation, Warehousing, Distribution, Freight Forwarding, Supply Chain Management	BD	00:58:00

Table 2. Profile of the Interviewees (Continued).

3PL10	Company Operations Manager	10+ years	In Person	3PLH	Number of Employee: 50-100 Scope: Europe Services: Transportation, Warehousing, Distribution, Freight Forwarding, Supply Chain Management	BD	00:32:06
3PL11	Seaway Operations Specialist	3 years	Teams Meeting	3PLI	Number of Employee: 1000+ Scope: International Services: Transportation, Warehousing, Distribution, Freight Forwarding, Supply Chain Management	BD	00:29:26
3PL12	Air Cargo Customer Services and Operations Manager	4 years	Teams Meeting	3PLJ	Number of Employee: 101-500 Scope: International Services: Transportation, Warehousing, Supply Chain Management	BD	00:30:00
P1	Software Development Manager	10+ years	Teams Meeting	PA	Number of Employee: 501-1000 Scope: International Services: Transportation, Warehousing	BD	01:39:43

Table 2. Profile of the Interviewees (Continued).

P2	IT Manager	10+ years	Teams Meeting	PB	Number of Employee: 101-500 Scope: International Services: Port Management	BD	00:36:51
CC1	Founder	10+ years	In Person	CCA	Number of Employee: 50 Scope: International Services: Customs Consultancy	DD	00:25:11
CC2	IT Manager	20+ years	In Person	CCB	Number of Employee: 50-100 Scope: Europe Services: Customs Consultancy, Customs Clearance	BD	00:25:22
OBM1	Logistics Manager	6 years	Teams Meeting	OBMA	Number of Employee: 501-1000 Scope: Europe-Asia-Africa-Australia Services: Transportation, Warehousing, Supply Chain Management	BD	00:55:10
OBM2	Expert SAP Specialist	9 years	Teams Meeting	OBMB	Number of Employee: 5000 Scope: Europe-Asia-America-Australia Services: Manufacturing and Supply Chain Management	BD	00:49:56

Table 2. Profile of the Interviewees (Continued).

Total						13:06:20
Average						00:43:41
Abbreviations: 3PL is for Third Party Logistics Service Provider, P is for Port, CC is for Customs Colsuntancy, OBM is Original Brand Manufacturer, BD is for Bachelor's Degree, MS is for Master's Degree, DD is for Docorate Degree.						

4.1.2. Content Analysis Method

According to Cole (1988), content analysis is a technique for examining written, spoken, or visual communication messages. As a research tool, content analysis provides an objective and methodical way to describe and measure occurrences (Krippendorff, 1980). Content analysis can be done both qualitatively and quantitatively. These are different from each other in terms of their analysis and conclusions. If we compare them, qualitative analysis aims to understand a phenomenon rather than making generalizations with statistical inferences (Forman and Damschroder, 2007).

Through content analysis, a researcher can test theoretical hypotheses to improve comprehension of the data. Words can be reduced to fewer content-related groups by using content analysis. Words, phrases, and the like are presumed to have the same meaning when placed into the same categories (Cavanagh, 1997).

In order to provide information, fresh insights, a representation of the facts, and a useful manual for action, content analysis is a research approach for drawing reliable and repeatable conclusions from data to their context (Krippendorff, 1980). The goal of the analysis is to produce concepts or categories that describe the phenomenon in a concise and comprehensive manner (Elo and Kyngäs, 2008).

The approach of content analysis can be applied to both qualitative and quantitative data, and it can be applied in an inductive or deductive manner. The study's objectives will dictate which of these is chosen. In cases where prior knowledge regarding the phenomena is either insufficient or dispersed, the inductive approach is

advised (Lauri and Kynga's, 2005). Through inductive content analysis, the categories are produced from the data. According to Kynga's and Vanhanen (1999), deductive content analysis is employed when the study's goal is theory testing and the analysis's structure is operationalized based on prior knowledge.

Qualitative content analysis was used to systematically analyze the semi-structured interview transcripts obtained from the participants (Eisenhardt, 1989). This method allows for the interpretation of the content of text data through a systematic classification process of coding and identifying themes or patterns (Hsieh and Shannon, 2005). The analysis followed a multi-stage coding process, which began with initial coding (also referred to as "quotation" or "first-order coding"), followed by more abstract and higher-order categorization through subsequent levels of coding (second-order, third-order, and fourth-order codes), to capture the deeper meanings and relationships embedded in the data.

The first stage of the process involved open coding, where quotations and relevant textual segments were assigned, initial codes based on the data's content (Elo and Kyngäs, 2008). This "first-order coding" helped identify specific concepts and ideas, which were then grouped into broader categories in the second-order coding phase. These categories were derived inductively from the data, following an emergent approach as advocated by Krippendorff (2018), where the coding scheme evolves during the analysis rather than being pre-determined.

In the third-order coding phase, the categories were further refined and grouped into themes based on shared characteristics or underlying patterns (Weber, 1990). This stage involved merging similar categories and distinguishing between different themes to ensure that the classification captured all relevant aspects of the data. The final stage, fourth-order coding, focused on the abstraction and synthesis of the themes into overarching theoretical constructs or narratives that reflect the interviewees' shared experiences and insights (Schreier, 2012).

To ensure the reliability of the coding process, the data was analyzed iteratively, with the coding framework being reviewed and adjusted as new themes emerged. This approach aligns with qualitative research principles, where the researcher remains open to modifying their understanding as new insights are discovered during analysis (Schreier, 2012). The use of multiple coding levels allowed

for a comprehensive analysis that captured the complexity of the data while retaining the richness of participants' responses.



CHAPTER 5: FINDINGS

This chapter presents the key findings of the study, highlighting the significant impacts of cyberattacks on 3PL service providers and the broader supply chain. The results indicate that cyber threats not only disrupt the operational efficiency of 3PL firms but also compromise the overall resilience of supply chain networks.

A critical finding is that when a cyberattack targets a 3PL provider, the effects extend beyond the firm itself, spreading throughout the supply chain in a domino-like fashion. Even in cases where integration levels between stakeholders are lower, vulnerabilities persist, leading to indirect disruptions in operational processes. While a lower level of integration may reduce the risk of data breaches, system failures, or ransomware propagation, supply chain operations remain susceptible to delays and inefficiencies due to their interconnected nature.

Additionally, the findings reveal that cyberattacks have both immediate and long-term consequences. In the short term, companies experience operational disruptions, data breaches, and communication failures. Over the long term, the impacts intensify, leading to financial losses, reputational damage, customer trust erosion, business relationship deterioration, increased operational costs, and heightened vulnerability to future attacks. These long-term effects may necessitate extensive organizational restructuring and prolonged efforts to restore stakeholder confidence.

The subsequent sections will explore how cyberattacks on 3PL service providers initiate immediate disruptions and then ripple throughout the supply chain, creating widespread impacts. Subsequently, effective mitigation strategies identified in this study will be discussed, offering insights into strengthening cybersecurity resilience across supply chain networks.

5.1 Ripple Effects on Cyberattacks on 3PL

We first started the analysis by analyzing the questions we asked the participants about long-term and short-term impacts. In this context, the participants reported that the impacts were not only for the 3PL company, but that the impacts would spread to all stakeholders in the supply chain like a ripple effect or domino effect. According to our analysis results, ripple effects were categorized under the titles: Employee Impacts, Financial Impacts, Information Security Impacts, Legal

Impacts, Operational Impacts, Reputational Impacts, Industrial Impacts, Information Sharing Impacts, and Societal Impacts as short-term and long-term. These effects will be examined under nine main categories below. In Table 3, these nine categories are given together with their long and short term ripple effects.

Table 3. Short and Long Term Ripple Effects.

	Short Term Ripple Effects	Long Term Ripple Effects
Employee Impacts	Employee Stress	Employee Layoffs
		Job Losses
Financial Impacts	Cost Of Loosing Business Opportunity	Additional Security Costs
	Depreciation Costs	Bankruptcy
	Employee Overtime Cost	Business Closure
	Idle Labor Costs	Business Losses
	Increased Operational Costs	Commercial Losses
	Loss Of Capital	Cost Of Rebuilding Reputation And Trust
	Loss Of Sales	Cost Of Regaining Customers
	Penalty Costs	Cybersecurity Investment Cost
	Product Quality Issues	Facility Closures
	Vehicle Wait Time Costs	Global Trade Disruptions
		Increased Operational Costs
		Loss Of Market Share
		Macro Economic Issues
		National Economy Disruptions
		Operational Losses
		Penalties
		Regulatory Complicance Costs
		Restructuring Costs
Information Security Impacts	Customer Data Exposure	Disclosure Of Trade Secrets And Confidential Business Information
	Customs Data Exposure	Know-How Leak
	Data Manipulation	Opportunistic Data Breach
	Data Security Losses	Sustained Cybersecurity Threats
	Financial Data Exposure	
	Personal Information Breach	
	Pricing Strategy Exposure	
	Product Data Exposure	
	Proprietary Data Breach	
	Route Data Exposure	

Table 3. Short and Long Term Ripple Effects (Continued).

	Short Term Ripple Effects	Long Term Ripple Effects
Information Security Impacts	Sensitive Data Exposure	
	Supplier Data Exposure	
	Trade Documents Exposure	
	Trade Secrets Exposure	
	Transportation Data Exposure	
Legal Impacts		Legal Sanctions
Operational Impacts	Bottlenecks In Inbound Operations	Business Disruptions
	Chaos In Global Logistics	Disrupted Financial Operations
	Container Tracking Failures	Facility Closures
	Delivery Delays	Human Resources Issues
	Disrupted Air Freight Operations	Loss Of Resources
	Disrupted Delivery Operations	Operational Breakdown
	Disrupted Import/Export Operations	Production Shutdown
	Disrupted Shipping Operations	Supply Chain Breakdown
	Distribution Breakdown	Time To Recovery
	Downtime In Customer Operations	Resource Challenges
	Global Trade Interruption	
	Limited Data Availability and Accessibility	
	Logistics Planning Confusion	
	Loss Of Operational Data	
	Operational Breakdown	
	Operational Congestion	
	Operational Data Insecurity	
	Operational Delays	
	Order Fulfillment Failure	
	Performance Inefficiency	
	Routing Inefficiencies	
	Service Performance Issues	
	Shipment Tracking Failure	

Table 3. Short and Long Term Ripple Effects (Continued).

	Short Term Ripple Effects	Long Term Ripple Effects
Operational Impacts	Supply Chain Breakdown	
	Transportation Planning Issues	
Reputational Impacts	Customer Dissatisfaction	Customer Dissatisfaction
		Loss Of Business Partners
		Loss Of Customers
		Loss Of Reputation
		Loss Of Trust
		Reduced Loyalty
		Reputation Recovery Issues
Industrial Impacts	Cancelled Order Surplus	Increased Product Prices
	Increased Transportation Charges	Spread Of Counterfeit Products
		Unfair Competition
Information Sharing Impacts	Communication Breakdown	
	Cooperation Challenges	
	Integration Challenges	
	Loss Of Data	
	Software Integration Issues	
Societal Impacts	Scarcity In the Supply of Critical Products	

5.1.1. Employee Impacts

Looking at employee impacts, in the short term, cyberattacks contribute to increased employee stress from addressing disruption pressures, uncertainties, and extra workload. Employees feel burnt out as they try to get operations back to normal and deal with crisis management. In the long term, the above-stressed factors lead to even worse outcomes, such as job losses and employee lay-offs. Organizations experiencing losses of finances and efficiency in operations often turn to downsizing, thereby affecting employee stability as well. Table 4 gives answers from industry experts about employee impacts.

Table 4. Codes and Participant Responses of Employee Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Job Losses	Employee Impacts	Long Term Ripple effects	<i>"Moreover, we have some customers. Especially in the automotive sector, the production line may stop if we do not supply, production may stop. You can imagine that it will cause serious losses. Therefore, I think the effect is no less than banking, that's why I always say these when people ask if we are a bank, we are not a bank, but in fact we are in a sector where we can lose more money or jobs." (3PL9)</i>
Employee Layoffs	Employee Impacts	Long Term Ripple effects	<i>"Also, there are factory costs like electricity, water, depreciation, etc. These are short-term losses, but in the long term, they can lead to layoffs, factory closures, or shop closures." (MNI)</i>
Stress Issues	Employee Impacts	Short Term Ripple effects	<i>"The additional operational load placed on all units resulted in increased pressure, with everyone exerting extra effort to continue operations in any way possible." (3PL1)</i>

5.1.2. Financial Impacts

Short-term financial losses in the financial implications originate from missed business opportunities, higher operational costs, penalty charges, and idle labor and equipment depreciation costs. Other losses include overtime expenditures by employees, missed sales, and truck idle time losses due to delayed shipments. In the longer term, the above economic burdens shift to even higher structural challenges. Businesses encounter bankruptcies, plant shutdowns, and national economic disruption. Rebuilding reputations and replenishing customers come at the expense of even more economic hardship. Other expenditures incurred include regulatory compliance expenditures, restructuring expenditures, and investment in cybersecurity, which considerably raise the economic liabilities, further making long-term recovery harder. Table 5 presents industry experts' responses to the financial implications.

Table 5. Codes and Participant Responses of Financial Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Increased Operational Cost	Financial Impacts	Short Term Ripple Effects	<i>"An attack not only affects logistics companies but also other links in the chain. For example, retailers may not receive the product on time, which causes problems in their stock management. When products that should not reach customers are delayed, customer satisfaction decreases and there is a loss of trust on the customer side. This process also causes costs to increase. Late delivery of products triggers the replanning of logistics operations, additional costs and a general inefficiency in the supply chain." (3PL10)</i>
Penalty Cost, Truck Wait Time Cost, Product Quality Issues	Financial Impacts	Short Term Ripple Effects	<i>"Of course, short-term effects, the demurrage costs that will occur when the cargo that has finally arrived or will depart remains in the container or in customs, in other words, port and container usage fees, as well as what we call truck layover fees, these are short-term costs. However, if there is a material that needs to be delivered and complied with on time, possible problems may arise because it does not arrive. In other words, the things that will arrive in the short term are usually financial." (3PL4)</i>
Cost of Losing Business Opportunity	Financial Impacts	Short Term Ripple Effects	<i>"Immediate issues, like the ones I mentioned from my previous job, would halt our daily operations and make us unable to perform tasks. For example, we couldn't do any work when emails didn't come through for half a day, and we missed out on opportunities." (3PL1)</i>

Table 5. Codes and Participant Responses of Financial Impacts (Continued).

Loss of Capital, Loss of Sales, Truck Wait Time Costs, Employee Overtime Costs, Idle Labor Costs, Depreciation Costs	Financial Impacts	Short Term Ripple Effects	<i>"In the long term, they would directly close the factory, that's where it would lead. Because as I mentioned, I work for a large company, and from what I've observed, during these moments, they really experience a significant cash loss. They experience a serious cash loss in these short-term situations. However, in the long term, for example, we've had situations where we couldn't resolve an issue in a day or two. Let me give you an example: maintenance work will be done from midnight Saturday to 8 AM Sunday. This was for resolving an issue we faced two days ago. Because of this, we couldn't issue invoices. This resulted in lost sales and transport costs. Essentially, we are working with one less shift. One less shift means one less transport, which translates to 100 trucks. If you calculate it at 40,000 lira per truck, that's the loss we have right from the start. Then there are the costs for employees; they are going to work but not doing anything. You could say they're getting paid for nothing. Also, there are factory costs like electricity, water, depreciation, etc. These are short-term losses, but in the long term, they can lead to layoffs, factory closures, or shop closures." (MN1)</i>
Additional Security Costs	Financial Impacts	Long Term Ripple Effects	<i>"Of course, increasing security measures also causes extra costs. This may increase disruptions or additional costs of resources or security chain costs. In other words, our measures will also increase the cost." (3PL2)</i>

Table 5. Codes and Participant Responses of Financial Impacts (Continued).

Restructuring Costs, Business Losses,	Financial Impacts	Long Term Ripple Effects	<i>"In the long term, the effects of attacks become more complex, including loss of customer trust, damage to business partnerships, financial losses and restructuring processes. Such attacks can seriously damage the reputation of companies and have a negative impact on future business volumes. In addition, restructuring business processes and closing security gaps entail significant costs."</i> (3PL2)
Global Trade Disruptions	Financial Impacts	Long Term Ripple Effects	<i>"Depending on the size of the attack, some companies may have to stop their operations for days or weeks. Especially if a global logistics provider company is subject to a cyberattack, it can disrupt not only local but also international operations. This creates a chain reaction and can even cause global trade to be disrupted. For example, stopping operations at a port or distribution center immobilizes other stakeholders and causes delays throughout the entire supply chain."</i> (3PL10)
Bankruptcy	Financial Impacts	Long Term Ripple Effects	<i>"So if we are interrupted for 3 weeks, we will probably close down, we will close down. That's why a backup system needs to be able to get back on its feet immediately, and this is where backups are very important. You need to replace the loss of a few days of data with a backup, or you need to accept it and then get it back on its feet immediately. But it's really interesting that such a big systematic outage lasted for 3 weeks and it's still standing."</i> (3PL7)

Table 5. Codes and Participant Responses of Financial Impacts (Continued).

Cybersecurity Investments Costs, Business Losses	Financial Impacts	Long Term Ripple Effects	<i>"Long-term effects include loss of customer trust, loss of reputation for the company, and the need for additional security investments. And again, loss of customer and reputation can lead to a decrease in the company's business volume and financial losses." (3PL11)</i>
--	-------------------	--------------------------	---

5.1.3. Information Security Impacts

In short-term information security ramifications, there is exposure of confidential information like customer data, pricing strategies, suppliers information, trade documents, and shipping information. Some of the immediate risks include financial information leakage, trade secret misappropriation, and personal information disclosures, with immediate danger to corporate security and reputation. Long-term ramifications include the perpetual risk of cyberthreats and permanent disclosure of trade secrets and proprietary information. Leaked information has the potential to help competitors and bring unfair competition and long-term reputational harm. Moreover, information and knowledge leaks have the potential to alter industry behavior and create new security threats. Table 6 presents answers from industry experts regarding information security ramifications.

Table 6. Codes and Participant Responses of Information Security Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Data Manipulation, Sensitive Data Exposure	Information Security Impacts	Short Term Ripple Effects	<i>"API integrations are used to share data between companies and their stakeholders, but weak API security measures can create serious risks such as data manipulation or leakage. Unauthorized access through APIs can disrupt operational processes and may also cause sensitive data to be exposed." (3PL2)</i>

Table 6. Codes and Participant Responses of Information Security Impacts
(Continued).

Customer Data Exposure, Product Data Exposure, Financial Data Exposure, Supplier Data Exposure, Trade Secrets Exposure	Information Security Impacts	Short Term Ripple Effects	<i>"Information theft is another effect. The seizure of customer data, product information, billing and payment information, supplier information or trade secrets through cyberattacks can cause serious damage to stakeholders. This type of information theft can provide an advantage to competitors." (3PL2)</i>
Customer Data Exposure, Product Data Exposure, Financial Data Exposure	Information Security Impacts	Short Term Ripple Effects	<i>"For stakeholders, it results in loss of trust in the company, theft of customer data, products, invoices, payments, etc. This also brings legal problems." (3PL10)</i>
Route Data Exposure	Information Security Impacts	Short Term Ripple Effects	<i>"My customer is affected, my supplier is affected, they can take my price and affect it. If the attackers achieve their goal, they will have all the data, the route, what I will do, when, where and how I will do it, all the records of income and expenses. This will spread to the market and make it difficult for me to both gain credibility and keep the job." (3PL8)</i>
Sustained Cybersecurity Threats	Information Security Impacts	Long Term Ripple Effects	<i>"Long-term effects can be complex and sustainable, and customers may lose trust at the first stage. This damages the reputation of companies. Regaining customers is challenging in terms of time and resources. In addition, the risk of constant cyberattacks increases the operational costs of companies and brings with it new security measures that need to be invested in. " (3PL10)</i>

Table 6. Codes and Participant Responses of Information Security Impacts (Continued).

Disclosure of Trade Secrets and Confidential Business Information	Information Security Impacts	Long Term Ripple Effects	<i>"Therefore, this information should not be leaked in any way, both commercially and also because a country has a certain export orientation. For example, there may be cases where it targets a certain market for export in certain goods. It is completely natural that all such information is sensitive, first of all." (3PL3)</i>
Disclosure of Trade Secrets and Confidential Business Information	Information Security Impacts	Long Term Ripple Effects	<i>"Secondly, there is also the import part of this. Because most of the goods exported today are imported anyway. This import information is also important, there is nothing to argue about. If it is not known, what happens, if it is not known, this happens, if these things are not followed, all the commercial information about a country can be circulating around." (3PL3)</i>
Disclosure of Trade Secrets and Confidential Business Information	Information Security Impacts	Long Term Ripple Effects	<i>"The issue I mentioned earlier is entirely instantaneous. But in the long term, if this data falls into someone else's hands and they use it to create different processes, for example, if information about a customs broker is given to another customs broker, saying 'this company does this and that, and does it like this,' and the other customs broker gets involved and connects the relevant company to themselves, the current customs broker working as a stakeholder could lose their customer." (P1)</i>

5.1.4. Legal Impacts

When we examine Legal Impacts, there is no mention made about any legal implications occurring in the short term by industry experts. But in the long term, there has been evidence to come to light which says companies might experience legal penalties because of violations of data privacy, breach of contracts and failure to comply. Table 7 provides responses from industry experts on legal impacts.

Table 7. Codes and Participant Responses of Legal Impacts.

Second Order code	Third Order Code	Fourth Order Code	Quote
Legal Sanctions	Legal Impacts	Long Term Ripple Effects	<i>"For stakeholders, it results in loss of trust in the company, theft of customer data, products, invoices, payments, etc. This also brings legal problems." (3PL10)</i>
Legal Sanctions	Legal Impacts	Long Term Ripple Effects	<i>"In the long term, there will be a loss of trust and reputation damage. Companies may lose customer relationships, which can cause difficulty in gaining new customers in a domino effect. Apart from these, legal sanctions and financial penalties may also come to the agenda as a result of cyberattacks." (3PL 12)</i>

5.1.5. Operational Impacts

When we examine Operational Impacts, short-term disruption takes the form of delay, congestion, container tracking inaccuracies and worldwide logistics congestion. Businesses experience service performance degradation, inefficiencies in routes and fulfillment mistakes, resulting in significant operations slowdowns. In the longer term, the operational failures may escalate to large-scale business disruption, plant shutdown and SCD. Businesses experience shortages in resources, production slowdown and finance operations breakdown. Table 8 provides responses from industry experts on operational impacts.

Table 8. Codes and Participant Responses of Operational Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Supply Chain Breakdown, Delivery Delays	Operational Impacts	Short Term Ripple Effects	<i>"DDOS attacks overload a system, making its services inaccessible. Since systems used in supply chains are particularly time-critical in terms of operations, such attacks can seriously disrupt operations. It can lead to consequences such as system failure, products not being delivered on time, and communication disruptions." (3PL2)</i>

Table 8. Codes and Participant Responses of Operational Impacts (Continued).

Operational Data Insecurity	Operational Impacts	Short Term Ripple Effects	<i>"API integrations are used to share data between companies and their stakeholders, but weak API security measures can create serious risks such as data manipulation or leakage. Unauthorized access through APIs can disrupt operational processes and may also cause sensitive data to be exposed." (3PL2)</i>
Shipment Tracking Failure, Operational Breakdown	Operational Impacts	Short Term Ripple Effects	<i>"Cyberattacks can have serious impacts on both the immediate and long-term resilience of the supply chain. Immediate impacts include downtime, data loss, and disruption of logistics flow. For example, if a system is compromised, companies cannot track shipments, communication in the supply chain is disrupted, and operational processes are paralyzed." (3PL2)</i>
Supply Chain Breakdown	Operational Impacts	Short Term Ripple Effects	<i>"Depending on the size of the attack, some companies may have to stop their operations for days or weeks. Especially if a global logistics provider company is subject to a cyberattack, it can disrupt not only local but also international operations. This creates a chain reaction and can even cause global trade to be disrupted. For example, stopping operations at a port or distribution center immobilizes other stakeholders and causes delays throughout the entire supply chain." (3PL10)</i>
Supply Chain Breakdown	Operational Impacts	Short Term Ripple Effects	<i>"We can say that the biggest impact on this issue is the operational shutdown, as the damage that occurs on the general supply chain creates a domino effect and reaches all stakeholders." (3PL10)</i>

Table 8. Codes and Participant Responses of Operational Impacts (Continued).

Delivery Delays, Distribution Breakdown, Global Trade Interruption	Operational Impacts	Short Term Ripple Effects	<i>"Yes, when we look at our sector, it can cause serious problems on the port side. As I said, I am saying it once, there is actually a chain reaction of unrest here, which can go as far as our inability to dock a ship, our inability to share container information with our stakeholders and their inability to receive their products due to this. Therefore, you become unable to do business. You cannot conduct any commercial activities in any way, very clearly. Yes, we experienced this, but we managed to eliminate it within seconds. This is what set us apart here, such as the fact that the firewalls we use are up-to-date, that we use new generation firewalls." (P2)</i>
Disrupted Air Freight Operations	Operational Impacts	Short Term Ripple Effects	<i>"Apart from that, I don't think I've heard much, but we also had a problem with an airline. The cargo hadn't flown significantly. There was a lot of cargo left in the Far East. The systems were affected, they were shut down, etc." (3PL4)</i>
Container Tracking Failures, Transportation Planning Issues	Operational Impacts	Short Term Ripple Effects	<i>"Warehouses are facing issues. There is no system in place that can provide directives about where and how the containers are. For example, there are 100 containers, but Maersk doesn't know where they are. They request 200 containers, and 200 vehicles go, but there are no containers, and so on." (3PL1)</i>
Operational Breakdown	Operational Impacts	Long Term Ripple Effects	<i>"In the long term, the slowdown in operations and the financial impact are both immediate and long-term. So, the difference actually depends on when it is noticed. Because after a certain point, when it is noticed, a lot of work has already been done, but of course, since this is a job with a lot of partnerships, it may result in a reconsideration of working together on the next job." (3PL7)</i>

Table 8. Codes and Participant Responses of Operational Impacts (Continued).

Operational Breakdown	Operational Impacts	Long Term Ripple Effects	<i>"In other words, in instantaneous situations, it does not create a huge impact in terms of logistics, but in long-term attacks, in long-term incapacity situations, many links in the supply chain will be affected, and we are the most important of them, as you know. In fact, maritime transportation is a sector that has been maintained since ancient times, even if the form of maritime transportation changes, whether we call it container transportation or general freight transportation, it is actually a sector that constitutes approximately 60% or 65% of the logistics chain, so an attack on the ports in the logistics chain, long-term attacks will definitely break the chain and throw it aside." (P2)</i>
Facility Closures	Operational Impacts	Long Term Ripple Effects	<i>"If our operations are cut off for 3 weeks, we cannot export or import. Then we will have to close down the business. It is a very serious danger for us to stop operations for 3 weeks." (CC1)</i>
Production Shutdown	Operational Impacts	Long Term Ripple Effects	<i>"If the company loses this data and shares it with another port, it could lead to the loss of customers for the port as well. Due to these long-term issues, more companies, including customers, could be harmed. For example, if raw materials don't arrive on time, the company won't be able to produce them, which will put them in a difficult position with their own customers. Their deliveries will be delayed. As a result, all firms within this chain will face a trust issue, and the outcome of this lack of trust means losses at every point." (P1)</i>

5.1.6. Reputational Impacts

In Reputational Impacts, in the short term, customer dissatisfaction due to delays, service failures and security breaches emerges as the primary reputational impact. Over time, this dissatisfaction leads to greater reputational damage, such as loss of customers, reduced loyalty, and an inability to regain trust. Additionally,

businesses suffer from the loss of important partners and struggle to regain their market position. Table 9 provides responses from industry experts on reputational impacts.

Table 9. Codes and Participant Responses of Reputational Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Customer Dissatisfaction	Reputational Impacts	Short Term Ripple Effects	<i>"Of course, short-term effects, the demurrage costs that will occur when the cargo that has finally arrived or will depart remains in the container or in customs, in other words, port and container usage fees, as well as what we call truck layover fees, these are short-term costs. However, if there is a material that needs to be delivered and complied with on time, possible problems may arise because it does not arrive. In other words, the things that will arrive in the short term are usually financial." (3pl4)</i>
Customer Dissatisfaction, Reduced Loyalty	Reputational Impacts	Long Term Ripple Effects	<i>"It can also cause customer dissatisfaction. Delays in deliveries and potential decreases in product quality can lead to dissatisfaction of end customers and a decrease in brand loyalty." (3PL2)</i>
Customer Dissatisfaction, Loss of Trust	Reputational Impacts	Long Term Ripple Effects	<i>"Losing customers' trust in particular can lead to greater damage in the long run. Because as 3PL providers, we both maintain our own operations and are responsible for securely managing our customers' data and supply chains. Any vulnerability in cybersecurity can disrupt not only our systems but also our customers' operations directly." (3PL10)</i>

Table 9. Codes and Participant Responses of Reputational Impacts (Continued).

Loss of Customers	Reputational Impacts	Long Term Ripple Effects	<i>"In the long term, there may be a loss of customers in existing international trade. In other words, a product that the exporter company cannot send abroad on time may mean that the next batch will be cancelled. The customer may face anxiety." (CC1)</i>
Loss of Trust, Loss of Customers	Reputational Impacts	Long Term Ripple Effects	<i>"In the long term, there will be a loss of trust and reputation damage. Companies may lose customer relationships, which can cause difficulty in gaining new customers in a domino effect. Apart from these, legal sanctions and financial penalties may also come to the agenda as a result of cyberattacks." (3PL12)</i>
Loss of Business Partners	Reputational Impacts	Long Term Ripple Effects	<i>"In the long term, it may even lead to terminating the agreement with them. Because there has been a loss of trust and quality there." (MN2)</i>

5.1.7. Industrial Impacts

Looking at Industrial Impacts, short-term impacts include order cancellations and increased shipping costs, both of which disrupt market stability. Over time, these short-term market fluctuations translate into industry-wide challenges, such as increased product prices, increased counterfeit manufacturing, and the emergence of unfair competition. Table 10 provides responses from industry experts on industrial impacts.

Table 10. Codes and Participant Responses of Industrial Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Increased Product Prices	Industrial Impacts	Short Term Ripple Effects	<i>""So, as I said, if they attack the 3PL, they steal all the information. This causes them to shut down their system. Shutting down the system means that logistics and transportation will stop. That also means that everything will increase, you are now paying for transportation, but when the cars stop, they charge you money. In other words, the cars must always be on the move." (MN1)</i>
Cancelled Order Surplus	Industrial Impacts	Short Term Ripple Effects	<i>"For example, if we consider the automotive industry, there are many raw material orders, and if something happens in the automotive sector, orders may suddenly be cut. Since it's the automotive sector, there are also enforcement clauses, and if you're a supplier in the automotive industry, all those products may end up in your hands" (MN2)</i>
Unfair Competition	Industrial Impacts	Long Term Ripple Effects	<i>"Let me explain this issue this way: When my partner's information is stolen, that partner causes my company to lose customers. This is the biggest factor. Because when that information falls into the hands of someone else, they will present the customer with other commercial presentations and my partner may face the risk of losing that customer." (3PL10)</i>
Increased Product Prices	Industrial Impacts	Long Term Ripple Effects	<i>"Exactly. Believe me, transportation is the most important issue and this affects transportation. If transportation is affected, the market is affected. The market being affected causes the price tag of everything to increase." (MN1)</i>
Unfair Competition	Industrial Impacts	Long Term Ripple Effects	<i>"Having a security breach here means that my prices will spread to the entire sector, or they will see not only the prices but also the specifications of the products I produce when necessary, or I can say that it will reduce the respect for competition." (MN2)</i>

Table 10. Codes and Participant Responses of Industrial Impacts (Continued).

Spread of Counterfeit Products	Industrial Impacts	Long Term Ripple Effects	<i>"Counterfeit product situations may occur due to cybersecurity vulnerabilities in the environment." (MN2)</i>
--------------------------------	--------------------	--------------------------	--

5.1.8. Information Sharing Impacts

In Information Sharing Impacts, cyberattacks cause immediate communication disruptions, integration failures, and loss of critical data. Stakeholders experience collaboration challenges, making it difficult to coordinate recovery efforts. Based on responses from industry professionals, no long-term impacts have been identified. However, continued reliance on unstable or compromised systems may prolong short-term impacts if vulnerabilities are not addressed. Table 11 provides responses from industry experts on information sharing impacts.

Table 11. Codes and Participant Responses of Information Sharing Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Cooperation Challenges, Integration Challenges	Information Sharing Impacts	Short Term Ripple Effects	<i>"Apart from that, it can cause collaboration and integration problems. Cybersecurity problems can lead to collaboration and integration with other companies in the supply chain. This can reduce the efficiency of the operation." (3PL2)</i>
Loss of Data, Communication Breakdown	Information Sharing Impacts	Short Term Ripple Effects	<i>"Cyberattacks can have serious impacts on both the immediate and long-term resilience of the supply chain. Immediate impacts include downtime, data loss, and disruption of logistics flow. For example, if a system is compromised, companies cannot track shipments, communication in the supply chain is disrupted, and operational processes are paralyzed." (3PL2)</i>
Integration Challenges	Information Sharing Impacts	Short Term Ripple Effects	<i>"While each stakeholder experiences disruptions to their own systems and processes, the biggest impact is a breakdown in collaboration and a weakened supply chain." (3PL6)</i>

Table 11. Codes and Participant Responses of Information Sharing Impacts (Continued).

Software Integration Issues, Cooperation Challenges	Information Sharing Impacts	Short Term Ripple Effects	<i>"The attack also affects other partners that 3PL companies cooperate with. When data sharing between partners is interrupted, operational processes begin to fail. Especially if integrated software cannot communicate with each other, this causes a chain reaction that slows down or stops the entire supply chain. Damage to trust between partners weakens operational cooperation and puts joint operations at risk." (3PL6)</i>
Communication Breakdown	Information Sharing Impacts	Short Term Ripple Effects	<i>"After that, freight forwarders like us also experienced problems. Since we could not receive information flow from there, we could not provide information flow to the customer, etc." (3PL1)</i>

5.1.9 Societal Impacts

In the short term, cyberattacks cause critical shortages of supplies as they disrupt or slow the delivery of critical goods. They include food, medicines, and other critical materials, impacting both consumers and business entities. Their long-term impact on society has not been established. Yet, long-term global SCD has the potential to worsen economic instability and market volatility, thereby affecting overall societal welfare indirectly. Table 12 provides responses from industry experts on societal impacts.

Table 12. Codes and Participant Responses of Societal Impacts.

Second Order Code	Third Order Code	Fourth Order Code	Quote
Scarcity in the Supply of Critical Products	Societal Impacts	Short Term Ripple Effects	<i>"I mean, I have to answer this as a sector. For example, there is no sector that will not be affected. I mean, even the country could be affected because, as I said, the vast majority of our operations are pharmaceuticals, if we stop e-commerce, of course, there would be financial or reputational damage, but if we disrupt the distribution of pharmaceuticals, for example, there could be a very big problem there." (3PL9)</i>
Scarcity in the Supply of Critical Products	Societal Impacts	Short Term Ripple Effects	<i>"Now of course, the work we do is not actually our own work. Since we do the customer's work, it seriously affects whoever our current customers are. But here, we also have a customer who provides ancillary parts to an automotive company. We can stop the automotive production lines because we cannot provide this. There are drug distributions where we distribute pharmaceutical warehouses. These are not just aspirin, I mean, things like daily serums and medications, it can be an operation that can endanger the health of a patient in surgery. Therefore, this is very broad, I mean, it really affects a very wide area. It has an operational threat. As I said, we think that this will affect our customers the most, of course, very directly, directly and destructively." (3PL9)</i>

The ripple effects of cyberattacks on 3PL service providers are illustrated in Figure 5 with detailed immediate and long-term consequences.



Figure 5. The ripple effects of cyberattacks on 3PL service providers.

5.2. The Ripple Impacts of Cyberattacks on Key Stakeholders

It is outlined that a cyberattack on a 3PL service provider can trigger a chain reaction, potentially exposing numerous stakeholders to substantial risks, particularly, 3PL service providers, importers/exporters, ports, customs agencies, shipowners and retailers. Table 13 outlines the impacts observed across these six key stakeholders.

Table 13. Impacts of Cyberattacks on Stakeholders.

Ripple Effects	3PL Service Provider	Importer/Exporter	Port	Customs	Shipowner	Retailer
Employee	X	X	X			
Financial	X	X	X	X	X	X
Information Security	X	X	X	X		
Legal	X		X			
Operational	X	X	X	X	X	X
Reputational	X	X	X		X	X

Table 13. Impacts of Cyberattacks on Stakeholders (Continued).

Industrial	x	x				
Information Sharing	x	x	x	x		

Regarding the types of impacts, it is observed that 3PL firms, as the initial target of the cyberattack, experience all the impact categories presented in the table below. Importers and exporters, following 3PLs, are affected by almost all impact factors. However, they are not specifically impacted by legal issues. Looking at ports, since these organizations are subject to taxes and tariffs, cyber incidents in this domain lead to legal consequences. However, unlike other stakeholders, ports do not experience industrial impacts, such as loss of competition. Operational and financial impacts are common across all stakeholders, reinforcing the ripple effect concept. Specifically, a cyberattack originating from a 3PL firm spreads financial losses and operational disruptions to all other actors. Regarding customs firms, they are the most affected by information security impacts, as they store trade secrets and customs documents for the entire supply chain. However, they do not face reputational impacts as a direct consequence. In the case of shipowners, they are mainly affected through the aspects of finance, operations, and reputation. Information security and information sharing implications affect four of the six actors, leaving behind retailers and shipowners. Finally, looking at industrial implications, we have the finding that importers, exporters, and 3PL companies are affected only. This is attributed to the level of competition and market substitutes in such industries.

5.3. Detailed Impacts by Stakeholder

This section examines the specific impacts of cyberattacks on different supply chain stakeholders. While the main targets are the 3PL service providers, the ripples reach many entities such as importers, exporters, shipping terminals, customs brokers, owners of vessels, and retailers. The identified impacts will then be discussed in detail for each of the following stakeholders. The detailed impacts on stakeholders are provided in Table 14.

Table 14. Detailed Impacts on Stakeholders.

		3PLs	Importer/ Exporter	Ports	Customs	Ship owners	Retailers
employee impacts	employee demotivation	X					
	employee layoffs		X	X			
	employee overtime	X					
	employee stress	X	X				
	job losses	X					
	Loss of talented employees	X					
	reduced employee productivity	X					
financial impacts	additional security costs	X	X				
	bankruptcy	X	X				
	business losses	X	X				
	cost of extra personnel	X					
	cost of losing business opportunity	X					
	depreciation costs			X			
	downsizing	X					
	financial loss	X	X	X		X	
	global trade disruptions			X	X		
	increased operational costs	X	X	X			
	increased product prices		X				
	insurance costs	X					
	loss of capital	X					
	loss of investor interest	X					
	loss of market share	X	X				
	loss of sales	X	X				X
	lost deliveries	X					
	penalty costs	X		X			
	product quality issues		X				X

Table 14. Detailed Impacts on Stakeholders (Continued).

financial impacts	ransom demands	X					
	reduced competitive power						X
	regulative costs			X			
	stolen deliveries		X				
	vehicle wait time costs			X			
industrial impacts	cancelled order surplus		X				
	unfair competition	X	X				
information security impacts	customer data exposure	X	X				
	customs data exposure	X					
	data manipulation	X					
	data security losses	X	X				
	disclosure of trade secrets and confidential information	X	X	X			
	email exposure	X					
	financial data exposure	X	X				
	global trade disruptions			X			
	operational data insecurity		X				
	opportunistic data breach		X	X	X		
	personal information breach	X	X		X		
	pricing strategy exposure	X	X				
	product data exposure	X	X				
	sensitive data exposure	X	X				
	software integration issues	X					
	supplier data exposure		X				

Table 14. Detailed Impacts on Stakeholders (Continued).

information security impacts	sustained cybersecurity threats	X					
	trade documents exposure	X		X	X		
	transportation data exposure	X	X				
information sharing impacts	communication breakdown	X	X	X	X		
	cooperation challenges	X					
	loss of data	X	X				
	software integration issues	X	X				
legal impacts	legal sanctions	X		X			
operational impacts	container tracking failures	X		X			
	coordination challenges			X			
	delays in import/export				X		
	delivery delays	X	X	X			X
	disrupted shipping operations	X					
	distribution breakdown	X					
	efficiency issues	X					
	finance operations breakdown	X					
	incorrect deliveries	X	X	X			
	incorrect production planning		X				
	logistics planning confusion	X					X
	loss of operational data	X					
	loss of resources	X					
	lost deliveries		X	X			

Table 14. Detailed Impacts on Stakeholders (Continued).

operational impacts	manual operations	X					
	operational breakdown	X	X	X		X	
	operational congestion	X		X	X		
	order fulfillment failure	X					
	performance inefficiency	X					
	product inventory issues		X				X
	production shutdown		X				
	service performance issues	X	X				
	shipment tracking failure	X					
	software integration issues	X		X			
	stolen deliveries		X	X			
	transportation planning issues	X					
	warehouse management failures	X					
	workflow mismanagement	X					
reputational impacts	brand damage	X	X				
	customer dissatisfaction	X	X				X
	loss of customers	X					X
	loss of reputation	X	X	X		X	X
	loss of trust	X	X				
	relationship dissolution	X	X	X			
	spread of speculations	X					

5.3.1. Detailed Impacts on 3PLs

3PL companies are centrally placed within supply chain functions and are therefore extremely exposed to cyberattacks. Consequently, such companies, as the focal point for the attack as transportation, warehousing, distribution, and SCM intermediaries, experience serious disruptions to various sectors like labor stability, finance, industrial placement, information security, execution efficiency, and reputation status.

From the perspective of the employee, cyberattacks induce a very stressful working environment, giving rise to numerous challenges for the staff. Workers often feel demotivated, as cyberattacks hinder normal operations, instill unforeseen delay, and add unplanned workloads. A sense of pressure to recover from downtime causes reduced output, as staff members take time to cope with breached digital infrastructure and inefficient manual workarounds. Staff members experience high levels of stress, as they have to work under great pressure to fix the breach in security, recover the data loss, and facilitate business continuity. In most situations, staff members are compelled to work overtime to counter the attack, resulting in burnout and low job satisfaction. With time, competent employees choose to resign due to the challenging and volatile working environment, resulting in long-term expertise loss to the firm. Table 15 below provides illustrative quotes on employee impacts on 3PLs.

Table 15. Illustrative Quotes About Employee Impacts on 3PLs.

Interviewee	Illustrative Quotes
3PL2	<i>"This situation can reduce employee motivation. Employees who have to work under constant stress will lose motivation. This situation negatively affects productivity and may cause talented employees to leave the company."</i>
3PL5	<i>"Let me put it this way, it was a period when we were working manually, working until 1 a.m. and trying to get it together. Everyone was working manually, and as I said, since we were in line, 15 people were working with 1 computer, and those who had not caught the virus worked like this. We have 3 offices in Istanbul, Izmir and Mersin, and at that time, I think there was 1 computer in Mersin, there were 2 in Izmir, and there were 3 or 4 in Istanbul. Think about it, while there were nearly 500 employees, we were working with 4-5 computers in this environment at that time. It was a very difficult period for us. "</i>

3PL1	<i>"People lost their health due to stress. However, one of the great things about Maersk was that they didn't disregard the efforts of their employees. For example, they provided drinks and meals in the offices, sparing no expense to ensure morale and motivation remained high, especially considering the extraordinary effort people were putting in. Even under normal circumstances, they are a company that prioritizes employee well-being, and I believe they managed this crisis exceptionally well. I have many friends there, and I still talk to them. The stress and challenges of that period were so intense that some even needed psychological support due to the demanding workload."</i>
------	---

Financially, 3PL firms are the most severely affected stakeholders in the supply chain due to their central role in logistics and distribution. A cyberattack can result in substantial business losses, including disruptions to freight management, warehousing operations, and order fulfillment. Additionally companies have to incur further security expenses to fend off further incursions, including investments in security infrastructure, the acquisition of specialist security staff, and system auditing. Some kinds of attacks, like ransomware attacks, may oblige companies to pay possible ransoms to access key data and business operations. Operating costs rise substantially after attacks, with companies investing in system recovery, damage control, and crisis management. All such overheads lower profit levels and weaken financial viability. Reduced revenue from sales compounds the problem further, with clients losing trust in the company's capability to provide secure logistics services. In some instances, regulatory bodies impose penalties for not protecting confidential logistics data, and insurance premiums increase due to the risk profile of the exposed company. In extreme situations, repeated cyber events resulting in prolonged economic pressure push some 3PL companies out of business, compelling some of them to withdraw from market altogether. Table 16 below provides illustrative quotes on financial impacts on 3PLs.

Table 16. Illustrative Quotes About Financial Impacts on 3PLs.

Interviewee	Illustrative Quotes
3PL2	<i>"Service interruptions can cause delays in deliveries to customers, which can lead to breaches of SLAs (Service Level Agreements) set out in customer contracts and can leave the company open to heavy fines and compensation claims."</i>

3PL2	<i>"Apart from that, of course, we may have financial losses. The company may experience serious financial losses due to interruptions, data breaches, penalties, possible ransom demands and customer losses resulting from cyberattacks. For example, we may lose our customers. Cancellation or non-renewal of customer contracts will lead to a serious decrease in the company's revenues. Customers will start looking for safer alternatives and the 3PL company may lose market share."</i>
3PL2	<i>"In addition, high security expenses are another factor. After a breach, the company may make investments to strengthen its IT infrastructure (new security software, staff training, consultancy services, etc.), which create extra costs."</i>
3PL2	<i>"Moreover, the number of companies that can withstand a complete halt in operational processes is very low. An attack like the Maersk example could push many companies into bankruptcy."</i>
CC1	<i>"Either the partner who provides the information may lead to the disclosure of these trade secrets. If they have bad intentions. This may cause the loss of business of existing customers, and since those negative reflections on the workflow cause the loss of business, the company will suffer serious financial losses."</i>

From an industrial perspective, cyberattacks contribute to unfair competition within the 3PL sector. When sensitive business information—such as trade secrets, financial records, business strategies, and personal or customer data—is exposed, competitors may gain an advantage by leveraging stolen insights. This places vulnerable companies at a serious disadvantage, as rivals have access to the information and may utilize it to poach clients, refine their internal processes, or control their pricing decisions. 3PL companies that have been the victim of cyberattacks might lose the opportunity to secure new business contracts because compromised security reputation makes potential clients reluctant to build long-term relationships with them. Moreover, 3PL companies usually land in legal trouble due to regulatory infractions linked to data breaches, specifically customer or supplier data. Table 17 below provides illustrative quotes on industrial impacts on 3PLs.

Table 17. Illustrative Quotes About Industrial Impacts on 3PLs.

Interviewee	Illustrative Quotes
3PL10	<i>"Let me say this for the stakeholders, company information should always remain confidential and company freight information should remain between the two companies. When it is passed on to a third party, this already stops the competition or our partners' customers and cargo purchases. Passing on to third parties like this makes our job very difficult. That's why we either tell our partners to use secure systems or we have to proceed in that way and proceed safely."</i>
3PL8	<i>"First of all, this is the case in the sector and in the world because everyone can go to everyone else's customer; in other words, the most important thing is that another company does not know who my customer is or does not know the value of the cargo, the type of product, the value of the goods, or does not know the payment information, the maturity information. Cyber security is one of the most important things that must be done to protect myself and my customers."</i>

Information sharing is another critical challenge for 3PL firms during and after a cyberattack. Integration problems arise when digital logistics systems, such as transportation management systems (TMS) and WMS, fail due to cyber disruptions. These integration failures prevent seamless coordination between supply chain partners, leading to inefficiencies in order processing and shipment tracking. Further compounding such issues is data losses where key supply chain documentation, such as inventory information, order information, and delivery timetables, gets overwritten or corrupted. Cooperation issues arise where impacted companies are unable to share information with customers, suppliers, and carriers, throwing overall supply chain alignment into chaos. Communication disruptions by cyberattacks complicate the situation where logistics companies cannot share updates, confirm shipments, or coordinate emergency actions. All such challenges hinder trust among parties and decrease total supply chain agility, ultimately making it much harder for impacted companies to recover from disruptions. Table 18 below provides illustrative quotes on information sharing impacts on 3PLs.

Table 18. Illustrative Quotes About Information Sharing Impacts on 3PLs.

Interviewee	Illustrative Quotes
3PL2	<i>"For example, Data System Crash: As a result of a cyberattack, the company's management systems (WMS, TMS) can be disabled. This can cause warehouse operations to stop, shipping plans to be disrupted, and even customer orders to fail to be processed. For example, a ransomware attack can cause all systems to crash, bringing the company's operational activities to a standstill."</i>
3PL2	<i>"In a situation where information is stolen or systems become inaccessible, operations are seriously disrupted. Errors occur in critical processes such as order management and inventory tracking. Data sharing with stakeholders throughout the supply chain stops, and shipments become uncontrollable."</i>
3PL10	<i>"Now, let's talk about potential risks. For example, ransomware attacks can infiltrate our systems and gain access to critical data. In such a case, our business can come to a standstill. If the ransom is not paid, we can face serious consequences such as data being deleted or disclosed."</i>
3PL5	<i>"All computers were shut down, all ships, their locations, and information were inaccessible, ships went to the wrong ports, it took more than 2 months to get the whole system back on its feet and the effects lasted up to 6 months. It took 2 months for us to be able to use the computers again."</i>

Operationally, 3PL firms experience widespread inefficiencies following a cyber incident. Delivery delays become common due to the inability to access shipment data, reroute cargo, or provide accurate estimated arrival times. Tracking errors result in misplaced shipments and incorrect delivery statuses, frustrating customers and increasing the likelihood of financial claims or contract disputes. Wrong deliveries occur more frequently when compromised systems generate incorrect routing information, leading to inefficiencies in order fulfillment. Additionally, operational data losses disrupt warehouse inventory management, making it difficult to locate products, process returns, or optimize stock levels. Performance inefficiencies arise as firms resort to manual processes to compensate for digital system failures, slowing down operations and increasing error rates. Operational interruptions further reduce service reliability, as compromised software systems prevent firms from maintaining normal workflow continuity. Warehouse management problems intensify, as cyber disruptions hinder automated stock tracking, order picking, and storage optimization, leading to inventory mismatches and logistical

bottlenecks. Table 19 below provides illustrative quotes on operational impacts on 3PLs.

Table 19. Illustrative Quotes About Operational Impacts on 3PLs.

Interviewee	Illustrative Quotes
3PL2	<i>"If we want to list them in general: of course there are effects on the company. Here we experience operational interruptions. Cyber attacks can affect the company's IT infrastructure and cause interruptions in logistics operations. This delays the processing of customer orders and deliveries."</i>
3PL2	<i>"This type of situation leads to loss of customers, loss of revenue and long-term operational disruptions for our company. Logistics planning in particular is disrupted due to delays, and products cannot be delivered on time. As in the case of Maersk, a 3-week outage can throw the entire global logistics system into chaos, and it can take months to regain customer trust."</i>
3PL6	<i>"Logistics providers, Manufacturers, Retailers, Consumers, Customs and Ports can be seriously affected. When a cyberattack occurs, logistics providers are usually the first and most directly affected parties. If the operational systems of logistics providers are disrupted by an attack, transportation and distribution processes can come to a halt. In particular, cargo, inventory and route optimization systems that are tracked with digital tools become inaccessible. This causes deliveries to be delayed or even stopped, customer satisfaction decreases, and financial losses occur. In addition, an attacked logistics provider can lose its credibility with other stakeholders."</i>
3PL3	<i>"Here is the biggest example of Maersk. Maersk could not load for about 15 days as far as I remember. It could not accept the bookings, it could not close the ships, in other words, it could not close the manifests, it could not deliver the cargo that had arrived, so the system was paralyzed."</i>
3PL5	<i>"Containers left the ports where they were not supposed to be, containers went to the wrong places, the entire operation stopped, 15 customer representatives had to work with 1 computer. It was a big chaos and trouble."</i>

Reputationally, 3PL companies have the most extreme long-term consequences of all supply chain participants. Damage to customer trust is one of the most immediate and debilitating implications, where customers question the security and trustworthiness of the affected firm. The negative reputation for vulnerability has serious consequences, as customers have to shift to substitute logistics companies with better cyber controls. Affected companies experience widespread brand damage, as the information about the cyberattack reaches the industry, tarnishing the firm's reputation. Word of mouth worsens the situation, where rivals, customers, and stakeholders discuss the firm's cyber vulnerability, reinforcing negative perceptions.

Customer dissatisfaction rises where order fulfillment is affected by late delivery and disruption in services, where order fulfillment and supply chain efficiency are reduced. With time, repeat cyber-related issues cause total disruption in business relationships, where customers and suppliers pull out from unreliable logistics providers. Combined economic pressure, operational efficiency, and reputational consequences considerably lower market share for 3PL companies, making recovery extensive and exhausting. Table 20 below provides illustrative quotes on reputational impacts on 3PLs.

Table 20. Illustrative Quotes About Reputational Impacts on 3PLs.

Interviewee	Illustrative Quotes
3PL2	<i>"It can cause reputational damage. A company experiencing a cybersecurity vulnerability can lose its reputation in the industry. This can lead potential business partners and customers to choose other companies."</i>
3PL2	<i>"In this case, partner A suffers serious damage in terms of both reputation and reliability. Theft of information can disrupt partner A's business processes, undermine operational security and efficiency. In addition, stolen information can damage the partner's relationships with customers or other stakeholders. As a result, the partner will have to incur additional costs to close the vulnerability and repair its reputation."</i>
MN2	<i>"So, it's actually a loss of trust again. That person, that supplier, will no longer want to work with us after such a security breach. It also causes your name to be tarnished in the sector. It's like it becomes more difficult for you to do business with others."</i>
3PL1	<i>"However, you could say to a supplier, 'I transport 50 containers with you every month. You are my number one supplier, and with the next one, I only transport a maximum of 15 containers.' Then one day, you might find yourself hit by a cyberattack, and everything you've done with others is exposed, and all kinds of issues arise. You will realize that the situations you thought were non-existent or lies—those little white lies you used to manage people—actually caused trouble in your commercial relationships."</i>

5.3.2. Detailed Impacts on Importer and Exporters

When we focus on importers and exporters, we find that they face all kinds of disruptions to the different aspects of their business, ranging from their employees to finances, industrial placement, information security, efficiency, and reputation.

From the employee's side, cyberattacks bring about much stress among employees due to managing uncertainties in the supply chain, late shipments, and interrupted business operations. Increased workload, along with economic insecurity, compels companies to take tough decisions, resulting in terminating employees. Reducing staff further increases the inefficiencies in operations, where fewer employees have to manage an already stressed logistics network. Psychological distress among employees is also reflected in decreased productivity, decision-making, and workplace morale, which results in decreased performance and job satisfaction. Table 21 below provides illustrative quotes on employee impacts on importers and exporters.

Table 21. Illustrative Quotes About Employee Impacts on Importers and Exporters.

Interviewee	Illustrative Quotes
MN1	<i>"It lasted for a week. It was really bad, everyone was very tense, managers, executives, top-level people, they were constantly coming and going, visiting the factories. It was like they wanted to see the stocks instantly."</i>
MN1	<i>"There are departures from work, those who do not feel confident leave and leave, causing a loss of experienced workforce. When you look at it, there are small things that leave such deep effects."</i>

Financially, importers and exporters are the next most impacted parties after 3PL providers. They experience both direct and indirect economic consequences, such as higher security expenditures, reduced business opportunities, increased working costs, reduced revenues, and reduced market share. Additionally, cyberattacks expose them to unique financial threats such as product theft, fluctuations in pricing due to supply chain instability, and a decline in product quality caused by compromised logistics and handling conditions. These financial losses accumulate over time, reducing the long-term sustainability and competitiveness of affected firms. Table 22 below provides illustrative quotes on financial impacts on importers and exporters.

Table 22. Illustrative Quotes About Financial Impacts on Importers and Exporters.

Interviewee	Illustrative Quotes
3PL11	<i>"Cyber attacks can have a wide area of impact, from logistics service providers to customers. In addition to our one-on-one stakeholders, the impact will also be wide, from manufacturing companies to buyers at the destination. The attack can lead to data loss, operational interruptions and major financial losses."</i>

MN1	<i>"It affects us like this, now for us, everything material. The profit we make from material determines the price of the product we sell. That's why the shipment needs to arrive very well and without any problems and without damage. If there is a cybersecurity attack, if we can't access the information, they will steal our products, and we won't know about it."</i>
MN1	<i>"This is what happened to us, for example, the other day, 2 days ago, at around 4:00 in the afternoon, at around 4:30, I mean, it wasn't a cyberattack, but rather an outage in the system. That caused us to stop. It stopped in 3 factories in Turkey. No delivery notes are issued, cars can't leave. There is no transportation, in other words, transportation doesn't work. They covered the transportation costs of all the drivers who suffered losses."</i>
MN1	<i>"So, the factory closes. It literally closes, because, well, they work with a certain amount of stock. If you can't produce after that stock runs out, because everything is the internet for us. When the internet goes out, everything stops, production stops. So, when production stops, that means your name in the sector is already damaged. So, you lose prestige. Then the demand for your drops. When people's demand drops, you have a really bad sales problem. In financial terms, your stocks drop on the stock exchange anyway. You lose a lot of income as a company."</i>
MN2	<i>"In other words, this will shake the trust in them and at the end of the day, no one will want to work with them, which is why it is very, very important."</i>

From an industrial standpoint, importers and exporters experience significant disruptions beyond standard business losses. Unfair competition arises when cyberattacks give competitors an advantage through stolen intellectual property, trade secrets, or manipulated market conditions. Additionally, a surplus of canceled orders becomes a pressing issue, as disruptions force businesses to either delay shipments or fail to fulfill contractual obligations. These cancellations can strain relationships with international clients, leading to long-term loss of trust and business opportunities. Table 23 below provides illustrative quotes on industrial impacts on importers and exporters.

Table 23. Illustrative Quotes About Industrial Impacts on Importers and Exporters.

Interviewee	Illustrative Quotes
MN2	<i>"Having a security breach here means that my prices will spread to the entire sector, or they will see not only the prices but also the specifications of the products I produce when necessary, or I can say that it will reduce the respect for competition."</i>

MN2	<i>"For example, if we consider the automotive industry, there are many raw material orders, and if something happens in the automotive sector, orders may suddenly be cut. Since it's the automotive sector, there are also enforcement clauses, and if you're a supplier in the automotive industry, all those products may end up in your hands. There is such a risk, a major risk. This could also happen due to cybersecurity vulnerabilities, and fake situations could arise in such an environment."</i>
-----	---

Information security is another serious concern for importers and exporters, as they deal with extremely sensitive trade-related information. Cyberattacks regularly lead to serious data breaches, leaking trade secrets, customer data, finance records, product specifications, pricing information, and supplier information. Not only does such data breaches affect competitive advantage, but they also pose compliance difficulties, particularly in dealing with international trade regulations. Exposure of confidential information may culminate in fraudulent practices, illegal market access to competitors, and overall degradation of trust in digital security protocols. Table 24 below provides illustrative quotes on information security impacts on importers and exporters.

Table 24. Illustrative Quotes About Information Security Impacts on Importers and Exporters.

Interviewee	Illustrative Quotes
3PL8	<i>"First of all, this is the case in the sector and in the world because everyone can go to everyone else's customer; in other words, the most important thing is that another company does not know who my customer is or does not know the value of the cargo, the type of product, the value of the goods, or does not know the payment information, the maturity information. Cyber security is one of the most important things that must be done to protect myself and my customers."</i>
3PL7	<i>"It could be customer information, and of course the customer information is like this, that company may not work with you anymore on the next move because you are creating a new competitor for yourself. It could be a problem, where it goes. So of course you need to be careful about that."</i>
3PL4	<i>"Of course, it shows and knows who goes where and which freight is going based on that order. This is directly what the ship or truck owner carries, let's not just look at it as a ship, I mean the airline also comes into it. Then the complexion of the matter changes a little bit. Likewise, there are very critical works in project transportation. There are very serious paid, very assembled loadings. Here too, a small leak can cause very serious costs. That's why it becomes a part of our lives, sometimes including confidentiality agreements, from the materials to be carried to the things that are made. We have always worked with this awareness here."</i>

MN1	<i>"There are tracking devices in the vehicles, location tracking, etc. and we work incredibly fast, in terms of supply. But as I said, if we can't prevent these and they launch a cyberattack, they will first access personal information. This is already a very important thing, so they shouldn't access it. They can access personal information, the company's policy, budget, everything. "</i>
MN2	<i>"Having a security breach here means that my prices will spread to the entire sector, or they will see not only the prices but also the specifications of the products I produce when necessary, or I can say that it will reduce the respect for competition."</i>
MN2	<i>"The information sent to the supplier ends up in the hands of the supplier's customer. Essentially, it falls into the hands of the competitor of the party we are working with. As a result, sales of products planned for that season or period may suddenly drop, and there can be situations where raw materials are planned but remain unsold or unutilized."</i>
MN2	<i>"But if you are producing a very specialized product, there could be a risk of your formula being stolen, which might vary from industry to industry. Where does this typically occur? It usually happens in the core data or financial areas, but it also includes procurement, where information related to purchases can be stolen."</i>
3PL1	<i>"The information about what customers are trading would become something that could be bought and sold with money."</i>

When looking at information-sharing challenges, cyber incidents cause severe communication breakdowns among importers, exporters, and their global trade partners. Integration issues arise, particularly when digital platforms used for tracking shipments, managing supplier relations, or coordinating logistics fail due to cyber disruptions. These challenges are compounded by data loss, which further complicates supply chain coordination. However, despite these vulnerabilities, importers and exporters do not face significant legal consequences directly stemming from cyber incidents. Table 25 below provides illustrative quotes on information sharing impacts on importers and exporters.

Table 25. Illustrative Quotes About Information Sharing Impacts on Importers and Exporters.

Interviewee	Illustrative Quotes
3PL6	<i>"Cyber attacks can create major problems for manufacturers at the very beginning of the supply chain. If manufacturers' connections to logistics providers are cut off, the distribution of products can stop. At the same time, if access to order and demand management systems is lost, manufacturers may not know how much they need to produce. Overproduction or underproduction can occur, which can increase costs. The attack can also disrupt manufacturers' sales and marketing processes."</i>
3PL5	<i>"And there is something like this, on the customer side, a customer wants to know where my cargo is, when it will arrive, when it will arrive. When will my cargo arrive on the way, they say, but since all our systems are down, we couldn't know where the ship is, when it will arrive, when the container will be unloaded at the port the customer wants, none of this was possible, it was complete chaos, complete terror, a bad environment."</i>
3PL11	<i>"Cyber attacks can have a wide area of impact, from logistics service providers to customers. In addition to our one-on-one stakeholders, the impact will also be wide, from manufacturing companies to buyers at the destination. The attack can lead to data loss, operational interruptions and major financial losses."</i>

As regards information-sharing difficulties and challenges, cyberattacks lead to critical communication breakdowns among exporters, importers, and global trade partners. Integration difficulties come about typically where digital tools applied in tracking shipments, managing suppliers, or coordination of logistics are hindered by cyberattacks. This is all made worse by data losses, which actually add to difficulties in coordinating supply. All the same, in spite of all these weaknesses, importers and exporters are not significantly exposed to legal repercussions directly from cyberattacks. Table 26 below provides illustrative quotes on operational impacts on importers and exporters.

Table 26. Illustrative Quotes About in Operational Impacts on Importers and Exporters.

Interviewee	Illustrative Quotes
3PL2	<i>"Although IoT devices and industrial control systems play an important role in monitoring and optimizing the supply chain, these devices are often equipped with weak security measures. Hacked IoT devices can stop production lines, manipulate data, or disrupt operational processes."</i>

3PL2	<i>"There may be some impacts on suppliers. Interruptions in logistics providers' systems can cause serious disruptions in suppliers' inventory management, production planning and response to customer demands. Companies that work with kanban or just-in-time (JIT) methods in particular may face the risk of production lines being shut down if they cannot receive critical materials on time."</i>
3PL6	<i>"Cyber attacks can create major problems for manufacturers at the very beginning of the supply chain. If manufacturers' connections to logistics providers are cut off, the distribution of products can stop. At the same time, if access to order and demand management systems is lost, manufacturers may not know how much they need to produce. Overproduction or underproduction can occur, which can increase costs. The attack can also disrupt manufacturers' sales and marketing processes."</i>
3PL6	<i>"Any cyberattack in the supply chain also affects consumers at the end point. They may experience situations such as products not arriving on time, stock issues or service interruptions. This reduces customer satisfaction and may cause consumers to switch to alternative brands. If consumers' personal information is stolen as a result of a cyberattack, the situation becomes even more serious, and security issues are felt at the individual level."</i>
CC1	<i>"Here is the example I just gave, for example, an important example; there can be serious problems in money transfers. Foreign currency that needs to go to different places can go. This cannot be retrieved later, or a cyberattack on a port operating system or customs operating system can cause dozens of containers and hundreds of trucks to wait in the customs area at the port. This can cause the importer company waiting for raw materials to not be able to reach the goods or the exporter company to not be able to send the goods abroad."</i>
CC1	<i>"There may be a problem in the export of fresh products such as fresh fruits and vegetables that are produced at that moment. These products may spoil, products with a shelf life may not be able to go abroad, and this may cause direct products not to reach their destinations on time due to a cybersecurity breach, and raw materials may not reach the relevant places instantly."</i>
P1	<i>"Similarly, the customs broker will face difficulties because they won't be able to track the process, and the customer will face issues because they can't receive the goods. This is because they need the goods for production or other purposes. At this point, I will face problems as well because my storage areas won't open, and I won't be able to receive new loads. Therefore, these are serious issues."</i>

One of the worst long-term consequences for both importers and exporters is reputational damage. When such companies lose trust in the credibility of both customers and business partners, they experience brand degradation, customer dissatisfaction, and reputation loss overall. Trust decay is one of the grave issues, as repeated disruptions build up to tense relationships among suppliers, intermediaries,

and users. In the worst-case scenario, prolonged cyber-related inefficiencies will even contribute to the total disruption of business relationships, with involved companies in a very vulnerable market position. Table 27 below provides illustrative quotes on reputational impacts on importers and exporters.

Table 27. Illustrative Quotes About in Reputational Impacts on Importers and Exporters.

Interviewee	Illustrative Quote
CC2	<i>That company will not be able to do business, it will cause customer dissatisfaction, this situation will cause customer satisfaction since that company will not be able to do business while we are doing our transactions."</i>

5.3.3. Detailed Impacts on Ports

When we look at ports, ports go through a full spectrum of disruptions, ranging from workforce stability to financial performance, information security, efficiency of operations, legal compliance, and reputation.

From the perspectives of employees, port cyber disruptions usually result in workforce cuts. Lay-offs happen when slowdowns in operations compel port authorities and logistics companies to cut costs by lowering labor costs. Also, uncertainty at the workplace due to cyberattacks translates into stress and job dissatisfaction for workers who remain on the job, decreasing general productivity, as well as workplace climate. Table 28 below provides illustrative quote on employee impacts on ports.

Table 28. Illustrative Quotes About Employee Impacts on Ports.

Interviewee	Illustrative Quote
P1	<i>It is affecting my operations and causing loss of workforce.</i>

Financially, ports experience a combination of direct and indirect costs associated with cyberattacks. These include depreciation costs arising from underutilized infrastructure, disruptions to global trade that affect revenue streams, increased operational expenses due to system failures, penalty costs imposed by shipping clients, regulatory fines for failing to comply with trade guidelines, and additional expenses related to extended vehicle wait times. Cyber disruptions lead to

inefficiencies in cargo handling, causing increased congestion at port terminals, which further elevates operational costs and delays. The cumulative effect of these financial burdens puts significant strain on the profitability and long-term sustainability of port operations. Table 29 below provides illustrative quotes on financial impacts on ports.

Table 29. Illustrative Quotes About Financial Impacts on Ports.

Interviewee	Illustrative Quotes
3PL6	<i>"Of course, port operations are also affected. The failure of digital systems in ports slows down or completely stops operations such as docking of ships, unloading and transporting cargo. This can cause a major blockage in the logistics chain, ship traffic accumulates, and product arrival times are extended. In addition, theft of data related to port operations can lead to a decrease in trade volume and an increase in security vulnerabilities."</i>
P1	<i>"Additionally, while performing these tasks, there are various costs involved such as fuel consumption of the equipment, depreciation of the equipment, and other related expenses. These costs, of course, return to you as expenses, which creates problems."</i>
P1	<i>"There is also something, especially during the unloading and loading stages of ships, where agreements with agents include a clause stating that when my ship arrives, it will work with 2 cranes. The average operation time of these 2 cranes will be set to a certain amount. If the processes take longer than expected—let's say a task that should take 3 hours is completed in 7 hours—they apply a demurrage charge and issue you an invoice. The reason for issuing this invoice is that when the ship departs, it gives you specific time windows, saying 'I will be at this port at this time,' and the port plans its operations based on the ship's arrival. Now, imagine a ship with 5 ports of call. If there's an issue with the system at the second port, the operations are delayed. As a result, the task that should have been completed in 5 hours is done in 15 hours. This causes a delay to the next port of call, and ultimately, the time lost results in the inability to complete the work at another port."</i>
P1	<i>"Now, if we look at it from the simplest perspective, imagine a situation where a transportation company is attacked, and that company is unable to operate. In that case, I won't be able to give them the loads they need to take from my port. Therefore, my operations will be disrupted, and as a result, I will incur financial losses due to the work not being completed at the port."</i>
3PL1	<i>"They faced severe problems at the ports, reaching a point where operational information could not be communicated to the ports. The penalties incurred from the ports, the operations they couldn't carry out, and similar issues led to significant losses."</i>

Industrially speaking, ports have no severe industry-specific threats from cyberattacks. Yet, as they are gateways of trade, their interruptions cause far-reaching

effects across various industries with consequent ripple effects that touch world markets' supply chains.

Information security is a concern for ports because they deal with massive volumes of trade-related information. The leakage of trade secrets, shipment details, and customs records normally occurs due to cyberattacks. Breaches of data by opportunistic hackers pose a threat to international trade because unauthorized individuals get valuable trade information at their convenience. Leaks of trade documents lead to unauthorized shipments, violations of regulatory compliance, and counterfeit trades. Table 30 below provides illustrative quotes on information security impacts on ports.

Table 30. Illustrative Quotes About Information Security Impacts on Ports.

Interviewee	Illustrative Quotes
3PL6	<i>"If there is a scenario where he will demand ransom, it would be the operations department in his mind, here are the loading lists, the docking permits of his ships, the discharge permits, the exit permits because if you lock that with a cyberattack, the company would suddenly not know what is going on. In other words, it is a process that he cannot handle because a ship is something that has to float constantly and should not wait. From time to time, if there are delays at some ports, the next port of call can even be cancelled in order not to incur losses. In other words, even if the biggest company in the world is going to load that ship with its cargo, the ship owner can say, excuse me, I am apologizing for this port."</i>
P1	<i>"Because sometimes there may be some conveniences that we provide to some customers on a company basis. In such cases, if such information were to circulate or fall into the hands of someone else, these would not be welcomed."</i>

In terms of information sharing, ports largely incur communication disruptions instead of complete loss of data. These interruptions hamper port authorities, shipping companies, customs authorities, and logistics companies from coordinating cargo transport smoothly. Delays within the flow of information also increase congestion levels, which creates port operation inefficiencies. Table 31 below provides illustrative quotes on information sharing impacts on ports.

Table 31. Illustrative Quotes About Information Sharing Impacts on Ports.

Interviewee	Illustrative Quotes
P2	<i>"Yes, when we look at our sector, it can cause serious problems on the port side. As I said, I am saying it once, there is actually a chain reaction of unrest here, which can go as far as our inability to dock a ship, our inability to share container information with our stakeholders and their inability to receive their products due to this. Therefore, you become unable to do business. You cannot conduct any commercial activities in any way, very clearly. Yes, we experienced this, but we managed to eliminate it within seconds. This is what set us apart here, such as the fact that the firewalls we use are up-to-date, that we use new generation firewalls."</i>
P1	<i>"For example, the ship has arrived, but I haven't received any data about it. Because of this lack of information, I don't know what to load onto the ship right now; I need that information to be sent to me. Operationally, since the ship has arrived, I've already made a plan for it. The cranes are supposed to work on that ship, but either they can't or they're working at a slower pace. Since the operation is slower, I'm delayed in taking the next ship. All the ship agents are affected by this delay. The customs broker is also affected, and the customer, the goods owner, is impacted as well."</i>

From a legal perspective, ports may face regulatory consequences due to cyber incidents. Non-compliance with taxation and tariff regulations can result in legal sanctions, financial penalties, and stricter oversight from regulatory bodies. Cybersecurity breaches that expose sensitive trade data can also lead to legal disputes involving affected businesses, further complicating regulatory compliance efforts. Table 32 below provides illustrative quote on legal impacts on ports.

Table 32. Illustrative Quote About Legal Impacts on Ports.

Interviewee	Illustrative Quotes
P1	<i>"If that authorization is obtained without proper access, and someone else gets their hands on it, connects to the system, and carries out the necessary attack, you will face a significant loss of time in trying to find and fix the issue. This could potentially lead to serious financial or tax-related problems for you."</i>

From an operational perspective, we see that disruptions primarily hinder the cargo management processes and logistics coordination of ports. Since cyberattacks cause errors in container tracking processes, it becomes difficult to manage shipments efficiently. In addition, coordination difficulties arise when automatic systems at the port are interrupted, which leads to miscommunication or incorrect communication between port employees and other carriers. Faulty deliveries and container loss further

complicate logistics operations, resulting in financial losses for both port operators and shipping clients. Additionally, software integration failures disrupt automated cargo handling systems, causing operational breakdowns that extend congestion issues within port facilities. These inefficiencies contribute to significant trade slowdowns, affecting global supply chain resilience. Table 33 below provides illustrative quotes on operational impacts on ports.

Table 33. Illustrative Quotes About Operational Impacts on Ports.

Interviewee	Illustrative Quotes
3PL10	<i>"Depending on the size of the attack, some companies may have to stop their operations for days or weeks. Especially if a global logistics provider company is subject to a cyberattack, it can disrupt not only local but also international operations. This creates a chain reaction and can even cause global trade to be disrupted. For example, stopping operations at a port or distribution center immobilizes other stakeholders and causes delays throughout the entire supply chain."</i>
3PL6	<i>"Cyberattacks can be like this. There can be cybe attacks targeting different departments, for example, nowadays, in order to get permission for ships to dock or permission for ships to depart, in the past, for example, coast guard, etc., you would fill out a draft on an A4 paper, sign it, stamp it, go there and get permission from there. After those permissions were received, the dock permission would be approved. But now it has become a bit of a system. For example, as a result of a cyberattack on that region, the ships of that shipping line or a company that provides maritime transportation services may not be able to dock at ports."</i>
3PL6	<i>"Of course, port operations are also affected. The failure of digital systems in ports slows down or completely stops operations such as docking of ships, unloading and transporting cargo. This can cause a major blockage in the logistics chain, ship traffic accumulates, and product arrival times are extended. In addition, theft of data related to port operations can lead to a decrease in trade volume and an increase in security vulnerabilities."</i>
P2	<i>"Frankly, potential risks can go as far as the port not being able to provide service. Because any data that disrupts the integrity here means the entire flow chain is broken for us. For example, if we cannot somehow receive a ship's berthing request and experience a problem with this data, we cannot berth the ship at the port. We cannot unload or load containers from a ship that does not berth at the port. Accordingly, you can think of it as not being able to provide service to our customers."</i>
3PL8	<i>"In the example you gave, the answer to the question is actually the delay or delay of all voyages and this goes on like dominoes. A ship or a ship arriving late at two ports or stopping by, or leaving the port late, prevents the next ships from approaching those ports or preventing their evacuation. This is the biggest problem it will create."</i>

- P2 *"Yes, when we look at our sector, it can cause serious problems on the port side. As I said, I am saying it once, there is actually a chain reaction of unrest here, which can go as far as our inability to dock a ship, our inability to share container information with our stakeholders and their inability to receive their products due to this. Therefore, you become unable to do business. You cannot conduct any commercial activities in any way, very clearly. Yes, we experienced this, but we managed to eliminate it within seconds. This is what set us apart here, such as the fact that the firewalls we use are up-to-date, that we use new generation firewalls."*
- P2 *"You know the stacks in ports. Think of it like there is a stack of 6 rows, 6 rows of stacks, you put containers on the stack for the last 3 days, but you don't have the last 3 days. You don't know where which container is. They are always arranged and placed according to the plan. They are positioned according to this program. Therefore, if you don't have those 3 days, none of the containers you took during that period are gone. So, you can imagine how deadly this would be for a port."*
- P1 *"Before the containers arrive at the port, if we know the weight, origin, and the ship they will be loaded onto, we can organize the stacking accordingly. For example, let's say we have an area with 5 rows horizontally and 6 rows vertically, making up about 30 rows in total. If you place a container right in the middle of this area, and the ship is arriving tomorrow, to access that container, you will have to remove the containers on top of it, set them aside, and then put them back again, repeating this process. Once you get to the container, you will have to rearrange the others as well, but now their positions will have changed. As a result, you'll have to open 3 or 4 different work orders to complete the task, which causes a significant waste of time."*
- P1 *"Now, there is something we call the center of gravity in these. Especially when used on ships, think about it like this, a container can have 5 tons of load or 20 tons of load on one side of the ship. Now, when you put 20 tons of load on one side, you cannot prevent the ship from tipping over, it will sink, in other words, as a result. Therefore, you should put containers in both areas of the ship, front and back, and you should do something accordingly. The ship should be properly stabilized and move accordingly. Now, since we cannot get this data from the company, this is a big problem."*
- P1 *"There is also something, especially during the unloading and loading stages of ships, where agreements with agents include a clause stating that when my ship arrives, it will work with 2 cranes. The average operation time of these 2 cranes will be set to a certain amount. If the processes take longer than expected—let's say a task that should take 3 hours is completed in 7 hours—they apply a demurrage charge and issue you an invoice. The reason for issuing this invoice is that when the ship departs, it gives you specific time windows, saying 'I will be at this port at this time,' and the port plans its operations based on the ship's arrival. Now, imagine a ship with 5 ports of call. If there's an issue with the system at the second port, the operations are delayed. As a result, the task that should have been completed in 5 hours is done in 15 hours. This causes a delay to the next port of call, and ultimately, the time lost results in the inability to complete the work at another port."*

P1 *"In other words, the slow work there can come to a point where the port is completely stopped."*

Reputation-wise, ports have long-term costs associated with cyber-related inefficiencies. Reliability loss that is caused by cargo handling and trade facilitation deteriorates the reputation of affected ports, breaking the relationship that the ports have with their shipment clients, importers, exporters, and logistics service providers. In the extreme cases, long-term business is lost because of recurring cyber-related failures as partners seek alternative paths for trade and logistics solutions. Table 34 below provides illustrative quotes on reputational impacts on ports.

Table 34. Illustrative Quotes About Reputational Impacts on Ports.

Interviewee	Illustrative Quotes
P1	<i>"At first, people usually think about the financial aspects, but when you look at it, imagine if something like this happens today. Do you think the customs broker, or the customer would want to work with you again? No. So, because I couldn't protect the data I provided to them, that third-party company took it and it was stolen from me. That's a bigger issue, because once it's gone from me, I will be responsible at that point. It reflects poorly on working with good companies, etc. So, it's an element that will affect every part of the business."</i>
P1	<i>"In the case of a cyberattack, let's say I receive an email from a person. This email could be manipulated, or maybe an employee from the company acted maliciously or made a mistake in writing the container number, for example. In such cases, I receive the email, and I keep working on it, investigating it, but I can't find it in the system. I check everywhere. Before me, customer service checks, marketing checks. They ask, 'Did we receive such data from you?' Operations checks, 'Did I make a plan for this?' Therefore, people who should be focusing on their work are spending extra time solving this issue. This wasted time, of course, disrupts our relationship with the customer and the customs broker."</i>

5.3.4. Detailed Impacts on Customs

W In evaluating the impacts of cyberattacks on customs operations, there are no serious effects seen with regard to legal issues, employee side issues, industrial issues and interruptions and lastly reputation loss. Unlike other actors, customs do not face direct employee consequences like job loss, additional workload, and personnel inefficiencies. Just as there is no major legal repercussions that are specific to customs

operations, there are no large-scale industrial consequences or reputation loss that is linked to cyberattacks on customs operations.

Financially, customs only encounter the risk of trade disruptions on a global scale and not direct financial loss. Cyberattacks on 3PL providers and other partners along the supply chain may result in general slowdowns on a trade scale, impacting customs clearing processes and general trade flow overall. Direct financial losses do not occur for customs authorities but could indirectly help cause overall economic inefficiencies from slowed imports and exports. Table 35 below provides illustrative quotes on financial impacts on customs.

Table 35. Illustrative Quotes About Financial Impacts on Customs.

Interviewee	Illustrative Quotes
3PL6	<i>"When a cyberattack affects customs processes, the movement of goods across borders can be significantly slowed down or stopped. On the customs side, it can prevent the verification of documents and cause long delays in import-export processes. These delays increase costs for importers and exporters, while creating disruptions in the international trade chain. In addition, theft or alteration of customs data can undermine the reliability of trade."</i>
CC1	<i>"In our sector, especially exporters, importers and public institutions are directly affected. Customs consultants are directly affected. This has a significant negative impact on our foreign trade."</i>

Its strongest impact is on customs operations within the context of information security. Most cyberattacks fall on opportunistic violations of data, unauthorized leakage of individual details, and exposure of classified confidential trade documents. These violations pose severe threats to international trade because affected documents may cause regulation issues, fraud cases, and unauthorized use of trade-related intelligence. Table 36 below provides illustrative quotes on information security impacts on customs.

Table 36. Illustrative Quotes About Information Security Impacts on Customs.

Interviewee	Illustrative Quotes
3PL3	<i>"So, everyone is affected, in the example I gave, for example, this simplicity company, the customs software company Evrim, yes, and then the exporter, customs consultant, transporter, everyone who does business with it, it is clear that at least their user information has been stolen."</i>
3PL3	<i>"Of course, it can go as far as customer information. Let me say this, customs information for some countries in the world is sold. Customs declarations</i>

are sold in some countries. In other words, you go and pay money, you can get your hands on invoice samples or declarations for all the goods entering and leaving that country."

3PL1 *"I'm saying this with a very simple example, or for instance, all of our financial data passes through there. As you can imagine, in our country, the finance part is a very sensitive area for companies, especially for importers and exporters, where they often say that customs are like our bedroom. Customs is really the secret part of people's businesses, where they disclose all the details of their trade to the government. If you expose that, you are essentially laying bare your entire business. You make everything transparent. That's why they refer to it as our "bedroom."*

When we look at the operational side, it can be seen that customs authorities are facing great difficulties due to cyberattacks. Since it slows down or even stops procedures such as cargo tracking processes, declaration processing processes, permit approval processes, there are delays in export and import processes. The resulting delays cause operational congestion at border inspection points, ports and areas where logistics processes are managed. Moreover, the resulting interruptions negatively affect the information sharing processes between customs companies, logistics providers and other supply chain stakeholders, preventing coordination in workflow and causing slowdowns in trade. Table 37 below provides illustrative quotes on operational impacts on customs.

Table 37. Illustrative Quotes About Operational Impacts on Customs.

Interviewee	Illustrative Quotes
3PL6	<i>"When a cyberattack affects customs processes, the movement of goods across borders can be significantly slowed down or stopped. On the customs side, it can prevent the verification of documents and cause long delays in import-export processes. These delays increase costs for importers and exporters, while creating disruptions in the international trade chain. In addition, theft or alteration of customs data can undermine the reliability of trade."</i>
P1	<i>"Similarly, the customs broker will face difficulties because they won't be able to track the process, and the customer will face issues because they can't receive the goods. This is because they need the goods for production or other purposes. At this point, I will face problems as well because my storage areas won't open, and I won't be able to receive new loads. Therefore, these are serious issues."</i>

5.3.5. Detailed Impacts on Shipowners

When examining the impact of cyberattacks on shipowners, it is evident that the primary consequences fall under three key categories: financial losses, operational interruptions, and reputational damage. Unlike other stakeholders, shipowners do not experience employee-related consequences, legal implications, or information security breaches to the same extent.

Financial costs fall on shipowners for the disruptions that occur from cyber incidents, with any delay or inefficiency within logistics operations immediately being translated into higher costs of operations. Shipowners experience revenue loss from delayed voyages, higher fuel usage, and even penalties for failing to make up missed delivery deadlines. Shipowners may be compelled to reroute ships or prolong anchorage times from disruptions at the ports and customs clearance, adding to the costs further.

Operationally, shipowners experience extreme disruptions to fleet management, cargo operations, and voyage scheduling. Logistic network application attacks are capable of interfering with ship tracking systems, resulting in navigation inefficiencies and slow-downed shipping routes. Attacks on port resources or on 3PL service operators also cause congestion at the ports, delaying the unloading or loading of cargo. These issues of shipment-based operations have a ripple effect on global-wide supply chains, impacting delivery schedules and overall efficiency of trade.

Reputation loss is another severe result endured by shipowners after a cyberattack. Because the level of trust required in maritime logistics is so substantial, any interference brought on by cybersecurity vulnerabilities has the capability to seriously undermine a shipping company's reputation. Clients and trading partners lose confidence in the integrity of breached shipowners, which culminates into compromised alliances, diminished business opportunities, and long-term business setbacks. Table 38 below provides illustrative quotes on reputational impacts on shipowners.

Table 38. Illustrative Quotes About Reputational Impacts on Shipowners.

Interviewee	Illustrative Quotes
3PL1	<i>"The operation is completely negatively affected. For example, the port example I mentioned earlier: the ship arrives, but you can't submit the manifesto. This leads to a serious delay in the port operation, which means a loss of hundreds of thousands of dollars, both for the port and for the shipowner."</i>
P1	<i>"For example, the ship has arrived, but I haven't received any data about it. Because of this lack of information, I don't know what to load onto the ship right now; I need that information to be sent to me. Operationally, since the ship has arrived, I've already made a plan for it. The cranes are supposed to work on that ship, but either they can't or they're working at a slower pace. Since the operation is slower, I'm delayed in taking the next ship. All the ship agents are affected by this delay. The customs broker is also affected, and the customer, the goods owner, is impacted as well."</i>

5.3.6. Detailed Impacts on Retailers

Retailers find themselves facing a varied spectrum of impacts due to cyberattacks with substantial financial, functional, and reputational effects, yet no appreciable effects with regard to employee issues, security breaches of information, legal issues, or industrial consequences are seen. Compared with other actors, retailers are less directly vulnerable to the threat of cyberattacks but severely indirectly affected by the interruption of the supply chain.

Financially, retailers may experience significant sales losses as cyberattacks disrupt logistics and supply chain infrastructure. Retailers may be unable to meet customer demand due to stockouts and delayed shipments due to stock availability. Furthermore, long-term interruptions in the chain may lead to spoilage of shelf-stable products or the use of new alternative sources, which may reduce product standards, which may result in a decrease in product quality. These problems will reduce the competitiveness of retailers and make it difficult to maintain their customer and market shares.

Operationally, retailers encounter significant challenges in maintaining smooth inventory management and distribution processes. Planning errors become more frequent as disrupted supply chains make demand forecasting more difficult. Delivery delays further exacerbate operational inefficiencies, causing customer dissatisfaction

and logistical bottlenecks. Inventory inaccuracies also arise due to inconsistent supply flows, leading to stock mismatches and increased operational costs.

Reputationally, retailers are among the most affected stakeholders after 3PL service providers and importer/exporters. The primary reputational consequences stem from customer dissatisfaction, which results in negative reviews, complaints, and loss of consumer trust. As delays and stock shortages persist, retailers may experience a decline in customer retention, ultimately leading to a loss of market reputation. The inability to provide reliable service can push customers toward competitors, further diminishing long-term business viability. Table 39 below provides illustrative quotes on reputational impacts on retailers.

Table 39. Illustrative Quotes About Reputational Impacts on Retailers.

Interviewee	Illustrative Quotes
3PL6	<i>"Retailers are also severely affected by an attack in the logistics chain. When data flow with logistics providers is disrupted, retailers cannot get products to fill the shelves in a timely manner, leading to stock shortages. Large retail chains in particular experience customer churn and significant sales losses when they cannot supply products throughout their store networks. In addition, SCDs reduce retailers' competitiveness and damage long-term customer relationships."</i>
3PL10	<i>"An attack not only affects logistics companies but also other links in the chain. For example, retailers may not receive the product on time, which causes problems in their stock management. When products that should not reach customers are delayed, customer satisfaction decreases and there is a loss of trust on the customer side. This process also causes costs to increase. Late delivery of products triggers the replanning of logistics operations, additional costs and a general inefficiency in the supply chain."</i>

5.4 Mitigating the Ripple Effects of Cybersecurity Issues Along a Supply Chain

This section examines in detail effective mitigation strategies that aim to prevent or minimize the ripple effects of cyberattacks throughout the entire supply chain. These strategies were derived from a detailed content analysis of the responses collected from semi-structured interviews with industry experts.

5.4.1. Employee Related Mitigation Strategies to Reduce Employee Impacts

In the Impacts section, we saw that employee impacts are significant impacts that companies experience during and after cyberattacks. In this section, nine key mitigation strategies were created based on responses from industry professionals to minimize the challenges created by these impacts.

The first of our employee-related strategies is audit for employee training. The strategy is one of the cornerstones for reducing security vulnerabilities originating from employees and is the systematic audit of cybersecurity training programs. The strategy covers both internal and external audits. In this way, audits ensure that cybersecurity training is not a one-time event but a sustainable corporate practice. Thanks to audits, the current status of employees regarding cybersecurity is revealed and companies can take action accordingly and equip their employees with up-to-date cybersecurity knowledge. In this way, employees can maintain their productivity in the event of any cybersecurity vulnerability.

Another important strategy is awareness programs. These programs are vital in creating an effective company culture by applying them to employees. Awareness programs make employees sensitive and prepared for threats of attacks targeting the company such as phishing, phishing, social engineering, and e-mail attacks, and encourage them to adopt cybersecurity practices in their daily routines. The effects experienced by employees who gain awareness and knowledge with the strategy can be minimized during and after an attack.

Instilling a skeptical mindset in employees and building a company culture around this is another important mitigation strategy. Instead of accepting their emails, messages, digital transactions and other workflows as they are, employees are encouraged to adopt a skeptical and critical perspective towards them and evaluate them accordingly. With a healthy culture of skepticism, the company significantly reduces the success rate of potential attacks and the likelihood of impacts to employees is reduced at the same rate.

Another strategy we uncovered with the answers of industry experts is creating a system for generating security tickets for employees. Creating an effective reporting mechanism like this strategy is very important for early threat detection and management of cyber incidents. By creating such ticket systems for employees, organizations allow relevant teams to respond and intervene quickly to incidents, preventing attacks from turning into larger crises and reducing potential damage. In addition, in such a case, the threat is directed only to the relevant units, minimizing overtime and stress levels for employees.

Our fifth strategy is employee training. Beyond general awareness, specialized cybersecurity training and organizations should be implemented to further deepen employees' technical equipment and their role in cyber defense. It includes appropriate actions such as password management, data encryption, recognizing suspicious activity situations, and resistance training against phishing attacks. In addition, training should not only be in-house but also be provided by an external cybersecurity expert institution if necessary. In this way, the first line of defense for the company, namely the human element, is strengthened.

Another strategy is hiring competent IT staff. The competencies of IT staff directly affect the company's ability to defend and respond to cyberattacks. Interview findings particularly emphasized the need to hire skilled and educated IT professionals who can effectively manage the cybersecurity incident. This strategy not only strengthens the company's defense shield against cyberattacks but also minimizes the impact on company personnel in the event of a cyberattack. Establishing a competent IT staff provides effective services to employees during crises, reducing staff stress levels and anxiety, and preventing misinformation, thus maintaining workforce morale and productivity.

Our next finding is the strategy of implementing incentive programs for employees. In the employee impacts section, we talked about quitting jobs and talented employees leaving the job. In such cyber incidents, it is very important to maintain employee morale. Implementing incentive programs that offer privileges to employees and reward them strengthens employees mentally, reduces burnout, and greatly reduces the thoughts of employees who are thinking of quitting their jobs due to stress and excessive workload. In this way, the company will retain its talented experts.

Our eighth strategy, which we revealed with the answers of experts, is restrictions to personal applications. Not only does enforcing limits on personal application use inside business environments help to improve cybersecurity, but it also helps to minimize employee-related effects both during and after cyber events. Results of semi-structured interviews showed that unrestricted access to outside applications can greatly raise system vulnerabilities, so exposing the whole workforce to possible disruptions and data breaches. Organizations can significantly lower the possibility of cyberattacks by restricting access to high-risk applications including web-based

messaging platforms and enforcing rigorous browser monitoring policies. Though at first, they may cause employee inconvenience and frustration, these steps eventually help to reduce the psychological load related with cyber threats, enable more operational stability, and stop the escalation of stress and workload during recovery stages.

We are finishing the employee-related strategies section with employee-based security drills, one of our last and most important strategies. This strategy prepares employees for possible cyber threats. It helps employees to put their theoretical knowledge into practice under attack and pressure. The strategy generally reveals possible weaknesses within the company and allows companies to create effective response plans for attacks. In addition, it is critical to minimize the effects on employees. Employees who are prepared for what to do in the event of an attack will have a minimum stress level and will also prevent a decrease in productivity. As mentioned above, the opportunity for companies to create a preparedness plan will also reduce the workload of employees in the event of such cyberattack scenarios. Table 40 below provides employee related mitigation strategies and illustrative quotes to prevent ripple effects on employees.

Table 40. Employee Related Mitigation Strategies and Illustrative Quotes Aimed at Preventing Ripple Effects on Employees.

Ripple Effects	Mitigation Strategy	Quote
reduced employee productivity	Audit of employee training.	<i>"When assessing the cybersecurity level of stakeholders, we pay attention to factors such as the currency of security policies, employee training, the state of technological infrastructure, their response to past cyber incidents, and third-party security. These criteria also help us understand how prepared stakeholders are." (3PL12)</i>

Table 40. Employee Related Mitigation Strategies and Illustrative Quotes Aimed at Preventing Ripple Effects on Employees (Continued).

employee demotivation, employee stress, reduced employee productivity	Awareness programs	<i>"More people are being trained and growing on this subject, and for this reason, as I said earlier, we need the appropriate budget and resources. Employees need to be aware, not fall behind technology, and constantly have examples and information on the subject. As I said, as a company, we are regularly assigned trainings on cybersecurity, other issues, namely information sharing, and our operations, and in our common system, we have to do that training within a certain deadline so that all employees are aware. The company also has such practices." (3PL11)</i>
All employee impacts	Being Skeptical	<i>"For this reason, we attach importance to it, but as I always say, we are as strong as the strongest link in the chain. Unfortunately, one hand can always be stronger than the other. We approach every event with suspicion as if we could be attacked at any moment, and we continue our work to be skeptical of everyone, even on the information processing side of our business, and even if it does not happen, we continue our work to consider the possibility of it." (CC2)</i>

Table 40. Employee Related Mitigation Strategies and Illustrative Quotes Aimed at Preventing Ripple Effects on Employees (Continued).

employee stress, employee demotivation, employee overtime, Loss of talented employees	Creating a system for generating security tickets for employees	<i>"Here's how we handle it: if there's a system disruption or attack, we have a 24/7 team available. We just need to inform them. For example, at our Izmir factory, we have a feature within Efes, our online system, called "ticket creation." Efes has a very advanced system with a well-developed network, and almost every topic and issue are covered there. You simply click on the relevant issue, specify the urgency (such as very important, important, or not urgent), and send it to the authorized person. The responsible person then contacts you immediately. There's a team working 24/7, and they inform their superiors if needed. If necessary, they shut down or suspend the system." (MN1)</i>
All employee impacts	Employee trainings	<i>"As I just said, our top priority is user education. Because nearly ninety percent of cyberattacks come from the internal network. In other words, when a user's computer is infected with a Trojan, it starts working on the internal network. Therefore, we first educate our users on which emails to read, to delete emails they do not recognize, and to be very careful when browsing websites. Our top priority is user education because everything starts there." (P2)</i>

Table 40. Employee Related Mitigation Strategies and Illustrative Quotes Aimed at Preventing Ripple Effects on Employees (Continued).

employee demotivation, employee stress, reduced employee productivity, Job losses	Hiring competent IT	<i>"So, users need to take control. So, this is not about how strong your IT infrastructure is but how strong your human resources are. Human resources need to step in when selecting personnel. Unfortunately, in this sector, there are usually a lot of relationships between friends and acquaintances. Therefore, personnel may not be selected by elimination."</i> <i>"So, every sector, every company, needs to dip a data processor once, but it is necessary to work with competent data processors."</i> <i>(CC2)</i>
Job losses, employee demotivation, employee stress, loss of talented employees	Implementing incentive programs for employees	<i>"People lost their health due to stress. However, one of the great things about Maersk was that they didn't disregard the efforts of their employees. For example, they provided drinks and meals in the offices, sparing no expense to ensure morale and motivation remained high, especially considering the extraordinary effort people were putting in. Even under normal circumstances, they are a company that prioritizes employee well-being, and I believe they managed this crisis exceptionally well. I have many friends there, and I still talk to them. The stress and challenges of that period were so intense that some even needed psychological support due to the demanding workload."</i> <i>(3PL1)</i>

Table 40. Employee Related Mitigation Strategies and Illustrative Quotes Aimed at Preventing Ripple Effects on Employees (Continued).

employee overtime, employee stress	Restrictions to personal applications	<i>As I mentioned, our company has very high-level security, which can sometimes be frustrating. For instance, when you open Google Chrome, you have to wait 1-2 minutes. The internet works very slowly because they monitor everything in the background, including your login and log-out activities. They even recently blocked WhatsApp Web due to a potential security vulnerability, in order to prevent it from affecting the factory or causing a breach. Every incoming email is monitored in the system before it can be opened. Everything takes a long time because of this, and it can be a bit frustrating. In this fast-paced technological age, we work slowly, but it's all for security, of course. Everything is monitored, and there is a very strict management system in place. In fact, the system is set up with backups of backups. (MN1)</i>
All employee impacts	Employee based security drills	<i>"Secondly, these precautions you take will not remain on paper. You will definitely implement them. In other words, when something like this happens, you will conduct a drill. For example, I did it with the security team and said, friends, we have a drill, yes, this incident happened, what are we doing now? We all looked at each other. I think recreating this incident, in other words, a drill is a very important thing. This also needs to be done." (3PL9)</i>

5.4.2. Industrial Mitigation Strategies

This subsection presented 11 distinct industry-level risk coping strategies to mitigate industrial impacts of cyberattacks against 3PL service providers and their vast supply chains. Industrial impact like unfair competition and market instability can cause serious antitrust trouble in an entire industry after a cyber event. Recommended responses to these widespread impacts and for fostering solidarity and collective resilience, based on expert interviews and rigorous content analysis, include the following strategies.

The first recommended strategy is collaborative (Single Expert IT) IT team for the entire supply chain. Creating a single, specialized IT staff to manage cybersecurity throughout the entire supply chain eliminates variations in security applications across all parties. A centralized technical authority can avoid making the weakest among the distributed some sort of backdoor or risk, and hence avoid cyberattacks leading to industrial-scale unfair competition and systemic failures.

Our second recommended strategy is collaboration among stakeholders. Encouraging continuous cooperation among supply chain stakeholders is conducive to facilitating timely information sharing when cyber threats arise. The sharing of information in this area allows for more rapid reaction times, acts to develop collective defenses and avoids isolated cyber challenges to spread into wide-ranging industrial crises, in which otherwise businesses can lose competitive positions.

The third strategy we propose is the industry adoption of a common security standard. Standardizing shipping industry cybersecurity protocols provides for a more across-the-board method of defense. This approach alleviates the industrial impact by avoiding any weaker players to turn into filling-the-gap targets, and subsequently keeping the playground fair, and market breakdowns post-attack under control.

Another strategy we came up with based on responses from industry experts is creating incident response teams for the entire chain. Cross-organizational incident response teams can allow for a quicker containment and recovery across multiple, interconnected firms. If companies have already pre-coordinated a team, then large industrial damages, such as service interruptions, canceled orders, and supplier bankruptcies, cannot be as easily affected across the network of companies.

Another strategy we came up with based on responses from industry experts is creating events for the entire chain. Regular and joint organization of cybersecurity awareness events, workshops, seminars and symposiums, and training practices that all stakeholders and the supply chain will participate in will encourage all chain members to find common ground and contribute to the development of a defense culture. This interaction will encourage all stakeholders, regardless of whether they are big or small, to care about emerging threats and take steps against them, thus minimizing widespread industrial disruptions.

The sixth strategy we came up with based on the responses of industry experts is cybersecurity status sharing among stakeholders. Creating secure systems for sharing real-time cyber threat statuses with shared partners enhances risk visibility across the supply chain. Early detection and early response to breaches reduce the risk of isolated breaches turning into systemic failures that would protect the competitive landscape while preserving the continuity of operations across sectors.

The seventh strategy we came up with based on the responses of industry experts is joint security agreements. Ultimately, a formal agreement around shared security protects the entire group by formalizing the terms as a minimum. Everyone can institutionally hold each other accountable if they are noticed to be not applying any minimum commitment to best practices regarding broader cybersecurity practices. Creating these agreements creates collective responsibility, which minimizes the risk of losses due to competitive advantage, and market conditions after a successful cyber breach.

Another strategy we came up with based on responses from industry experts is collaborative security drills. Performing collaborative cybersecurity drills across various stakeholders simulates real attack events and enhances the coordinated response capability. Because supply chain partners are able to respond in concert, it mitigates the industrial impact, curtailing the interruptions and collapse of operational flows.

Another strategy we came up with based on responses from industry experts is undergoing a unified audit for the entire chain. A common cybersecurity audit which is applied throughout the supply chain provides a broad and system-wide risk profile with systemic limitations mapped. Issues can be remediated as a group, ensuring that

the entire chain is made robust and preventing outcomes, in the worst case, on an industrial scale - such as the collapse of market and cancelled order surplus.

Another strategy we came up with based on responses from industry experts is use of Cloud. When a cloud service is appropriately secured, the infrastructure it provides is scalable, flexible, and resilient, which will substantially bolster a supply chain's operational resilience against cyber threats or attacks. Real time backup of data, security for remote access via any network, and redundancy across multiple and different servers naturally reduces the risks for the total loss of data and/or extended business downtimes that would put the employment and viability of the whole industry sector at risk. As revealed through the interviews, the expectations are that businesses across the supply chain, particularly smaller businesses, should anticipate moving to the cloud-based system in the very near future. There is also a strong view that investment in cloud solutions will be as standard practice, not optional if there is an ambition of remaining market competitive and operating businesses continuity rationale. In terms of the use of industrial impacts as a rationale, engaging cloud helps reduce the odds of widespread supply chain failures. Businesses that are using cloud can provide reliable continuity of service, do their utmost to prevent sensitive data loss after a breach, and maintain continuity operations after a cyber incident. Without such engagement across the supply chain, businesses risk failures that lead to industry instability, particularly an over influx of unfair competition and/or broad stakeholder trust erosion. Therefore, cloud is fundamental as a deterrent, not only preserve individual businesses but the structure of the industry.

The final strategy we came up with based on responses from industry experts is utilizing unified software across the entire supply chain. Standardized software systems across the supply chain create consistent security settings, easier patch management, and fewer compatibility issues. This kind of alignment will help mitigate industrial consequences by minimizing systemic vulnerabilities, while ensuring that cross-organizational digital operations can continue during cyberattacks. Table 41 below provides mitigation strategies and illustrative quotes to mitigate industrial ripple effects.

Table 41. Mitigation Strategies and Illustrative Quotes to Mitigate Industrial Ripple Effects.

Ripple Effects	Mitigation Strategy	Quote
Unfair Competition	Collaborative (Single Expert IT) IT team for the entire supply chain	<i>"Supply chains need to operate over a large network against cybersecurity, and all companies need to operate over that network, meaning there is only one common connection, so it will be difficult to overcome it. There needs to be a single common connection, and I say a single IT department should look after the entire chain." (3PL10)</i>
All Industrial Impacts	Common Security Standard Implementation for the Industry	<i>"As I said, first of all, I think this needs to become an ecosystem. Everyone, the supplier, the customer and the state, will want this. Because when you want and do it alone, it doesn't do much. This needs to be end-to-end. Every part of the ecosystem needs to have the same standard and the same perspective. When your competitor doesn't do it, it doesn't make sense. When you do it and your customer doesn't, it doesn't make sense or when the supplier doesn't do it, you do it, it doesn't make sense. If there is an ecosystem, I think there should be an authority within it. The state is also taking steps in this sense, they are aware of it too. Now, something like this needs to be brought to all sectors, there are certain laws. They brought a law called 56-51. Like the obligation to keep records for crimes committed on the internet. I think they need to make this a bit more mandatory with similar laws." (3PL9)</i>

Table 41. Mitigation Strategies and Illustrative Quotes to Mitigate Industrial Ripple Effects (Continued).

Unfair Competition	Collaboration	<i>"Establishing information sharing protocols and security collaboration among organizations in the supply chain is critical because without strong collaboration, it is impossible to overcome cybersecurity threats." (3PL2)</i>
All Industrial Impacts	Create Incident Response Teams for the Entire Chain, Cybersecurity status sharing among stakeholders	<i>"There is no such thing in the logistics sector, but there is such a thing in the cybersecurity sector. There are some events held there, sometimes I participate as a speaker, or at those events you meet, talk to, your producers, customers, people in the same sector, related to these, on the state side, a bit like this, there is a cybersecurity cluster or SOMEs (Cyber Incident Response Team), for example, there are sector-based SOMEs. We are also subject to this as cyber incident response teams. If you find a cyber incident or a case, you report it. You know, there is USAM, maybe there are SOMEs under the roof of USAM. They are trying to share information like this, but I don't think it is very sufficient. It can usually come from far behind or it depends on the city. Nobody wants to say that I have such a vulnerability easily, and they also hesitate to report it. That's why there is such information sharing on the initiative of many people. First of all, as I said, the right way should be provided in some way by the state authority." (3PL9)</i>

Table 41. Mitigation Strategies and Illustrative Quotes to Mitigate Industrial Ripple Effects (Continued).

All Industrial Impacts	Cybersecurity events for the entire chain.	<i>"Actually, this can be achieved by triggering each other. In other words, if the supplier, manufacturer, 3PL companies, customs brokers, and others continue to push and develop each other, the stakeholders will also develop to that extent. Therefore, it is important not to lose this trigger and to continue development across all stakeholders. After that, I believe training in this area should be increased. If necessary, cybersecurity meetings could even be held with stakeholders. The importance of certain things becomes clearer the more they are emphasized. The more it is emphasized; I think it will show how necessary it is. It's like saying, "I need this computer to do my job, I want it, I want it, I want it." If you don't give it to me, I can't do my job. I think it will be something like that." (MN2)</i>
All Industrial Impacts	Collaborative Security Drills	<i>"Common security standards, security training and attack simulations are important parts of this cooperation. In particular, emergency response teams and joint security exercises created against major attack risks will encourage cooperation and solution searches across the sector." (3PL2)</i>

Table 41. Mitigation Strategies and Illustrative Quotes to Mitigate Industrial Ripple Effects (Continued).

All Industrial Impacts	Joint security agreements	<i>"Maersk signs contracts in these areas, and we also sign information and security contracts with our suppliers. Are there any specific cybersecurity measures? Honestly, I'm not sure. This is a bit outside my area, but what I can say is that in our sector, this is not given much attention. Very large, corporate companies try to pay attention to this more for the sake of formality, but there is no real standard. As I mentioned earlier, there is a profile review process—if a supplier isn't just two desks and one chair, then it's considered whether or not to work with them. But when a problem suddenly arises, there's nothing that can be done. It's essentially a risk-taking situation. But as I said, in Turkey, cybersecurity is not considered important until something actually happens. It's not given much importance unless it's experienced here." (3PL1)</i>
All Industrial Impacts	Undergoing a unified audit for the entire chain.	<i>"Of course, the implementing body here needs to be the public. Therefore, the chambers of commerce, the industry dollars or, apart from that, the ministry of commerce needs to bring all stakeholders together under one roof and provide legality. Is there currently such a system in the works? There is not, but I think there should be." (CCI)</i>

Table 41. Mitigation Strategies and Illustrative Quotes to Mitigate Industrial Ripple Effects (Continued).

Unfair Competition	Use of Cloud	<i>"Therefore, companies within the supply chain need to focus on software and invest in quality software and networks. There's no way around this anymore. In the next 10 years, even small companies will likely handle these tasks in the cloud. Perhaps they will enable everyone to adapt by running localized versions of software." (P1)</i>
All Industrial Impacts	Utilizing a unified software across the entire supply chain	<i>"Now, for example, how does the logistics distribution or selection in our country work, it is either through customer or freight selection. But for example, a logistics transportation in America, you have a load and you will take it from one place to another; all the transporters of the country are in a program, all of them determine the freights within themselves as a cooperative and you only choose something, as comments and stars, this transporter is very good, this transporter is very bad, you make choices according to the 3-star, 5-star rate and range, so if a transporter has 100 cars there, they cannot give and get the best price. Like a cooperative, the top car goes. The system there is different anyway. It would be better for our country to do this, but I think it is a very difficult choice." (3PL8)</i>

5.4.3. Information Security Strategies

In this section, 17 strategies that emerged as a result of our analysis for information sharing impacts, which we examined in detail in the impacts section, will be examined in detail.

Our first strategy is backup in cloud and different locations, which industry experts emphasize. Experts have stated that companies that create data backups will protect against information and data-based security problems such as data manipulation and disclosure of commercial documents. In addition, experts have clearly stated that switching to cloud backups in the event of an attack while the main servers are under threat will prevent permanent loss of all sensitive data such as customers, suppliers, etc.

Our second strategy, which emerged from the responses of industry experts, is budget allocation for security. They emphasized the importance of allocating a separate budget for security tools, personnel, technology and cybersecurity. They stated that this budget allocation will allow companies to implement high-standard protocols in the supply chain that can resist cybersecurity threats, data breaches and other types of attacks. Allocating a sufficient security budget will allow the company to implement security tools such as encryption tools, IDS, etc. that protect sensitive records such as financial data, company strategies and customer information from being stolen or leaked.

Our next strategy is again certification and standardization, which is the common view of the majority of participants. Experts emphasized that obtaining nationally and internationally accepted certificates such as KVKK, ISO270001, Authorised Economic Operator (AEO), CTPAT will provide standardized applications throughout the chain and provide solid frameworks to ensure information security. In addition, it was suggested that the requirements of frameworks such as National Institute of Standards and Technology (NIST) and SysAdmin, Audit, Network, and Security (SANS) be fulfilled on a chain basis in addition to these certifications. In this way, effective controls will be made in the processing processes of trade secrets, customs data, personal information and leakage and manipulation cases will be reduced. In addition, since these standards require various audits, controls and official protocols, they will increase security and compliance on a stakeholder basis.

According to experts, another strategy that should be implemented is creating emergency response teams. It has been stated that the strategy is a structure that should be created in every company in order to find the source of the attack at the time of the attack, to keep the damage to a minimum and to recover the systems as quickly as possible by taking action against the cyber incident. Since these teams to be created will be composed of personnel equipped to isolate the systems, monitor the attack vectors and recover the manipulated data, they are very critical to minimize the risk of data breach in a possible situation. In addition, these teams can prevent the spread of the threat to the chain with effective interventions and ensure the integrity of the stakeholder data. Under cyberattacks where even seconds matter, these teams to be created will serve to greatly reduce the security vulnerability threats for the entire chain.

One strategy that was specifically suggested by the IT personnel with more than ten years of experience in the sector among the participants was creating an effective network infrastructure. These participants stated that in order to ensure that the security measures of effective devices can be used, the appropriate infrastructure should be created first. First of all, they emphasized that appropriate signal-transmitting materials (such as concrete structure) should be used when establishing the facility, the right device, firewall, switch, cable selection should be made, and that licensed and effective server companies should be worked with for server support. In addition, they stated that external threats can be kept to a minimum by establishing server bridges between companies and adding virtual LANs to the network infrastructure. These applications and network structure can protect data disclosure and create a secure data exchange framework on a chain basis.

Another strategy that experts agree on is data encryption and monitoring. Encrypting and continuously monitoring data that is kept in systems and shared within the chain is an important defense method against unauthorized access and data manipulation. Continuous monitoring will provide an opportunity to detect any intervention early on and prevent it from spreading. On the other hand, applying various encryptions will both make it difficult to access data and ensure that the data remains unreadable even if access is provided, thus protecting sensitive data within the supply chain.

The seventh strategy for information security is establishing an internal audit department. Internal audit departments are in a preventive shield position, auditing data processing steps, incorrect configurations, in short, all internal company processes, reducing risks such as leakage and disclosure of information such as databases, sensitive data and documents. Internal auditing also identifies weak points in software, allowing information security to be effectively implemented across departments and to be constantly updated.

Another strategy that has been developed to ensure information security and reduce the risks that may occur after an information security breach is getting an external security audit. It was stated by many participants that external security audits are a step that should be implemented regularly every year for companies. These audits will ensure that situations that cannot be noticed by internal personnel are identified and revealed.

Investing in stakeholders is another strategy recommended by experts. Companies can reduce risks from external factors by implementing security and integration investments in stakeholders they already cooperate with and stakeholders they see potential for. One of our participants working in a 3PL company stated that they are already implementing this strategy. Since small stakeholders in the chain usually have access to the sensitive systems and data of large companies or there is a data exchange situation, a security breach on their side can lead to risks such as the disclosure of trade secrets and customs data or even the disclosure of company-specific strategies. Investments applied to stakeholders, practices such as providing training programs, security tools, and integration systems will help reduce these breaches.

Another strategy is the mandatory establishment of dedicated cybersecurity and in-house software development departments, which significantly strengthens an organization's ability to anticipate, detect, and respond to cyber threats. More than one of our participants also stated that they implemented the strategy in their current companies. A good in-house cybersecurity team will ensure that potential security vulnerabilities that could lead to major problems such as critical data breaches (customer data, trade documents, operational data) are monitored and attacks are prevented. At the same time, an in-house software department will provide the opportunity to solve software integration processes and problems, develop special

encryption and solutions on a system basis, apply special patches, and respond quickly to problems. The two departments established with this strategy will also reduce external dependency and provide a great advantage in cases where possible response times may be delayed.

Experts have stated that regular access controls are implemented throughout the companies' networks and information systems and that entry restrictions are imposed on these networks and systems as another strategy. With this strategy, only authorized persons will be able to access sensitive areas of the system, and auditability and accountability will be clarified, thus limiting attacks.

Regular drill practices are another strategy that experts agree on. They stated that practices such as routine cybersecurity drills, cybersecurity scenario simulations, system tests, penetration tests, and simulations will keep both the system and personnel ready for possible cybersecurity incidents. These practices will reduce software integration problems, keep personnel informed and ready, and prevent possible data manipulation.

Another strategy that emerged from the analysis of the experts' responses is regular systems security updates, reviews, configurations and maintenance. Participants reported that all software, systems, antivirus programs, firewalls should be kept up-to-date, incoming updates should be constantly checked and applied, these systems should be constantly monitored, maintained and configured periodically, patched regularly, and system locks should be regularly checked, and changes should be made. It was reported that out-of-date systems invite possible cyber-attack results such as data disclosure and manipulation.

According to common expert opinions, another important strategy that should be implemented is reported as stakeholder audit. Experts emphasized the importance of safe partner selection, and emphasized that partners should be regularly monitored, audited, rules and contracts should be imposed on partners, and that companies that apply security assessments to potential stakeholders and fail to successfully complete these assessments should not be worked with for safe partner selection. These practices will bring a security standard to the supply chain ecosystem and will largely prevent attacks that may result in the seizure of sensitive data originating from weak links, and

the standardization provided on a chain basis will also prevent possible integration problems.

According to experts, another strategy that should be implemented is the implementation of secure and standardized EDI systems. They reported that EDI systems provide encrypted, secure and traceable data sharing among all chain stakeholders due to their structured structures, unique file types and encryption, and easy integration. It was added that potential integration problems will be eliminated with all stakeholders turning to EDI systems, and sensitive data shared with encrypted file formats will be protected.

Another strategy suggested by experts is the use of security software. The strategy includes licensed antivirus programs, proper firewall usage, use of AI security systems, IDS, use of secure file transfer protocols (SFTP), use of virtual private networks (VPN), use of web-based systems, patch management and solutions such as 802.1xNAC. The implementation of these solutions will greatly reduce the rate of cyberattacks, thus preventing all information security impacts.

The final strategy revealed in the expert responses for this section is using multi factor authentication. Multi-factor authentication provides an important additional layer of security by demanding several different access credentials to be entered in order to access an account, thus lessening the potential for account compromise even in a stolen password situation. This strategy covers vulnerabilities such as unauthorized access to all sensitive data and reduces the risk of data breaches from cyberattacks such as phishing attacks by requiring multi factor authentication protocols for all systems. Additionally, the method will provide accountability and the ability to generate access reports that can be used in taking action for incidents or in auditing processes. Table 42 below provides mitigation strategies and illustrative quotes to mitigate information security ripple effects.

Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects.

Ripple Effects	Mitigation Strategy	Quote
All Information Security Impacts	Backup in cloud and different locations	<i>"Backup and regular backup of all critical data and storing these backups in different physical and cloud-based locations. This makes it possible to minimize data loss in the event of a possible attack." (3PL2)</i>
All Information Security Impacts	Budget allocation for security	<i>"As an industry, I believe significant amounts of money should be invested in IT. It's crucial that people stop allocating only small budgets to this and treating it as something unimportant. As I mentioned earlier, there's still a group of suppliers in Turkey who don't take cybersecurity seriously. There are companies operating with just 10 vehicles, two chairs, one desk, and even using a Gmail instead of Outlook account to conduct business. These practices need to be addressed and brought to a much more advanced level." (3PL1)</i>
All Information Security Impacts	Certification and Standardization	<i>"There are other security frameworks that we follow on top of 27001, such as NIST, SANS, or those that stem from our own knowledge. We apply the tactics there. We use certain tools while applying the tactics there. We use certain methods. We have regular scans; we have penetration tests. We use active security measures, such as CM. There are products such as XDR and EDR. There are third party teams that follow the alarms sent by these. We also have our friends inside. I can say that we follow in this way." (3PL9)</i> <i>"Certification is the most important thing here. As I said, the world has already solved this issue. If you are going to get a supply chain security certificate, it will have to be ISO27001. Including our customs. The Republic of Turkey customs does not give the AEO Authorized Economic Operator Status certificate to those who do not have an ISO27001 certificate. Therefore, certification is very important." (3PL3)</i>

Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects (Continued).

All Information Security Impacts	Create Emergency Response Teams	<i>"In the event of a cyberattack, emergency response teams should be the first to step in. These teams take action to find the source of the attack, limit the damage, and quickly recover systems. In addition, backup systems should be put in place to try to regain access to lost data." (3PL2)</i>
All Information Security Impacts	Creating an effective network infrastructure	<i>"Here, from device selections, that is, even if we skip firewall and antivirus, choices need to be made according to the features of the switches used, according to the cables, and unfortunately I don't think every company can do this. Big companies probably do it." (CC2)</i> <i>"Again, within this system, you need to set up various LANs, such as virtual LANs, so that individuals within these networks cannot access other areas and view or interfere with the data there." (P1)</i> <i>"Of course, there are occasional problems. The reason for this is that the factories are very old. Due to the concrete used in the factory, the signals, namely these internet signals, security provider signals cannot be transmitted." (MNI)</i>
All Information Security Impacts	Data Encryption and Monitoring	<i>"Security is provided in several different layers during these processes: Well, data encryption is one of them. During data exchange with stakeholders, all information is encrypted and secured. Encryption is used both in data transmission and storage." (3PL2)</i> <i>"Apart from that, we monitor and audit data. Shared data is constantly monitored and audited. We also check the security of our systems with regular cybersecurity tests and audits." (3PL2)</i>
All Information Security Impacts	Establishing an internal audit department	<i>"We have our own internal audit department that checks these authorizations twice a year, once or twice a year." (P1)</i>

Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects (Continued).

All Information Security Impacts	Getting External Security Audit	<i>"In this sense, there is also a security company from which we receive consultancy services, not consultancy services but actually an operation, namely a security operation center service." (3PL9)</i> <i>"For example, regarding authorization, we have an auditor. We tell the auditor to check these things, and they do, but we don't stop there. We also ask more professional individuals to review it. For example, in the case of an attack, after the action is taken, let's say an attack occurred and you were affected, after taking your precautions, the checks need to be done again immediately after the attack. These checks should be done by relevant professionals, confirming that there is no longer a need for such an action and that your vulnerabilities have been closed. They should also provide a list of potential vulnerabilities and how to address them. The configuration and maintenance of things like privileges, network firewalls, and related topics should definitely be checked by an external professional at least once a year." (P1)</i>
All Information Security Impacts	Investing in stakeholders	<i>"Our supply chain partners are the following, the most important of which are Borusan Logistics and Spot Cars in Izmir; in other words, when we supply from outside, we work with Mars Logistics and DHL. Our logistics partners are these 3 main companies. They cooperate the most with Borusan among these 3 main companies. In other words, the security aspect of Borusan is actually provided by Efes. Of course, these are the computers used by Borusan's office, office or employees working in the supply section to Anadolu Efes, of course, not only in the main office." (MN1)</i>

Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects (Continued).

All Information Security Impacts	Mandatory establishment of a cybersecurity and in-house software departments for companies	<i>"We have offices in many countries, when I say many countries, I mean Poland, Bulgaria, Italy, France, and all our software here is our own internal software, our own security, our own internal security provided by our IT department, so we can provide this security with our own internal structure, regardless of which country our office is in." (3PL8)</i> <i>"We have a cybersecurity department. We have a cybersecurity defense center department. We provide this within ourselves in 3 different locations. Of course, we receive service from Microsoft or other companies. We also have consultants." (3PL5)</i>
All Information Security Impacts	Network and Systems Access Control and Restrictions Implementation	<i>"Access controls are limited according to the roles of employees. We restrict unnecessary access rights and ensure that only certain people can access critical data." (3PL2)</i> <i>"Our company works like this, namely personal ID cards, in other words, we use our ID cards even when taking printouts from every door, turnstile or printer. Without scanning this card, our magnetic cards defined in the system are never printed or we cannot enter or exit the factory or make any movements in the system. " (MNI)</i>
All Information Security Impacts	Regular drill practices	<i>"So, my professors used to say here. Back-up, back-up, back-up backup, backup, backup, this is the most important thing, if it doesn't happen, you can't do anything. Secondly, drills and penetration tests should be done periodically regarding this cyberattack, so you need to be prepared for this. You always need to be ready as if you're going to experience this problem 2 years later. Back-ups need to be checked from time to time. Even if nothing happens, you need to try to get out of this with as little damage as possible." (3PL7)</i>

Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects (Continued).

All Information Security Impacts	Regular Systems Security Updates, Reviews, Configurations and Maintenance	<i>"Absolutely, as I said, there was no attack here or I don't know what happened in America, the firewall devices we use, the antivirus company takes precautions against these. We also keep them up to date." (CC2)</i> <i>"We think we are good at this. As I said, we keep ourselves up to date and try to make updates. We also check its resistance with the firewall and various penetration tests we conduct at certain intervals." (3PL7)</i> <i>"Our hardware (server, client, network) is kept up-to-date with our patch management software." (3PL11)</i>
All Information Security Impacts	Stakeholder Audit	<i>"Also, as I said, as I mentioned, our customers have increased a lot, especially after the pandemic, in the sector. Our customers have almost made this a tender condition. Especially global customers definitely send an assessment either in the renewal of tenders or contracts or in new tenders. Some of these assessments go up to 300 questions and you know, down to the most detailed, what do you do in such a situation? Do you have such a security policy, how do you do instant response? Will you notify us in such a situation? Etc. We have started to enter into very serious assessments. For about 2-3 years, almost one of my friends has been dealing with an assesment every month. In this sense, of course, this has positively affected us." (3PL9)</i>
All Information Security Impacts	Use of EDI	<i>"When EDI transactions are made, there are specific file types and codings involved. Each system does this in a coded manner. Therefore, since the parts that solve and code this are the same, and because everyone uses the same program in a shared manner, they can adapt it to their needs. For this reason, at this stage, we do not see much of a cybersecurity threat in this situation, as it is a more secure and robust structure." (P1)</i>

Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects (Continued).

All Information Security Impacts	Use of Security Software	<i>"The main measures we take are network security; all networks must be protected by a strong firewall. We also use IDS in our systems. Suspicious activities are immediately flagged and investigated." (3PL2)</i> <i>"Stronger data encryption methods, AI-powered security systems, and continuously updated cybersecurity strategies will be the most important steps. Additionally, the establishment of common security standards and collaboration across the industry will play a key role in this process. Critical infrastructure investments will help increase the resilience of supply chains by focusing on security." (3PL2)</i> <i>"We also present users with up-to-date data through information trainings within the company, and we act in accordance with ISO 27001 standards. We have an antivirus system, firewall system, and 802.1x NAC solution. We stay up-to-date with patch management and WSUS. We have continuous backups to protect our test and live databases. We use our systems over the cloud. In addition to our data center, we also have a DRC (Disaster Recovery Center). Our systems are scanned globally by professional teams, and our e-mail systems and antivirus systems are managed from a single source. Computers are closed to USBs. We also have banned sites that need to be closed with Web Filter." (3PL11)</i>
----------------------------------	--------------------------	--

Table 42. Mitigation Strategies and Illustrative Quotes to Mitigate Information Security Ripple Effects (Continued).

All Information Security Impacts	Using Multi-Factor Authentication	<i>"The software solutions used have security protocols such as strong encryption and multi-factor authentication. In addition, our employees are regularly provided with cybersecurity training. Anomalous activities are closely monitored on our networks with firewalls, IDS and continuous monitoring tools." (3PL2)</i> <i>"Even in our company, while you could only enter the system in one step before, now it forces you to enter the system in 2-3 steps, via phone or another device." (MN2)</i> <i>"Therefore, a serious level of control is required in terms of networking. In addition to masking the data within the software, you also need to use various servers that require identity and authentication verifications to ensure network security." (P1)</i>
----------------------------------	-----------------------------------	--

5.4.4. Mitigation Strategies for Information Sharing Impacts

Fifteen different strategies were developed based on participant feedback and content analysis to reduce the ripple effects identified in the area of information sharing. This section examines fifteen strategies designed to reduce the critical information sharing ripple effects observed in the study.

As frequent partner audits have been proven effective in protecting partnership information-sharing processes, cybersecurity audits check for protective measures a partner has in place regarding sensitive information to determine if they are adequate. If companies conduct audits for all members of the supply chain, they would be able to mitigate damages turned from potential vulnerabilities. Implementing partner audits increases cooperation ease, since cooperation challenges are greatly reduced due to uniform adherence to minimum cybersecurity standards. During critical operations, this helps reduce breakdown in functions, improving smooth communication during operations, as there is minimal misunderstanding. Partner audits can also help identify unprotected systems vulnerable to data loss, enabling maintenance of integrity

throughout the information chain. Without frequent audits, stakeholders may carelessly increase risk exposure through weak encryption standards, insecure integration points, or outdated software.

Another critical strategy is to implement industry-recognized certifications and standardizations with supply chain partners. Certification ensures that firms meet pre-specified cybersecurity requirements and achieve consistent efforts to enable secure, standardized data transfer. Standardization addresses software integration concerns by addressing interoperability among different systems and reducing the different kinds of technical frictions related to integrating their systems. Standardization also enhances collaboration by establishing clear expectations for handling information in a way that diminishes ambiguity and increases trust among supply chain partners.

Our next strategy is effective communication and cyber information sharing, which are essential for information sharing processes. Effective communication and the use of communication mechanisms are very important to prevent communication disruptions in supply chains during cyber incidents. If all stakeholders in the chain can access the right information at the right time, the ability and process to make decisions at the time of the incident will increase and cooperation problems will be minimized. In addition, if companies share their cybersecurity status and cyber threat data, whether they are under attack or not, instead of hiding them openly from the entire supply chain, the defenses of all stakeholders in the chain will automatically improve and the probability of data loss will decrease with the coordination provided.

Regular and systematic scanning and monitoring of data entering and exiting the systems is another important strategy for information sharing processes in the supply chain. This real-time monitoring will allow for the early detection of suspicious situations and threats and the prevention of interruptions before they spread to wider areas. With this continuous monitoring and tracking, companies will largely prevent the problem of undetected breaches and leaks and possible data loss. Moreover, the detection of any problem in the flow will prevent possible confusion, disagreement, chaos and interruptions between integrated systems. The strategy will also prevent cooperation problems in the chain as it will allow for the reporting of threats and sharing them with stakeholders in early detection cases.

When a cyberattack occurs, all electronic equipment and integrations must be isolated immediately to limit the damage, which is our next strategy. Disconnecting protects sensitive operational and strategic information by preventing malware or intruders from spreading into network systems. This tactic is particularly important as a way to prevent communications outages because by quickly disconnecting infected networks, businesses can keep clean lines of communication open for vital crisis communications. It also minimizes collaboration barriers and keeps stakeholders safe by clearly identifying compromised and clean assets during a disaster scenario. Additionally, disconnecting access acts as a temporary protection against information loss by preventing hackers from continuing to extract or contaminate information. It also temporarily immobilizes potentially weak points in the integration, preventing the possibility of cascading software integration failures throughout the supply chain.

Our next strategy is to implement a single shared network and systems for the entire chain. The use of a common, shared infrastructure of networks throughout the supply chain improves operational consistency and security. Common networking reduces the complexity of having multiple dissimilar systems and ensures that all partners work under a common set of security measures. By utilizing a single system, companies significantly minimize software compatibility problems since less bridging of compatibility issues among various platforms is required. Shared networks also enhance cooperation as the partners are able to communicate effortlessly through integrated tools and standards. In addition, a common system prevents communications breakdowns by enhancing the flow of information within departments and partners. Lastly, it minimizes the potential for loss of information as a centralized infrastructure is easier to monitor, safeguard, and recover from a hack than a disjointed one.

Another strategy put forward by industry experts is implementing highly secure data sharing protocols. Implementing advanced encryption-based data-sharing methods secures the exchange of sensitive information among stakeholders. Methods like the use of end-to-end encryption, the application of SFTP, and multi-factor authentication protect the information while it's in transit as well as when stored. Secure information exchange directly prevents the loss of information by ensuring that even if information is intercepted, it cannot easily be accessed. It also prevents communication disruptions by ensuring the security and integrity of the exchanged

messages, especially during a crisis. Moreover, standard secured protocols make integrating different systems easier, thereby preventing software integration problems.

Developing clear assessment criteria for stakeholders based on their cybersecurity maturity and operational reliability is another strategy that can reduce cybersecurity-related information sharing issues in the supply chain. These criteria are necessary to ensure that information can flow securely throughout the supply chain. It is not enough to evaluate partners solely on traditional dimensions such as financial performance and logistics. Stakeholders should also be evaluated on their ability to protect sensitive information and maintain system compliance. Assessment criteria strengthen the technical reliability of collaborations, address potential integration issues, and ensure that all participants share a security awareness baseline, leading to a supply chain where data can be shared comfortably.

The creation of an information sharing system designed to cover the entire supply chain is another strategy suggested by experts and can lead to secure, real-time and structured communication between stakeholders. This strategy can significantly reduce communication disruptions by creating a single central line for all stakeholders. Moreover, it will try to minimize collaboration difficulties by providing a common infrastructure where data and updates can be shared securely. Another important contribution of the strategy is that it can minimize integration problems when a built-in digital system is provided that allows interoperability of all stakeholders from the beginning to the end of the chain.

Another fundamental mitigation measure is the establishment of specialized integration teams to monitor and control system connectivity throughout the supply chain. These are the teams whose job it is to make sure that the technical interfaces between partners are correctly and securely configured. The integration group is an essential force hunting down bugs that arise from the need to have different types of IT systems to work together but without adding risk. It also reduces the difficulty of collaboration as it acts as a technical intermediary between organizations which is conducive to better cooperation. Effective integration avoids communication breakdowns that result from incompatible systems and eliminates the risks of data loss by eliminating points of data leakage or integration failure.

Another important strategy recommended by experts is to provide financial and operational incentives to stakeholders and invest in their security technologies and existing integration technologies. Companies that support their stakeholders with secure systems will also increase their own security. With the strategy, stakeholders with limited resources will also increase their security levels and an environment will be created where more secure data and information sharing will take place. In addition, since more compatible integrated systems will be used on a chain basis with stakeholder integration investments, software integration problems will also be largely eliminated.

Reducing the dependency on certain stakeholders within the supply chain is another mitigation strategy. Diversifying stakeholders is important so that the entire chain does not become paralyzed if any stakeholder is compromised. By minimizing the dependency on certain stakeholders, companies will be able to prevent interruptions to some extent and possible communication gaps will be reduced. Moreover, since operational risks will be distributed to a wider group of stakeholders, cooperation difficulties can also be prevented. Finally, turning to alternatives as a quick response in the event of any breach will also help reduce the risk of data loss.

The thirteenth strategy recommended by industry experts is system and data restrictions both internal and external side. Enforcing strong access controls and restrictions on both internal as well as external system interfaces strongly improves information flow security. Limiting system privileges as well as data access to necessary parties limits exposure to insider threats as well as external intrusion. It is a highly effective means of preventing loss of data by limiting would-be attackers' access points to a minimum. It also makes cooperation stronger by having everyone act in a well-defined security context, minimizing misunderstandings as well as conflict. Access controls maintain system integrity, hence preventing software integration problems, and by securing information flow, preventing breakdowns of communication during operations as well as crises.

Implementing secure cloud platforms for data sharing provides a scalable, resilient, and protected secure information sharing environment to manage supply chain information and enable information sharing, which is the fourteenth strategy. Cloud services typically provide encrypted data storage, controlled access, and real-

time synchronization between multiple users. Using the cloud eliminates communication interruptions by enabling real-time, reliable communication between distributed partners. It also reduces data loss, as cloud providers often implement redundancy and backup measures that enable data recovery even in the event of system failures. Moreover, cloud-based solutions facilitate smoother software integration, as many modern platforms offer compatibility across different systems and APIs, thus increasing collaboration among supply chain stakeholders by providing standardized data sharing infrastructures.

The final strategy we have uncovered with the responses of industry experts to reduce information sharing problems is the use of EDI. Implementing EDI systems allows for standardized and secure data exchange between all chain links. The importance of EDI in information sharing processes is that it eliminates many of the processes that may cause errors, delays or security gaps in the flow. EDI implementations prevent communication interruptions thanks to automatic information flow and can help eliminate collaboration and integration problems by creating a single communication channel that all stakeholders can trust. Since it provides encrypted data sharing where manual intervention is minimized, data loss risks are also minimized. Table 43 below provides mitigation strategies and illustrative quotes to mitigate information sharing ripple effects.

Table 43. Mitigation Strategies and Illustrative Quotes to Mitigate Information Sharing Ripple Effects.

Ripple Effects	Mitigation Strategy	Quote
cooperation challenges, loss of data, software integration issues	Constantly scanning and monitoring data inflows and outflows	<i>"Of course, we are running a process as an intervention against cyber incidents. We have precautions for this, such as the operation of some sensors on firewalls, scanning through 6-7 different layers. Therefore, we are doing serious work on the up-to-dateness of antiviruses on the end user side, the character and capabilities of the software. Therefore, we are trying to position the right product, the right security measure in the right place." (P2)</i>

Table 43. Mitigation Strategies and Illustrative Quotes to Mitigate Information Sharing Ripple Effects (Continued).

communication breakdown, cooperation challenges, loss of data	Auditing Partners	<i>"Well, we say this in the purchasing department, that is, when choosing a supplier as much as we can, does it have a document? Does it have a policy at least, that is, this is already a requirement of 270001. I think there should be something important in supplier evaluation, in other words, supplier selection. And we want them to take these into consideration when evaluating suppliers. We also evaluate some suppliers in this way, on-site or, in other words, like the evaluations our customers make to us, that is, this is a developing culture in Turkey. But of course, as I said, it comes down to something again. In other words, price is always an effective element in every subject. Those who offer a good price can still get out of the way even if these are missing. I hope they will not get out of it anymore; I hope that a solution will be found with regulation." (3PL9)</i>
cooperation challenges, software integration issues	Certification and Standardization	<i>"As I said, standardization, certification and training, it will already be with that. You know, there will be such things that with the company that does not have a security certificate, right now our information processing software even blocks the computer I use at home if the website I want to visit is not secure, it asks are you sure, it says look there, your information may be stolen, this site is behaving suspiciously. What happens and thus it pushes it out of the system. So, this will happen in the future as well, for example, I know something in Izmir, I know a health institution. A private hospital, I could not access the website for days, I could not communicate, because the website was not secure, my computer rejected it when I connected and this is a huge company, a health institution that makes money. For example, I have no trust left in that institution. But they are reducing their own thing, what happened, my company is lacking in a customer, we do not do anything with them, we do not do business, we do not go to examinations, we do not want them, etc. because there is no information security. It should be given importance to comply with certifications, education and as I said, understanding these standards in all our stakeholders and showing the same seriousness." (3PL3)</i>

Table 43. Mitigation Strategies and Illustrative Quotes to Mitigate Information Sharing Ripple Effects (Continued).

cooperation challenges, loss of data	Communication and Cyber Information sharing	<i>"Unfortunately, I don't know the answer to that. But as a result, they have to share information. For example, when another company is directly subject to a cyberattack, they have to announce it directly, which is already a necessity. They have to inform their customers and suppliers immediately so that they don't open emails from them or if there has been any data leakage, and as a legal obligation, they have to keep themselves safe because if I find out that my information has been shared somewhere else, from another person, I would file a huge lawsuit against the company. But the company has to announce it directly so that at least I can take my precautions and they can take their precautions. Sometimes we get warnings like there has been a leak from this company, emails from this company have been temporarily blocked, our system blocks them immediately, our defense center." (3PL5)</i>
All Information Sharing Impacts	Cut off access to all electronic devices and integration	<i>"At first, it's important to detect the source of the cyberattack. Once you've identified it, the first step is to block that part of the system. After that, you'll need to figure out the next steps, like if the attack is coming from an external source, you should disconnect from the firewall and sever communication with the outside. You should then look at which ports were used, how the attack came in, and directly block those ports. We need to open the system and monitor if the attack is still ongoing. It may be necessary to block certain addresses, or other mitigation methods can be considered. The first thing to do is eliminate the current situation and then proceed with the necessary updates and configuration adjustments." (P1)</i>
All Information Sharing Impacts	Implementation of a single shared network and systems for the entire chain.	<i>"Supply chains need to operate over a large network against cybersecurity, and all companies need to operate over that network, meaning there is only one common connection, so it will be difficult to overcome it. There needs to be a single common connection, and I say a single IT department should look after the entire chain." (3PL10)</i>

Table 43. Mitigation Strategies and Illustrative Quotes to Mitigate Information Sharing Ripple Effects (Continued).

communication breakdown, loss of data, software integration issues	Implementing highly secure data sharing protocols	<i>"So, all of our things, movements, movements within the system are blocked and we collect them in a product called CM and with certain correlations, we provide both writing of alarms, sending of alarms and 24/7 monitoring. Apart from that, there are some products, of course, there are security products that we use." (3PL9)</i>
cooperation challenges, loss of data, software integration issues	Implementing stakeholder evaluation criteria	<i>"Before we start working with suppliers, we first assess the supplier's profile. This includes details such as what documents they have, who they are, their capital, the extent of their insurance coverage, and other relevant information. On the operational side, for example, when I send a shipment through a carrier, we collect detailed information such as who is going, which vehicle is being used, the vehicle's license plate, the driver's name, phone number, and other similar details. We also gather container information from warehouses." (3PL1)</i>
communication breakdown, cooperation challenges, software integration issues	Information-sharing software covering the entire chain.	<i>"Network formations that will ensure more cooperation in the sector regarding cybersecurity and the establishment of structures that will ensure information transfer will be beneficial for operational processes and stable continuity on a sectoral basis. Companies should come together on platforms that encourage information sharing and share their experiences." (3PL12)</i>
All Information Sharing Impacts	Integration Team Implementation	<i>"Of course, the biggest risk here is always the supplier. We also tell this to the upper management; I mean all the time. Because the one you cannot control, I don't know, it could even be a consultant or something. A consultant who connects once a day, once a month, can come with a virus from your computer. Therefore, this side of the supplier, that is, their access to your system, is a very problematic issue. It is an issue that needs to be controlled very well. You have to open your system on one side and let them in, but since it is a point you cannot control very much, we bring certain technical precautions for this. So, so that the person does not connect directly to the system, we try to get them into the systems with applications such as what we call a terminal, like we do now, like I actually see your screen, but the file is not with me, I just see it." (3PL9)</i>

Table 43. Mitigation Strategies and Illustrative Quotes to Mitigate Information Sharing Ripple Effects (Continued).

loss of data, software integration issues	Investment and integration incentive practices for stakeholders	<i>"We provide advice and incentives to companies that grow with us and to partners that we believe will grow and stay with us for a long time with our investments, investment examples, and system integrations." (3PL8)</i>
communication breakdown, cooperation challenges, loss of data	Reducing stakeholder dependency	<i>"The most important thing is definitely for them to invest in security. They shouldn't partner with just one company; that would be a mistake. At least two companies should be involved in collaboration because, as I mentioned, there needs to be a backup of the system's backup. For example, in transportation, it would be wrong to work with just one company. That's why we partner with multiple companies to ensure we don't fall short in these areas. You shouldn't rely on just one person. A lot of investment is needed, and technology should be utilized." (MN1)</i>
All Information Sharing Impacts	System and data restrictions both internal and external side	<i>"We leave these files at the addresses given for SFTP files, and they retrieve them from our address. While ensuring this process, we specify that only connections, requests, user codes, and passwords coming from this address should be accepted, meaning not just with the user code and password but also confirming the reliability of these addresses. In this way, a secure file exchange takes place, and apart from the security measures applied locally, we do not apply anything additional, to be honest." (P1)</i>
communication breakdown, cooperation challenges, loss of data	Use of Cloud for Data Sharing	<i>"For external purposes, our correspondence is always provided via corporate e-mail. Data transfer is provided through OneDrive and e-mail sharing methods." (3PL11)</i>
All Information Sharing Impacts	Use of EDI	<i>"At this point, software is truly important. People need to give more importance to software development. Also, companies should never leave data exchanges between each other to third-party software, such as using Excel to transfer data here and there. Instead, they should be using EDI systems for such tasks. Therefore, EDI integrations should be implemented within existing software systems so that companies can perform tasks in a more efficient and secure manner." (P1)</i>

5.4.5. Legal Mitigation Strategies

In the impacts section, we discussed how legal impacts associated with cyberattacks can initially be negligible but later turn into serious, long-term impacts such as regulatory fines, contract breaches, and legal action for companies in the supply chain. Based on the interviews, this section identifies three key mitigation strategies to respond to legal vulnerabilities. These strategies help reduce the legal spillover from cyberattacks and create a solid foundation for long-term compliance and resilience.

Following and strictly implementing national cybersecurity regulations and standards is our primary strategy to reduce legal impacts. Participants drew attention to the Personal Data Protection Law (KVKK), AEOS and Information Security Management System (ISMS) practices and regulations. In addition, they emphasized the importance of fulfilling the requirements of certifications such as ISO27001. Such practices not only ensure data security, but also significantly reduce the possibility of financial penalties and reputational losses that may occur in possible legal violations in the event of a cyberattack. Moreover, companies with documented compliance are in a more advantageous position in legal processes following cyber incidents, and this situation brings stakeholder assurance and strengthens trust throughout the supply chain.

The second strategy we uncovered, based on responses from industry experts, is government-mandated cybersecurity rules and intervention practices. Government intervention, through mandatory cybersecurity standards and emergency response processes, was also identified as another important mitigation tactic. Regulators can instrumentalize cybersecurity by establishing minimum cybersecurity expectations or requirements for port authorities, 3PL service providers, importers/exporters, customs agencies, ship owners, and retailers. Standards can level the playing field and can equally provide defenses against multiple legal failures along the supply chain if an attack occurs. Interview participants stated that banking systems are supervised by the state, and they also questioned why there are no state-authorized cybersecurity teams for the supply chain when there are institutions such as law enforcement agencies that provide public security, and they underlined the urgent need for this. They reported that in this way, chain security will be ensured, and legal problems can be prevented through legal means, that is, state practices.

Lastly, it is important for supply chain partners to formalize detailed security agreements legally where possible in order to limit the ripple effects of cyberattacks. Security contracts clearly articulate roles, responsibilities, liabilities, and security expectations across all stakeholders. Should an incident occur, clearly defined contracts will aid in clarifying accountability, limit ambiguity, and assist in legally managing the features of drawn-out litigation. This is in alignment to our discussions from the interviews. Getting cybersecurity expectations in a formally articulated, contractual structure varies the long-term risk to participants in a supply chain and reinforce mutual trust, improves active risk management, and all participants are legally protected from negligence and inaction on the part of other actors in the network. In addition, the agreements provide a baseline from which to coordinate incident recovery and incident response efforts, while simultaneously adding legal resiliences to protect the entire supply chain. Table 44 below provides mitigation strategies and illustrative quotes to mitigate legal ripple effects.

Table 44. Mitigation Strategies and Illustrative Quotes to Mitigate Legal Ripple Effects.

Ripple Effects	Mitigation Strategy	Quote
Legal Sanctions	Complying with legal requirements	<i>"It is essential to harmonize cybersecurity standards in the sector and increase security cooperation between companies through national and international regulations." (3PL2)</i> <i>"Yes, as a company or as a target, we are trying to catch up with the standard and exceed it. But unfortunately, as a sector, I do not think it is like this. We are trying to implement the requirements of ISO27001. Our KVKK compliance processes are constantly ongoing. Our adaptation to new technology continues, but unfortunately not every customs company is like this. We are trying to comply with many issues and standards." (CC2)</i> <i>"Compliance with laws (5651, YYS, BGYS) is always ensured at the highest level in the company. " (3PL11)</i>

Table 44. Mitigation Strategies and Illustrative Quotes to Mitigate Legal Ripple Effects (Continued).

Legal Sanctions	Government-mandated cybersecurity rules and intervention practices	<i>"I'm not sure if the government would provide support, but it could impose a requirement. Just as every company has an accountant, every company that operates online or uses computers should also be required to have a team, individual, or firm responsible for cybersecurity. If such a requirement were introduced, I believe it would be excellent for companies. It's a good analogy—just as the state is responsible for the safety of citizens walking in the streets, with law enforcement ensuring public security, I think companies should also be responsible for their own security. As you mentioned, there could be support plans or certain implementations and restrictions introduced. For example, when establishing a corporation, there could be conditions such as, 'You must meet these specific requirements before you can start a business.' It could be, 'You need to allocate this amount of budget, have this level of partnership, and fulfill these specific criteria.' Similarly, during the company registration process, there could be security-related conditions like, 'Your security level must meet these standards, and you need to pass through these security phases.'" (3PL6)</i> <i>"I was asked this question at the board of directors. They said, look, we spend so much time on these jobs, we do everything, but they named some company. This company does none of these. They bid much lower than us and win many tenders. When they asked what will happen to this job, I gave the same answer. Because they are not subject. Being subject is also at the initiative of the company. I mean, you only become subject if you get the AEO, is that not enough? I mean, getting a 27001 certificate is not a very difficult task today. I mean, we know that you can get it even if you do not meet all the conditions. It does not seem very realistic to me. Therefore, I think this needs to be done more seriously." (3PL9)</i> <i>"As I have just mentioned, the public sector is of great importance here. The only umbrella that concerns logistics and daily consultancy, exporters and importers in international trade, which we call the public sector, is actually the Ministry of Trade for us. I think a technology data information department should be established in the Ministry of Trade regarding this. A team that will provide technical support to third parties in all matters should be established with the experts to be recruited under this department, and a working group should be established by reaching out to all members of the supply chain, and everyone should be able to trade safely using a single system, provided that the chambers of commerce and industry and the exporters' union are also included in this work." (CC1)</i>
-----------------	--	---

Table 44. Mitigation Strategies and Illustrative Quotes to Mitigate Legal Ripple Effects (Continued).

Legal Sanctions	Security Contracts	<i>"Of course, we make a contract. Therefore, it is very important for us that their data is protected and that their data is backed up according to the KVKK laws."</i> (CCI)
-----------------	--------------------	---

5.4.6. Operational Mitigation Strategies

In this section, seven mitigation strategies were determined based on the content analysis of the semi-structured interview to minimize the operational impacts of cyberattacks and prevent attacks. These strategies are: backup in the cloud and in different locations, conducting operations from different locations, establishing a crisis management team, developing disaster recovery plans, keeping backup software, manual operations management and using cloud technologies.

Firstly, keeping data backups across multiple cloud environments and accounts stored in different locations rather than in a single cloud environment allows critical operational data to remain accessible when one or more systems are attacked or compromised. In our analysis of the impacts, we found operational impacts such as shipping delays, tracking errors, and warehouse management issues. This diversified backup strategy can enable faster system restores and therefore reduce downtime. This can prevent service bottlenecks that can spread throughout the supply chain.

The second strategy we uncovered, based on responses from industry experts, is conducting operations from different locations. By using multiple locations to provide operational decentralization, even if one facility is compromised, the sustainability of operations from other facilities can be ensured. The strategy contributes to overall operational sustainability by preventing distribution disruptions and disruptions to transportation operations. Furthermore, it protects against delivery delays, lost deliveries, and transportation planning issues that we have seen during our impact analysis, thus keeping disruptions to critical operations to a minimum.

The third strategy we uncovered, based on responses from industry experts, is crisis management teams. A dedicated crisis management team is essential for a well-organized, rapid, and effective response to cyber incidents that can threaten operational continuity. In the absence of a defined crisis response structure, companies are

extremely vulnerable to coordination issues, efficiency issues, and ineffectiveness. Companies can quickly find themselves in a downward spiral, leading to unacceptable service and operational performance across the supply chain. When a dedicated crisis management team is properly established, develop, and implements a structured incident response framework to react to some level of disruption. The framework ensures that if a cyberattack, disrupts digital systems, firms can respond very quickly and effectively with manual operations management and workflows as effectively as possible. It also gives them time to understand the nature and extent of the cyberattack, establish their priorities, and coordinate their recovery. Crisis teams can coordinate their recovery across all companies and firms, limiting the issues of software integration, shipment tracking issues, and container tracking issues that are among many key vulnerabilities that frequently exist, when a cyber breach occurs. In addition, crisis management teams are key and pivotal in minimizing operational breaches, distribution breaks, and disrupted shipping operations by communicating clearly between departments and stakeholders. Their resource allocation (or resource allocation) efficiencies are likewise opportunities to reduce the time for import/export activities to be delayed, delivery delays, or transportation planning. This helps maintain goods and service delivery and flow, even in emergency situations. They also cooperate (continuously) monitor to make rapid, data-driving decision-making to avoid potentially worse implications related to emergency situations (operational data loss, product inventory issues, delivery inaccuracies, and production down times). In addition to those abovementioned, protecting finance operations from collapsing completely allows organizations to engage critical economic activities while employees are recovering from crisis situations. Even further, crisis management teams are key components to the timely detection of order fulfillment failures, lost product deliveries, and stolen deliveries - and therefore critical to diminishing reputational damage or harm, client dissatisfaction, and business relationships. They also help coordinate to activate back up plans (cloud platforms or localized) to secure data, and continuity of operations.

The fourth strategy we uncovered, based on responses from industry experts, is Disaster Recovery Plans (DRPs). The participants believed DRPs are crucial, to predetermine an organized set of actions that need to occur to restore operations following a cyber incident. A comprehensive DRP will enable a company to rapidly

respond to their operational disruption, helping to minimize operational confusion during a crisis and subsequent restoration. Companies face a greater risk of an incorrect delivery or an incorrect production plan, or simply having problems with product inventory, if there is no DRP. During a cyber-attack a company's operational data and its software systems around them may be compromised providing numerous opportunities for disaster recovery failure. A structured recovery plan will ensure a company can restore a majority of its operational logistics functions, such as tracking shipments (containers, vehicles), and ensure that cascading failures do not happen throughout the supply chain. The DRP puts the company in a position to quickly recover from issues like loss of operational data, workflow being mismanaged, and warehouse management errors ensuring they can return to essential logistics planning activities without long delays. Simply put, disaster recovery plans are an essential safety net to quickly restore operations and safeguard their supply chain network as a whole against the indirect impacts of service interruptions and operational inefficiencies.

Another strategy we came up with based on responses from industry experts is keeping backup software. Aside from data backup, having readily accessible duplicates of key software applications or completely a secondary software is important for managing operations risks. Post-attack, core operations systems can be breached, causing shipment tracking to fail, causing confusion with their logistics plans, and causing warehouse management failures. Backup software enables firms to easily transition to backup platforms, creating continuity with inventory control, transportation scheduling, as well as delivery tracking. This minimizes service performance failures as well as hijacked deliveries, both of which take a huge hit on supply chain dependability.

The sixth strategy we uncovered, based on responses from industry experts, is manual operations management. Being able to work manually as a backup when digital systems fail is a significant contingency arrangement. Working manually can keep things going under crises, avoiding breakdowns in import/export processing, order fulfillment, as well as product delivery. It provides a bridge for the duration of extended system failures, lessening the adverse effects of mismanagement of workflows, loss of resources, as well as breakdowns of coordination. Witnesses emphasized that businesses that were able to transition seamlessly to manually based

methods succeeded in avoiding widespread paralyzing operations as well as establishing a baseline level of service even with cyber breakdowns.

The last strategy we uncovered, based on responses from industry experts, is use of cloud. Using cloud technology improves business resilience through scalable, redundant, and secure infrastructures for core applications. Cloud environments provide immediate restoration of data through real-time data recoveries to enable firms to overcome data loss incidents, software integration failures, as well as shipment tracking mistakes. It is recommended that cloud operations enable the quicker restoration of core processes as warehouse management, order fulfillment, as well as transportation planning. Cloud adoption can reduce productivity impediments as well as keep service delivery intact even under the threat of hacking. Table 45 below provides mitigation strategies and illustrative quotes to mitigate operational ripple effects.

Table 45. Mitigation Strategies and Illustrative Quotes to Mitigate Operational Ripple Effects.

Ripple Effects	Mitigation Strategy	Quote
warehouse management failures, container tracking failures, delivery delays, delays in import/export, logistics planning confusion, loss of operational data, distribution breakdown, shipment tracking failure	Backup in cloud and different locations	<i>“Yes, we normally take backups of our systems all the time. Backup policy is very important in this sense. Keeping different copies of the backups of the systems at different points. For example, if we were to give an example here, we normally take many steps to prevent cyberattacks. However, we may not be able to prevent them, and we start to suffer damage. Of course, we encourage and close these connections. In cases where we suffer damage, we actually keep a backup of our systems in different locations, that is, in different cloud providers outside the company, so that we can have feedback from there, backup processes are very important here.” (P2)</i>

Table 45. Mitigation Strategies and Illustrative Quotes to Mitigate Operational Ripple Effects (Continued).

lost deliveries, incorrect deliveries, stolen deliveries, delivery delays, operational breakdown, operational congestion,	Conducting operations from different locations	<i>"Of course, not every operation there can be done in another facility. Because there are automation systems, but we can move some operations. In other words, we can move the goods and do the operation there or we can run some of the systems in other ways. We can put manual processes into action. Even though some of them don't work, they require a lot of labor. In other words, they require a lot of effort. But we have things that we have backed up during these 3 weeks. For example, we have a separate storage in Ankara. We have plans like that where we keep our backups there, we can switch the operation there." (3PL9)</i>
container tracking failures, coordination challenges, delays in import/export, delivery delays, disrupted shipping operations, distribution breakdown, efficiency issues, finance operations breakdown, incorrect deliveries, incorrect production planning, logistics planning confusion, loss of operational data, loss of resources, lost deliveries, manual operations, operational breakdown, operational congestion, order fulfillment failure, performance inefficiency, product inventory issues, production shutdown, service performance issues, shipment tracking failure, software integration issues, stolen deliveries	Establishing a crisis management team	<i>"So, in conclusion, a crisis desk must be in every company. Disasters can happen; natural disasters can happen. Your data center may go. There may be an earthquake, a flood, these should be evaluated first for this crisis desk. The biggest advantage is that the people who will be here have experience. Those who are in these situations panic less, can see ahead or can close more risks." (3PL5)</i>

Table 45. Mitigation Strategies and Illustrative Quotes to Mitigate Operational Ripple Effects (Continued).

coordination challenges, incorrect deliveries, incorrect production planning, distribution breakdown, logistics planning confusion, shipment tracking failure, loss of operational data,	Disaster Recovery Plans	<i>"There are also disaster recovery plans. They need to be ready. In other words, what we call a disaster recovery plan is not just what happens if you are attacked in terms of information processing. For example, if there is an earthquake, all your information is lost where the server is. When no one can reach the server, all operations stop. But what is being done in the world now, servers are being distributed. In other words, these are happening in several countries, and they are backing each other up. These are important measures, and as I said, a disaster recovery plan needs to be ready. In the event of a disaster, plans such as what do we do, the backup server comes into play, the backup centers start working, etc. need to be ready." (3PL3)</i>
transportation planning issues, warehouse management failures, efficiency issues, loss of operational data, disrupted shipping operations, distribution breakdown, logistics planning confusion, warehouse management failures	Keeping backup software	<i>"For example, since we constantly use electronic archives, backup is very important for us. We do instant backups, we used to do daily backups, weekly backups, monthly backups. Right now, it is very important for us to back up instant data using the cloud system. It is also important to have a second software that will be activated as a plan B in case of a possible attack. In order for things to work immediately, we need to go outside the current portal and carry out transactions electronically with a new portal and a new user, and the program we are currently using is a system where we can back up our archive from which we can also get past data." (CCI)</i>

Table 45. Mitigation Strategies and Illustrative Quotes to Mitigate Operational Ripple Effects (Continued).

order fulfillment failure, delays in import/export, loss of resources, incorrect production planning, logistics planning confusion, coordination challenges, disrupted shipping operations	Manual operations management	<i>"Of course, not every operation there can be done in another facility. Because there are automation systems, but we can move some operations. In other words, we can move the goods and do the operation there or we can run some of the systems in other ways. We can put manual processes into action. Even though some of them don't work, they require a lot of labor. In other words, they require a lot of effort. But we have things that we have backed up during these 3 weeks. For example, we have a separate storage in Ankara. We have plans like that where we keep our backups there, we can switch the operation there." (3PL9)</i>
loss of operational data, logistics planning confusion, shipment tracking failure, container tracking failures, software integration issues, order fulfillment failure, transportation planning issues, warehouse management failures	Use of Cloud	<i>"So of course these are the most important issues for us. For example, we already have contracts with our technological partners about this, we include this in the contracts. We are currently using a cloud-based system. They are already a company that has defense systems against DDOS attacks. We choose from these and work with them. On the other hand, as I said, this is because we work with SAP. Let me put it this way, none of our servers are kept in our own buildings. We always use cloud servers, and their backups are kept in different locations. Well, we also approach this issue from a contractual perspective. That's why cybersecurity is a concept that is at the forefront for us." (3PL7)</i>

5.4.7. Reputational Mitigation Strategies

In this section, two main strategies to reduce reputational impact as a result of cyberattacks are backup with the cloud and disaster recovery plans. These strategies are designed to limit the amount of disruption to normal operations and reduce

customer dissatisfaction as these are the two main causes of reputational damage due to cyber events.

Utilizing cloud-based backup systems essentially creates opportunities for business continuity in the event of a cyberattack, as immediate recovery is vital. Cloud technologies allow for a real-time data backup to be coordinated simultaneously with remote, risk mitigated, storage of the operational data. In the event of a total data loss, the operational interruption for a company can be detrimental to business continuance, with the degree of operational loss affecting the business's ability to continue operations. With respect to reputational aspects, recovery time to service impacts on customer relationships is a major determinant of overall customer retention, as businesses that are able to quickly return to providing services and avoid extensive time delays or data loss are better able to maintain the confidence, trust and loyalty of its customers. Excerpts from the interviews concluded that the long-term interruption of services due to being a victim of a cyberattack creates discontent at a consumer level to the extent of permanent brand damage and loss in operational relationships should the claim held by the end-user to compensation based on lost business be lost. Therefore, in addition to providing a technical safeguard on the company's data, cloud-based backup systems act as a preventative mechanism for the company to retain its public image in times of crisis.

Creating and implementing comprehensive disaster recovery plans serve as an important tactic for minimizing reputational consequences. An effective disaster recovery plan reflects an organization's ability to respond to attacks in a consistent and timely manner to reduce service failures and downtime. Companies that are perceived to handle incidents in a forthright manner and displayed rapid recovery from issues earn customer and partner perceptions of greater reliability and resilience. The results indicated that without an effective recovery plan, companies not only had immediate service-related complaints, but also continued reputational harm in the form of reduced customer loyalty and erosion of trust across the supply chain. Accordingly, disaster recovery planning is critical to achieve the management of the downstream effects of cyberattacks on corporate reputation. Table 46 below provides mitigation strategies and illustrative quotes to mitigate reputational ripple effects.

Table 46. Mitigation Strategies and Illustrative Quotes to Mitigate Reputational Ripple Effects.

Ripple Effects	Mitigation Strategy	Quote
Brand Damage, Customer Dissatisfaction, Loss of Customers, Loss of Reputation, Loss of Trust, Relationship Dissolution	Backup With the Cloud, Disaster Recovery Plans	<i>"After an attack, fully recovering systems is a time-consuming and complex process. Backup and recovery plans must be put in place effectively. However, during this process, complete recovery of data may result in some data loss. It may take time to re-secure systems and return business processes to normal, negatively affecting customer satisfaction and business continuity. In addition, a comprehensive security review must be conducted to determine the source of the attack and prevent the same vulnerability from being used again." (3PL2)</i>

CHAPTER 6: CONCLUSION

This study provides a comprehensive review of the multifaceted impacts of cyberattacks centered on 3PL providers on supply chain stakeholders and introduces detailed cybersecurity strategies tailored to mitigate these cyberattacks and their impacts through analysis of interviews conducted with industry experts. Addressing two RQs, we investigate both the ripple effects created by cyberattacks throughout the supply chain and the proactive strategies required to mitigate these disruptions and increase overall resilience.

The findings from RQ1 reveals that the impacts of cyberattacks span across employee, financial, information security, legal, operational, reputational, industrial, information sharing, and societal domains. Among all stakeholders, 3PL firms, as the primary targets of cyberattacks, experience the most severe consequences, followed by importers and exporters who face significant ripple effects. Although other stakeholders, such as ports, customs firms, shipowners, and retailers, are also impacted, their level of exposure is relatively lower. These outcomes align with prior studies that emphasize the increasing centrality of 3PLs in cyber risk exposure (Perez-Moron, 2020). Our analysis reveals that the impact of such an attack on each stakeholder can differ in nature and vary in severity. Furthermore, we provide a new perspective by demonstrating that a cyberattack on a 3PL firm leads to distinct immediate and long-term effects on each stakeholder within the supply chain, a perspective that has not been explored before. Besides, Gkanatsas and Kirikke (2020) noted that the risks within the supply chain are increasingly shifting toward 3PL companies, yet they highlighted the lack of specific research on 3PLs. While there is a wealth of literature on cybersecurity within the supply chain, studies focusing on the role of 3PLs are limited, and the detailed impacts on these firms have not been thoroughly explored (Cheung, Bell, and Bhattacharjya, 2023). This study specifically examined the central role of 3PL firms in supply chain cyberattacks.

Meggiato et al., (2022) underscores the importance of strengthening cybersecurity measures within 3PL companies to ensure the resilience of the entire supply chain. By securing these measures, the ripple effects on all stakeholders can be prevented and mitigated, ultimately enhancing the overall stability of the supply chain. Therefore, in our second RQ, we identify effective mitigation strategies that will help reduce cyberattacks and prevent potential ripple effects.

First of all, the applications, practices and strategies in the literature are largely technology-oriented strategies. In the literature, big data, cloud computing, IoT sensors and blockchain-based systems and strategies have been proposed (Ugochukwu, Goyal and Arumugam, 2022; Enache, 2023). However, a study similar to our findings was implemented by Odimarha, Ayodeji and Abaku (2024). The researchers examined cybersecurity measures in logistics under the titles of Employee Training and Awareness, Network Security, Data Protection, Incident Response Plan, Compliance and Regulations, Continuous Monitoring and Threat Intelligence, Technology Updates and Patch Management, and these strategies are parallel to our analysis results, but our results are not limited to these 8 strategies, but are revealed under the titles of employee-related strategies, operational strategies, reputational strategies, legal strategies, information security strategies, information sharing strategies and industrial strategies on a broader scale. Our findings have contributed to the literature by revealing 9 strategies in the employee related strategies category, 7 strategies in the operational strategies category, 15 strategies in the information sharing strategies category, 17 strategies in the information security strategies category, 11 strategies in the industrial strategies category, 3 strategies in the legal strategies category, and 2 strategies in the reputational strategies category. This has not been presented in the literature before. In addition, the need to investigate the design of a flexible backbone network that combines information sharing strategies among supply chain partners is also emphasized by Cheung, Bell and Bhattacharjya (2023). The strategies we present under the title of information sharing strategies also fill this gap in the literature.

6.1. Academic and Practical Implications

Our study contributes to the academic literature on supply chain cybersecurity by providing comprehensive insights into the ripple effects of cyberattacks on 3PL providers and effective mitigation strategies for them. Previous studies have highlighted the importance of the topic (Cheung et al., 2021; Gkanatsas and Krikke, 2020), but the ripple effects from 3PL-centered cyber incidents and their impacts on a wide range of stakeholders have not been previously examined. This research addresses this gap by mapping both multidimensional outcomes and response strategies within a holistic framework.

Theoretically, the study enhances the application of systems theory in cybersecurity by showing how a disruption at one node particularly a 3PL firm can

propagate through the entire supply chain, affecting not only immediate partners such as importers and exporters but also downstream actors including customs brokers, manufacturers, port operators, and even retailers. Our findings primarily contribute to the literature by revealing the short- and long-term effects of these attacks. In the short run, operations can be disrupted, business-critical data can be compromised, and communications can be impeded. In the longer run, the damage can be even greater, with potential losses including customer distrust, strained business relations, high financial losses, large-scale organisational restructuring, damage in terms of reputation, reduced sales, greater exposure in terms of future attack, raised operational expenses, and recurring difficulties in rebuilding confidence. First, on the worker's side, attacks heighten anxiety as a result of intense crisis management, unpredictability, and increased workload. Eventually, there could be layoffs as businesses suffer financially. Financial losses in the short run arise due to lost business opportunities, penalty charges, and increased operational expenses. In the long run, bankruptcies, plant shutdowns, and damage to reputation make recovery even more challenging. In the context of information security, short-term consequences include disclosure of sensitive material like customer details, pricing plans, suppliers' details, trade reports, and delivery details. Direct threats consist of financial data leaks, theft of business secrets, and invasion of personal details, all of which compromise company integrity and security. In the long run, the violation leads to a perpetual risk of cybersecurity attacks and permanent disclosure of proprietary material and business secrets. Leaks of this nature can gain competitors an unfair advantage and result in permanent damage to reputation. Moreover, leakage of strategic material can shift the dynamics of the business and create new security challenges. In terms of legal implications, professionals in the industry tend not to consider short-term legal ramifications. In the long run, businesses are subject to legal penalties due to violations of privacy of the data, contractual violations, and nonconformances to regulations. Operationally, short-term impacts are manifested in delays, bottlenecks, tracking errors in containers, and worldwide logistics congestion. Firms face issues in performance of their services, routing inefficiencies, and errors in fulfilments, all leading to major operational delays. In the long run, operational failures have the potential to spiral into large-scale business interruptions, plant shutdowns, and supply chain failures. Firms are faced with shortages of resources, production stoppages, and financial operational breakdowns. Reputationally, security incidents and failure of

service erode customer trust. In the long run, businesses lose their main clients and have difficulty in recapturing market share. Order cancellations and increased shipping fees disrupt market stability industrially. Long-term impacts involve higher production of counterfeits and unfair business practices. In terms of information sharing, cyberattacks result in real-time communication interruptions, integration issues, and the compromise of sensitive data. Stakeholders are presented with collaboration challenges, impeding efficient coordination of restoration responses. If the vulnerabilities continue, short-term challenges could be longer lasting. Lastly, on the societal front, attacks result in shortages of essential commodities such as food and medicine. While long-term consequences are unknown, long-term interruptions have the potential of exacerbating economic instability. Moreover, our findings contribute to the literature by examining the impacts in detail on a stakeholder basis. In summary, it has been observed that 3PL service providers, as the primary target, experience all the impact categories we have presented in the findings section. Importers and exporters face almost all impacts except legal issues. Ports face legal consequences due to their role in taxation, but they are not affected by industrial competition. When we look at operational and financial disruptions, they are widespread across all stakeholders and affect all stakeholders. Customs agents who process trade secrets and documents are the most affected by information security breaches, but they do not suffer reputational damage either. Ship owners primarily face financial, operational and reputational challenges, while retailers are less affected by information security and sharing issues. Finally, industrial impacts are seen to be important for importers, exporters and 3PL firms due to intense market competition.

From a taxonomy perspective, the research adds by classifying cyberattack effects into nine separate domains employee, financial, information security, legal, operational, reputational, industrial, information sharing and societal with stakeholder-specific weaknesses and implications. This narrowed-down categorization provides a formal foundation for future empirical researches to embrace or develop.

Another academic contribution of the study is the development of a seven-dimensional strategic framework for cyber resilience in supply chains. Another academic contribution of the study is the development of a seven-category strategic framework that will reduce cyberattacks and their possible consequences in logistics operations and supply chains to provide cyber resilience. First of all, when we look at

employee-related strategies, we come across important strategies such as audit of employee training, creating a system for generating security tickets for employees, employee training, restrictions to personal applications, implementing incentive programs for employees. The most important of our industrial strategies are listed as collaborative IT team for the entire supply chain, common security standard implementation for the industry, creating incident response teams for the entire chain, cybersecurity status sharing among stakeholders, undergoing a unified audit for the entire chain, utilizing a unified software across the entire supply chain. For the information security category, some of the strategies we have come up with are backup in cloud and different locations, creating an effective network infrastructure, data encryption and monitoring, mandatory establishment of a cybersecurity and in-house software departments for companies, stakeholder audit. Some of the most important strategies we recommend for information sharing, which is another category, are stakeholder audit, implementation of a single shared network and systems for the entire chain, information-sharing software covering the entire chain, integration team implementation, investment and integration incentive practices for stakeholders, use of cloud for data sharing, use of EDI. When we look at legal strategies, we were able to come up with 3 strategies. These consist of complying with legal requirements, government-mandated cybersecurity rules and intervention practices, and security contracts. We list the most important of our operational strategies as backup in cloud and different locations, establishing a crisis management team, disaster recovery plans, and keeping backup software. Finally, we were able to come up with 2 strategies that will mitigate reputational impacts. These strategies were recommended by industry experts as backup with the cloud and disaster recovery plans. The majority of these strategies are directly based on real-world applications derived from semi-structured interviews with practitioners and therefore offer high contextual validity.

The practical implications of this study provide important insights for supply chain managers, cybersecurity officers, and logistics managers. Based on our findings, we recommend the following to supply chain managers:

First of all, awareness and budget allocation. The experts who participated in our interview stated that although we are in the age of technology, many companies do not understand the seriousness of the issue and do not see it as a subject worth allocating budget for. The most targeted and affected 3PL companies should first gain

awareness and allocate a budget for security investments for cybersecurity. Allocating a budget for the use of security software and applications, which is one of our strategies, will be key. Since the strategy includes adaptations such as antivirus, correct firewall, SFTP, VPN, AI tools, IDS, patch management, 802.1xNAC, allocating a budget for these will provide significant protection.

Moreover, we stated that such a cyberattack spreads throughout the entire chain in a wave. In this case, sector managers should also focus on stakeholders; protecting themselves alone may not be enough to prevent threats from stakeholders. Therefore, implementing applications such as assessment practices, evaluation criteria, mandatory security certification requests, stakeholder audits, and integration investments for stakeholders in stakeholder selection will create a safer environment for the entire chain.

Moreover, we mentioned operational effects. In order to prevent the vast majority of these effects, the sector has recommended backup and cloud solutions to experts. These applications need to be adapted to all companies, big or small. In the event of any interruption, these applications largely ensure operational continuity.

In addition, we recommend that the sector implement training and audits for in-house employees, and create an in-house cybersecurity department and software development department. Since attacks are generally carried out on employees, implementing such strategies on employees will reduce the possibility of attacks, and the established departments will take rapid action against incidents, prevent them from spreading, and minimize possible data loss.

Finally, we recommend that common systems, common integration, common network, and a common security team should be established for supply chains, thus external threats will be largely disabled and a safer commercial environment will be provided.

6.2. Limitations and Further Research

Although our study provides valuable contributions in academic and practical terms, there are some limitations. First, the study utilizes a qualitative approach founded on semi-structured interviews that, although facilitating in-depth analysis, restrict the external validity of findings. A quantitative survey or experimental approaches would enable future studies to test the frequency and efficacy of the

recognized strategies in larger populations or amongst different geographical locations. Second, the sample comes solely from Turkey, İzmir. Inasmuch as cybersecurity maturity, local regulation environments, as well as organizational structures and cultures differ considerably between countries, future studies must incorporate multiple regions in a comparative study to determine the universality or specificity of the results. In addition, we were able to include 2 participants from port and customs companies in our sample. The number of these actors can be increased or new actors can be included in the sample. Third, the current study deals primarily with the perception and experience of organizational actors; the study does not examine technical performance measures or the real-world incident response impact. Future studies might develop longitudinal case studies of incidents or use attack simulations to quantitatively estimate the efficacy of the strategies. We recommend that future research examine the subject more broadly, taking these limitations into account.

REFERENCES

- Ackoff, R. (1981) *Creating the corporate future*, 1st Edition, Wiley, New York.
- Adeoye-Olatunde, O.A. and Olenik, N.L. (2021) Research and scholarly methods: Semi-structured interviews, *JACCP Journal of the American College of Clinical Pharmacy*, Vol. 4(10), pp. 1358–1367.
- Afenyo, M. and Caesar, L.D. (2023) Maritime cybersecurity threats: Gaps and directions for future research, *Ocean & Coastal Management*, Vol. 236, 106493.
- Ahola, M. (2021) The role of human error in successful cybersecurity breaches, *Usecure*.
- Alkadi, O., Moustafa, N. and Turnbull, B. (2020) A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions, *IEEE Access*.
- Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021) Phishing attacks: A recent comprehensive study and a new anatomy, *Frontiers in Computer Science*, Vol. 3, 563060.
- Alkhatib, S.F., Darlington, R. and Nguyen, T.T. (2015) Logistics service providers (LSPs) evaluation and selection: Literature review and framework development, *Strategic Outsourcing: An International Journal*, Vol. 8(1), pp. 102–134.
- Amin, S., Schwartz, G.A. and Sastry, S.S. (2013) Security of interdependent and identical networked control systems, *Automatica*, Vol. 49(1), pp. 186–192.
- Anderson, R. and Moore, T. (2006) The economics of information security, *Science*, Vol. 314(5799), pp. 610–613.
- Andrés, B. and Poler, R. (2015) Dealing with the alignment of strategies within the collaborative networked partners, available at: https://link.springer.com/content/pdf/10.1007/978-3-319-16766-4_2.pdf
- Ashton, K. (2009) That ‘internet of things’ thing, *RFID Journal*, Vol. 22, pp. 97–114.
- Bechtsis, D., Tsolakis, N., Iakovou, E. and Vlachos, D. (2022) Data-driven secure, resilient and sustainable supply chains: Gaps, opportunities, and a new generalised data sharing and data monetisation framework, *International Journal of Production Research*, Vol. 60(14), pp. 4397–4417.
- Berr, J. (2017) WannaCry ransomware attack losses could reach \$4 billion, Technical Report, May 2017.

- Bertalanffy, L. (1951) General systems theory: A new approach to unity of science, *Human Biology*, Vol. 3, pp. 23–29.
- Bertalanffy, L. (1956) General systems theory, *General Systems: Yearbook of the Society for the Advancement of General Systems Research*, Vol. 1, pp. 1–10.
- Bloomberg. (2017) FedEx cuts profit forecast on \$300 million hit from cyberattack, *Bloomberg.com*. (Accessed: 16 April 2024).
- Boiko, A., Shendryk, V. and Boiko, O. (2019) Information systems for supply chain management: Uncertainties, risks and cyber security, *Procedia Computer Science*, Vol. 149, pp. 65–70.
- Boone, A. (2017) Cyber-security must be a C-suite priority, *Computer Fraud & Security*, Vol. 2017(2), pp. 13–15.
- Boyson, S. (2014) Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems, *Technovation*, Vol. 34(7), pp. 342–353.
- Burkhardt, M.E. and Brass, D.J. (1990) Changing patterns or patterns of change: The effects of a change in technology on social network structure and power, *Administrative Science Quarterly*, Vol. 35, pp. 104–127.
- Burkhead, R.L. (2014) A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management (Order No. 3682325), *ProQuest Dissertations & Theses Global*.
- Caddy, I.N. and Helou, M.M. (2007) Supply chains and their management: Application of general systems theory, *Journal of Retailing and Consumer Services*, Vol. 14(5), pp. 319–327.
- Calza, F. and Passaro, R. (1997) EDI network and logistics management at Unilever-Sagit, *Supply Chain Management: An International Journal*, Vol. 2(4), pp. 158–170.
- Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., and Walker, K. (2020) Purposive sampling: Complex or simple, *Research case examples. Journal of research in Nursing*, 25(8), 652–661.
- Cavanagh, S. (1997) Content analysis: Concepts, methods and applications, *Nurse Researcher*, Vol. 4, pp. 5–16.
- Chang, J.A., Katehakis, M.N., Shi, J.J. and Yan, Z. (2021) Blockchain-empowered newsvendor optimization, *International Journal of Production Economics*, Vol. 238, 108144.

- Charles, V., Emrouznejad, A. and Gherman, T. (2023) A critical analysis of the integration of blockchain and artificial intelligence for supply chain, *Annals of Operations Research*, Vol. 327(1), pp. 7–47.
- Checkland, P. (1981) *Systems thinking, systems practice*, 1st Edition, John Wiley & Sons, New York.
- Cheung, K.F. and 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*, Vol. 291(2), 471–481.
- Cheung, K.F., Bell, M.G. and Bhattacharjya, J. (2021) Cybersecurity in logistics and supply chain management: An overview and future research directions, *Transportation Research Part E: Logistics and Transportation Review*, Vol. 146, 102217.
- Choi, T.M., Kumar, S., Yue, X. and Chan, H.L. (2022) Disruptive technologies and operations management in the Industry 4.0 era and beyond, *Production and Operations Management*, Vol. 31(1), pp. 9–31.
- Chow, D. and Heaver, T. (1999) *Logistics strategies for North America* (3rd ed.), *Global Logistics and Distribution Planning*.
- Choy, K.L., Chow, H.K., Tan, K.H., Chan, C.K., Mok, E.C. and Wang, Q. (2008) Leveraging the supply chain flexibility of third party logistics – Hybrid knowledge-based system approach, *Expert Systems with Applications*, Vol. 35(4), pp. 1998–2016.
- Chukwu, N., Yufenyuy, S., Ejiofor, E., Ekweli, D., Ogunleye, O., Clement, T., Obunadike, C., Adeniji, S., Elom, E., and Obunadike, C. (2024) Resilient chain: AI-enhanced supply chain security and efficiency integration, *International Journal of Scientific and Management Research*, Vol. 7(03), pp. 46–65.
- Cisco. (2021) Cyber security threat trends, available at: <https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-cryptotop-the-list>. (Accessed: 12 March 2024).
- Cleary, G., Corpin, M., Cox, O., Lau, H., Nahorney, B., O'Brien, D., O'Gorman, B., Power, J.P., Wallace, S., Wood, P. and Wuest, C. (2018) *Internet Security Threat Report (ISTR)*, Technical Report.
- Clement, T., Obunadike, C., Ekweli, D., Ejiofor, O., Ogunleye, O., Yufenyuy, S., Nnaji, C. and Obunadike, C. (2024) Cyber analytics: Modelling the factors behind healthcare data breaches for smarter security solutions, *International Journal of*

Advance Research, Ideas and Innovations in Technology, Vol. 10(1). Available at: www.IJARIIT.com

Cole, F.L. (1988) Content analysis: Process and application, *Clinical Nurse Specialist*, Vol. 2(1), pp. 53–57.

Colicchia, C., Creazza, A. and Menachof, D.A. (2019) Managing cyber and information risks in supply chains: Insights from an exploratory analysis, *Supply Chain Management: An International Journal*, Vol. 24(2), pp. 215–240.

Collins, D., Dennehy, K., Conboy, K. and Mikalef, P. (2021) Artificial intelligence in information systems research: A systematic literature review and research agenda, *International Journal of Information Management*, Vol. 60, 102383.

Conklin, A. and Bronk, C. (2018) Enhancing a SCRM curriculum with cybersecurity, *International Journal of Systems and Software Security and Protection (IJSSSP)*, Vol. 9(2), pp. 46–56.

Craighead, C., Blackhurst, J., Rungtusanatham, J. and Handfield, R. (2007) The severity of supply chain disruptions design characteristics and mitigation capabilities, *Decision Sciences*, Vol. 38(1), pp. 131–156.

Creazza, A., Colicchia, C., Spiezia, S. and Dallari, F. (2022) Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era, *Supply Chain Management: An International Journal*, Vol. 27(1), pp. 30–53.

Crosignani, M., Macchiavelli, M. and Silva, A.F. (2023) Pirates without borders: The propagation of cyberattacks through firms' supply chains, *Journal of Financial Economics*, Vol. 147(2), pp. 432–448.

CyberEdge Group. (2021) 2021 cyberthreat defense report, *Technical Report*, 66 pages.

da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R. and de Albuquerque, V.H.C. (2019) Internet of Things: A survey on machine learning-based intrusion detection approaches, *Computer Networks*, Vol. 151, pp. 147–157.

da Cruz, M.A.A., Rodrigues, J.J.P.C., Al-Muhtadi, J., Korotaev, V.V. and de Albuquerque, V.H.C. (2018) A reference model for Internet of Things middleware, *IEEE Internet of Things Journal*, Vol. 5(2), pp. 871–883.

da Silva, R.M., Frederico, G.F. and Garza-Reyes, J.A. (2023) Logistics service providers and industry 4.0: A systematic literature review, *Logistics*, Vol. 7(1), 11.

- Deane, J.K., Ragsdale, C.T., Rakes, T.R. and Rees, L.P. (2009) Managing supply chain risk and disruption from IT security incidents, *Operations Management Research*, Vol. 2(1–4), pp. 4–12.
- Deeter-Schmelz, D. (1997) Applying teams to logistics processes: Information acquisition and the impact of team role clarity and norms, *Journal of Business Logistics*, Vol. 18(1), pp. 159–178.
- Deyannis, D., Papadogiannaki, E., Chrysos, G., Georgopoulos, K. and Ioannidis, S. (2022) The diversification and enhancement of an IDS scheme for the cybersecurity needs of modern supply chains, *Electronics*, Vol. 11(13), 1944.
- Dhillon, G. and Backhouse, J. (1996) Risks in the use of information technology within organizations, *International Journal of Information Management*, Vol. 16(1), pp. 65–74.
- Djatsa, F. (2019) Examining the relationship between millennial professionals' perceptions of cybersecurity risks and users' online security behaviors (Order No. 22623854), *ProQuest Dissertations & Theses Global*.
- Dubey, R., Gunasekaran, A., Childe, S.J., Fosso Wamba, S., Roubaud, D. & Foropon, C. (2021) Empirical investigation of data analytics capability and organizational flexibility as complements to supply chain resilience, *International Journal of Production Research*, Vol. 59(1), pp. 110–128.
- Dutta, P., Choi, T.M., Somani, S. and Butala, R. (2020) Blockchain technology in supply chain operations: Applications, challenges and research opportunities, *Transportation Research Part E: Logistics and Transportation Review*, Vol. 142, 102067.
- Eisenhardt, K.M., 1989. Building theories from case study research. *Academy of Management Review*, 14(4), pp.532–550. <https://doi.org/10.5465/amr.1989.4308385>.
- Elluru, S., Gupta, H., Kaur, H. and Singh, S.P. (2019) Proactive and reactive models for disaster resilient supply chain, *Annals of Operations Research*, Vol. 283(1–2), pp. 199–224.
- Elo, S. and Kyngäs, H. (2008) The qualitative content analysis process, *Journal of Advanced Nursing*, Vol. 62(1), pp. 107–115.
- Enache, G.I. (2023) Logistics security in the era of big data, cloud computing and IoT, *Proceedings of the International Conference on Business Excellence*, Vol. 17(1), pp. 188–199.

- ENISA. (2020) Insider threat, *ENISA Threat Landscape*, Technical Report, European Union Agency for Cybersecurity (ENISA), 18 pages.
- Ferdous, J., Islam, R., Mahboubi, A. and Islam, M.Z. (2023) A review of state-of-the-art malware attack trends and defense mechanisms, *IEEE Access*, Vol. 11, pp. 121118–121141.
- Fernández-Caramés, T., Blanco-Novoa, O., Suárez-Albela, M. and Fraga-Lamas, P. (2018) A UAV and blockchain-based system for Industry 4.0 inventory and traceability applications, *Proceedings*, Vol. 4, 26.
- Flick, U. (2014) *An introduction to qualitative research* (5th ed.), Sage, London, UK.
- Forman, J. and Damschroder, L. (2007) Qualitative content analysis, in *Empirical Methods for Bioethics: A Primer*, Emerald Group Publishing Limited, Vol. 11, pp. 39–62.
- Frankel, R., Bolumole, Y., Eltantawy, R., Paulraj, A. and Gundlach, G. (2008) The domain and scope of SCM's foundation disciplines—insights and issues to advance research, *Journal of Business Logistics*, Vol. 29(1), pp. 1–30.
- Gafni, R. and Levy, Y., 2023. Experts' feedback on the cybersecurity footprint elements: in pursuit of a quantifiable measure of SMBs' cybersecurity posture. *Information & Computer Security*, 31(5), pp.601–623.
- Galletta, A. & Cross, W.E., 2013. Mastering the semi-structured interview and beyond: From research design to analysis and publication. 1st ed. New York: NYU Press.
- Germain, R. and Droge, C. (1998) The context, organizational design, and performance of JIT buying versus non-JIT buying firms, *International Journal of Purchasing and Materials Management*, Vol. 34(2), pp. 12–18.
- Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R. (2020) Managing cyber risk in supply chains: A review and research agenda, *Supply Chain Management: An International Journal*, Vol. 25(2), pp. 223–240.
- Gibbs, L., Kealy, M., Willis, K., Green, J., Welch, N. and Daly, J. (2007) What have sampling and data collection got to do with good qualitative research? *Australian and New Zealand Journal of Public Health*, Vol. 31(6), pp. 540–544.
- Gkanatsas, E. and Krikke, H. (2020) Towards a pro-silience framework: A literature review on quantitative modelling of resilient 3PL supply chain network designs, *Sustainability*, Vol. 12(10), 4323.

- Gugiu, P.C. and Rodríguez-Campos, L. (2007) Semi-structured interview protocol for constructing logic models, *Evaluation and Program Planning*, Vol. 30(4), pp. 339–350.
- Hammi, B., Zeadally, S. and Khatoun, R. (2019) An empirical investigation of botnet as a service for cyberattacks, *Transactions on Emerging Telecommunications Technologies*, Vol. 30(3), e3537.
- Hammi, B., Zeadally, S. and Nebhen, J. (2023) Security threats, countermeasures, and challenges of digital supply chains, *ACM Computing Surveys*, Vol. 55(14s), pp. 1–40.
- Hardon, A., Hodgkin, C. and Fresle, D. (2004) *How to investigate the use of medicines by consumers*, World Health Organization and University of Amsterdam, retrieved from <http://apps.who.int/medicinedocs/en/d/Js6169e/>.
- Hassan, M.M.D. (2006) Engineering supply chains as systems, *System Engineering*, Vol. 9(1), pp. 73–89.
- Hassija, V., Chamola, V., Gupta, V., Jain, S. and Guizani, N. (2020) A survey on supply chain security: Application areas, security threats, and solution architectures, *IEEE Internet of Things Journal*, Vol. 8(8), pp. 6222–6246.
- Heizer, J., Render, B. and Munson, C. (2017) *Principles of Operations Management: Sustainability and Supply Chain Management* (Global ed.), Pearson.
- Hsiao, H.I., Kemp, R.G.M., Van der Vorst, J.G.A.J. and Omta, S.O. (2010) A classification of logistic outsourcing levels and their impact on service performance: Evidence from the food processing industry, *International Journal of Production Economics*, Vol. 124, pp. 75–86.
- Hsieh, H.F. and Shannon, S.E. (2005) Three approaches to qualitative content analysis, *Qualitative Health Research*, Vol. 15(9), pp. 1277–1288.
- Huang, C.D., Hu, Q. and Behara, R.S. (2008) An economic analysis of the optimal information security investment in the case of a risk-averse firm, *International Journal of Production Economics*, Vol. 114(2), pp. 793–804.
- Hyman, H.H., Cobb, W.J., Feldman, J.J., Hart, C.W. and Stember, C.H. (1954) *Interviewing in social research*, University of Chicago Press, Chicago.
- IT Revolution, Sonatype, Muse Dev. (2020) *2020 State of the Software Supply Chain*, Technical Report, 44 pages.
- ITU. (2009) Overview of cybersecurity, *Recommendation ITU-T X.1205*, Geneva: International Telecommunication Union (ITU), available at: <http://www.itu.int/rec/T-REC-X.1205-200804-I/en>. (Accessed: 10 April 2024).

- Ivanov, D., Dolgui, A. and Sokolov, B. (2019) The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics, *International Journal of Production Research*, Vol. 57(3), pp. 829–846.
- Karrapan, C., Sishange, M., Swanepoel, E. and Kilbourn, P.J. (2017) Benchmarking criteria for evaluating third-party logistics providers in South Africa, *Journal of Transport and Supply Chain Management*, Vol. 11(1), pp. 1–10.
- Katz, D. and Kahn, R. (1978) *The social psychology of organizations*, 1st Edition, John Wiley, New York.
- Kelly, S.E. (2010) Qualitative interviewing techniques and styles, in Bourgeault, I., Dingwall, R. & De Vries, R. (Eds.), *The SAGE Handbook of Qualitative Methods in Health Research*, 1st Edition, SAGE, London, pp. 307–327.
- Keskin, O.F., Caramancion, K.M., Tatar, I., Raza, O. and Tatar, U. (2021) Cyber third-party risk management: A comparison of non-intrusive risk scoring reports, *Electronics*, Vol. 10(10), 1168.
- Kleindorfer, P. and Saad, G. (2005) Managing disruption risk in supply chains, *Production and Operations Management*, Vol. 14(1), pp. 53–68.
- Klockner, M., Schmidt, C.G. and Wagner, S.M. (2022) When blockchain creates shareholder value: Empirical evidence from international firm announcements, *Production and Operations Management*, Vol. 31(1), pp. 46–64.
- Krippendorff, K. (1980) *Content analysis: An introduction to its methodology*, 4th Edition, Sage Publications, Newbury Park.
- Krippendorff, K. (2018) *Content analysis: An introduction to its methodology*, 4th Edition, Sage Publications.
- Kshetri, N. (2017) Can blockchain strengthen the internet of things? *IT Professional*, Vol. 19, pp. 68–72.
- Kshetri, N. (2022) Economics of supply chain cyberattacks, *IT Professional*, Vol. 24(3), pp. 96–100.
- Kumar, S. and Mallipeddi, R.R. (2022) Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions, *Production and Operations Management*, Vol. 31(12), pp. 4488–4500.
- Kunnathur, A. (2015) Information security in supply chains: A management control perspective, *Information and Computer Security*, Vol. 23(5), pp. 476–496.
- Kunreuther, H. and Heal, G. (2003) Interdependent security, *Journal of Risk and Uncertainty*, Vol. 26(2–3), pp. 231–249.

- Kyngäs, H. and Vanhanen, L. (1999) Content analysis (Finnish), *Hoitotiede*, Vol. 11, pp. 3–12.
- Latif, M.N.A., Aziz, N.A.A., Hussin, N.S.N. and Aziz, Z.A. (2021) Cyber security in supply chain management: A systematic review, *LogForum*, Vol. 17(1), pp. 49–57.
- Lauri, S. and Kyngäs, H. (2005) *Developing nursing theories (Finnish: Hoitotieteen Teorian Kehittäminen)*, Werner Söderström, Dark Oy, Vantaa.
- Lees, M.J., Crawford, M. and Jansen, C. (2018) Towards industrial cybersecurity resilience of multinational corporations, *IFAC-PapersOnLine*, Vol. 51(30), pp. 756–761.
- Lennane, A. (2020) Toll Group resists ransom demands from hackers after cyber attack, *The Loadstar*, 12 May, retrieved from <https://theloadstar.com/toll-groupresists-ransom-demands-from-hackers-after-cyber-attack/>. (Accessed: 17 June 2024).
- Levy, Y. and Gafni, R. (2021) Introducing the concept of cybersecurity footprint, *Information and Computer Security*, Vol. 29(5), pp. 724–736.
- Li, Y. and Xu, L. (2021) Cybersecurity investments in a two-echelon supply chain with third-party risk propagation, *International Journal of Production Research*, Vol. 59(4), pp. 1216–1238.
- Li, Y., Xu, X., Zhao, X., Yeung, J.H.Y. and Ye, F. (2012) Supply chain coordination with controllable lead time and asymmetric information, *European Journal of Operational Research*, Vol. 217, pp. 108–119.
- Liu, Z., Wang, Q. and Tang, Y. (2020) Design of a co-simulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems.
- Lu, G., Koufteros, X., Talluri, S. and Hult, G.T.M. (2019) Deployment of supply chain security practices: Antecedents and consequences, *Decision Sciences*, Vol. 50(3), pp. 459–497.
- Luo, S. and Choi, T.M. (2022) E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Production and Operations Management*, Vol. 31(5), pp. 2107–2126.
- Maersk (2020) A view from the other side of a crisis, *Maersk*, retrieved from https://www.maersk.com/~media_sc9/maersk/stay-ahead/maersk—a-view-from-theother-side-of-a-crisis—final.pdf. (Accessed: 15 April 2024).
- Magaldi, D. and Berler, M. (2020) Semi-structured interviews, in Zeigler-Hill, V. & Shackelford, T.K. (Eds.), *Encyclopedia of Personality and Individual Differences*, Springer, Cham.

- Mangla, S.K., Kazancoglu, Y., Ekinci, E., Liu, M., Ozbiltekin, M. and Sezer, M.D. (2021) Using system dynamics to analyze the societal impacts of blockchain technology in milk supply chains, *Transportation Research Part E: Logistics and Transportation Review*, Vol. 149, 102289.
- Manuj, I. and Mentzer, J. (2008) Global supply chain risk management strategies, *International Journal of Physical Distribution and Logistics Management*, Vol. 38(3), pp. 192–223.
- Martínez, M.M., Marin-Tordera, E. and Masip-Bruin, X. (2021) Scalability analysis of a blockchain-based security strategy for complex IoT systems, in *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, IEEE, pp. 1–6.
- Meggiato, G., Nterai, S., Skowronski, E., Gao, R., Atiqur, M. and Sorooshian, S. (n.d.) Warehouses against cyber-attack risks.
- Melnyk, S.A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J.F. and Friday, D. (2022) New challenges in supply chain management: Cybersecurity across the supply chain, *International Journal of Production Research*, Vol. 60(1), pp. 162–183.
- Min, H. (2019) Blockchain technology for enhancing supply chain resilience, *Business Horizons*, Vol. 62(1), pp. 35–45.
- Modi, S.B., Wiles, M.A. and Mishra, S. (2015) Shareholder value implications of service failures in triads: The case of customer information security breaches, *Journal of Operations Management*, Vol. 35, pp. 21–39.
- Mohurle, S. and Patil, M. (2017) A brief study of WannaCry threat: Ransomware attack 2017, *International Journal of Advanced Research in Computer Science*, Vol. 8.
- Momoh, O. (2016) Supply chain attack. Available at: www.investopedia.com/terms/s/supply-chain-attack.asp. (Accessed: 10 March 2024).
- Morgan, S. (2019) Global ransomware damage costs predicted to reach \$20 billion (USD) by 2021, *Cybersecurity Ventures*, October. Technical Report.
- Moshood, T.D., Nawanir, G., Sorooshian, S. and Okfalisa, O. (2021) Digital twins driven supply chain visibility within logistics: A new paradigm for future logistics, *Applied System Innovation*, Vol. 4(2).
- Mutek, M.W. and Irwin, A.D. (2018) Focus on supply chain risk management, *Contract Management*, Vol. 58(11), pp. 26–37.

- Narwane, V.S., Raut, R.D., Mangla, S.K., Dora, M. and Narkhede, B.E. (2023) Risks to big data analytics and blockchain technology adoption in supply chains, *Annals of Operations Research*, Vol. 327(1), pp. 339–374.
- New, S. and Westbrook, R. (2004) *Understanding supply chains: Concepts, critiques and futures*, 1st Edition, Oxford University Press, Oxford.
- Newman, L.H. (2021) A second SolarWinds hack deepens third-party software fears, *Wired*, 2 February 2021.
- Newman, L.H. (2021) The SolarWinds hackers used tactics other groups will copy, *Wired*, 19 January 2021.
- Niemann, W., Hall, G. and Oliver, K. (2017) South African 3PL firms' approaches to sustainable supply chain management, *Journal of Contemporary Management*, Vol. 14(1), pp. 204–237.
- Norman, D., Bhargava, N., Harmon, M., Wright, J., Springs, D. and Dawson, M. (2020) Supply chain and logistics management and an open door policy concerning cyber security introduction, *International Journal of Management*, Vol. 9(1), pp. 1–10.
- Nozari, H., Szmelter-Jarosz, A. and Ghahremani-Nahr, J. (2022) Analysis of the challenges of artificial intelligence of things (AIoT) for the smart supply chain (case study: FMCG industries), *Sensors*, Vol. 22(8), 2931.
- Nygård, A.R. and Katsikas, S. (2022) SoK: Combating threats in the digital supply chain, in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–8.
- O'Hara, G. (2010) Cyber-espionage: A growing threat to the American economy, *CommLaw Conspec.*, Vol. 19, pp. 241.
- Odimarha, A.C., Ayodeji, S.A. and Abaku, E.A. (2024) Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies, *World Journal of Advanced Science and Technology*, Vol. 5(1), pp. 026–030.
- Okonofua, H.I. (2018) The effects of information technology leadership and information security governance on information security risk management in USA organizations (Order No. 13426600), *ProQuest Dissertations & Theses Global*.
- Okoye, C.C., Ofodile, O.C., Tula, S.T., Nifise, A.O.A., Falaiye, T., Ejairu, E. and Addy, W.A. (2024) Risk management in international supply chains: A review with USA and African Cases, *Magna Scientia Advanced Research and Reviews*, Vol. 10(1), pp. 256–264.

- Park, J. and Park, J. (2017) Blockchain security in cloud computing: Use cases, challenges, and solutions, *Symmetry*, Vol. 9, 164.
- Parker Software (2021) The security risks of outdated software, *ParkerSoftware.com*. Available at: <https://www.parkersoftware.com>. (Accessed: 15 June 2024).
- Paul Trudgian Ltd. (2016) How security problems affect the supply chain. Available at: <https://www.paultrudgian.co.uk/security-problems-supply-chain/>. (Accessed: 12 March 2024).
- Pérez-Morón, J. (2022) Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda, *Journal of Asia Business Studies*, Vol. 16(2), pp. 371–395.
- Pirbhulal, S., Wu, W., Muhammad, K., Mehmood, I., Li, G. and de Albuquerque, V.H.C. (2020) Mobility enabled security for optimizing IoT based intelligent applications, *IEEE Network*, Vol. 34(2), pp. 72–77.
- Polit, D.S. and Beck, C.T. (2010) *Essentials of Nursing Research: Appraising Evidence for Nursing Practice*, 7th edn, Lippincott-Raven Publishers, Philadelphia.
- Ponemon Institute. (2021) 2020 cost of insider threats global report, *Technical Report*, 31 pages.
- Public Safety Canada. (2014) *Terminology Bulletin 281: Emergency Management Vocabulary*, Translation Bureau, Government of Canada. Available at: <http://www.bt-tb.tpsgc-pwgsc.gc.ca/publications/documents/urgence-emergency.pdf>. (Accessed: 8 April 2024).
- PwC. (2013) The Global State of Information Security Survey 2013. Available at: <https://www.pwc.com/gx/en/consulting-services/informationsecurity-survey/assets/2013-giss-report.pdf>. (Accessed: 12 March 2024).
- Radanliev, P., De Roure, D., Page, K., Nurse, J.R., Montalvo, R.M., Santos, O. and Burnap, P. (2020) Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and Industry 4.0 supply chains, *Cybersecurity*, Vol. 3, pp. 1–21.
- Raj, A., Choi, T.M. and Kumar, R.P. (2021) Implementing blockchain for supply chain operations: A proposed framework with applications, *National Taiwan University*, Working paper.
- Rao, S., Gulley, A., Russell, M. and Patton, J. (2021) On the quest for supply chain transparency through blockchain: Lessons learned from two serialized data projects, *Journal of Business Logistics*, Vol. 42(1), pp. 88–100.

- Reuters. (2017) Target pays millions to settle state data breach lawsuits. Available at: <https://fortune.com/2017/05/23/target-settlement-data-breach-lawsuits/>. (Accessed: 15 April 2024).
- Revilla, E. and Sáenz, M.J. (2013) A taxonomy of supply chain risk management strategies: Antecedents and performance. Available at: <http://gebrc.nccu.edu.tw/proceedings/APDSI/2013/proc/P130201019.pdf>.
- Rouse, W.B. (2005) Enterprises as systems: Essential challenges and approaches to transformation, *System Engineering*, Vol. 8(2), pp. 138–150.
- Rubin, H.J. and Rubin, I.S. (2005) *Qualitative Interviewing: The Art of Hearing the Data*, 2nd edn, SAGE, Thousand Oaks, CA.
- Ruslin, R., Mashuri, S., Rasak, M.S.A., Alhabsyi, F. and Syam, H. (2022) Semi-structured interview: A methodological reflection on the development of a qualitative research instrument in educational studies, *IOSR Journal of Research & Method in Education (IOSR-JRME)*, Vol. 12(1), pp. 22–29.
- RWJF (Robert Wood Johnson Foundation) (2008) Semi-structured Interviews. Available at: <http://www.qualres.org/HomeSemi3629.html>.
- Sadeghi, K., Azadegan, A. and Ojha, D. (2023) A path to build supply chain cyber-resilience through absorptive capacity and visibility: Two empirical studies, *Industrial Marketing Management*, Vol. 111, pp. 202–215.
- Sanjay, B.N., Rakshith, D.C., Akash, R.B. and Hegde, D.V.V. (2018) An approach to detect fileless malware and defend its evasive mechanisms, in *Proc. 3rd Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solutions (CSITSS)*, pp. 234–239.
- Schreier, M. (2012) *Qualitative Content Analysis in Practice*, 1st Edition, SAGE, Thousand Oaks, CA.
- Selviaridis, K. and Spring, M. (2007) Third party logistics: A literature review and research agenda, *International Journal of Logistics Management*, Vol. 18, pp. 125–150.
- Sharma, S. and Routroy, S. (2016) Modelling information risk in supply chain using Bayesian networks, *Journal of Enterprise Information Management*, Vol. 29(2), pp. 238–254.
- Shen, B., Dong, C. and Minner, S. (2021) Combating copycats in the supply chain with permissioned blockchain technology, *Production and Operations Management*, published online.

- Shi, C.H., Dong, K.J. and Ruan, J.H. (2009) Study on the risk sources of supply chains based on system theory, in *2009 IITA International Conference on Control, Automation and Systems Engineering (CASE)*, IEEE, pp. 156–159.
- Shukla, S., Rafatirad, S., Homayoun, H. and Dinakarrao, S.M.P. (2023) Federated learning with heterogeneous models for on-device malware detection in IoT networks, in *Proc. Design, Automation and Test in Europe Conference (DATE)*, pp. 1–6.
- Siegfried, P. and Al-Sobaihi, A. (2022) Cyber security in the logistics industry, *ResearchGate*. <https://www.researchgate.net/publication/360417486>
- Simon, J. and Omar, A. (2020) Cybersecurity investments in the supply chain: Coordination and a strategic attacker, *European Journal of Operational Research*, Vol. 282(1), pp. 161–171.
- Skipper, J., Craighead, C., Byrd, T. and Rainer, K. (2008) Towards a theoretical foundation of supply network interdependence and technology-enabled coordination strategies, *International Journal of Physical Distribution and Logistics Management*, Vol. 38(1), pp. 39–56.
- Sobb, T., Turnbull, B. and Moustafa, N. (2020) Supply chain 4.0: A survey of cyber security challenges, solutions and future directions, *Electronics*, Vol. 9(11), 1864.
- Stephens, J. and Valverde, R. (2013) Security of e-procurement transactions in supply chain reengineering, *Computer and Information Science*, Vol. 6(3), pp. 1–20.
- Svensson, G. (2000) A conceptual framework for the analysis of vulnerability in supply chains, *International Journal of Physical Distribution and Logistics*, Vol. 30(9), pp. 731–749.
- Tecuci, G. (2012) Artificial intelligence, *Wiley Interdisciplinary Reviews: Computational Statistics*, 2nd Edition, Vol. 4, pp. 168–180.
- Tezuka, K. (2011) Rationale for utilizing 3PL in supply chain management: A shippers' economic perspective, *IATSS Research*, Vol. 35(1), pp. 24–29.
- Tiwari, S., Sharma, P., Choi, T.M. and Lim, A. (2023) Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap, *Transportation Research Part E: Logistics and Transportation Review*, Vol. 170, 103012.
- Towill, D., Naim, M. and Wikner, J. (1992) Industrial dynamics simulation models in the design of supply chains, *International Journal of Physical Distribution and Logistics Management*, Vol. 22(5), pp. 3–14.

- Ugochukwu, N.A., Goyal, S.B. and Arumugam, S. (2022) Blockchain-based IoT-enabled system for secure and efficient logistics management in the era of IR 4.0, *Journal of Nanomaterials*, Vol. 2022.
- Urciuoli, L. (2015) Cyber-resilience: A strategic approach for supply chain management, *Technology Innovation Management Review*, Vol. 5(4).
- Urciuoli, L. and Hintsa, J. (2017) Adapting supply chain management strategies to security—an analysis of existing gaps and recommendations for improvement, *International Journal of Logistics Research and Applications*, Vol. 20(3), pp. 276–295.
- Van Marle, G. (2020) Toll refuses to pay cyber ransom as it acts to get its systems back online, *The Loadstar*, 5 February. Available at: <https://theloadstar.com/toll-refuses-to-pay-cyber-ransom-as-it-acts-to-get-its-systems-back-online/>.
- Venter, H.S. (2014) Security issues in the security cyber supply chain in South Africa, *Technovation*, Vol. 34(7), pp. 392–392.
- Verma, R.S. and Chandavarkar, B.R. (2019) Hard-coded credentials and web service in IoT: Issues and challenges, *International Journal of Computational Intelligence & IoT*, Vol. 2(3), Forthcoming.
- Vrijhoef, R. and De Ridder, H. (2005) Supply chain integration for achieving best value for construction clients: Client-driven versus supplier-driven integration, in *Proceedings QUT Research Week*, 4–6 July, Brisbane.
- Wahab, S.N., Loo, Y.M. and Say, C.S. (2020) Antecedents of blockchain technology application among Malaysian warehouse industry, *International Journal of Logistics Systems and Management*, Vol. 37(3), pp. 427–444.
- Wang, X. (2021) On the feasibility of detecting software supply chain attacks, in *MILCOM 2021–2021 IEEE Military Communications Conference (MILCOM)*, IEEE, pp. 458–463.
- Weber, R.P. (1990) *Basic Content Analysis*, 2nd Edition, Sage Publications, Newbury Park.
- Wengraf, T. (2001) *Qualitative Research Interviewing: Biographic Narrative and Semi-structured Methods*, 1st Edition, SAGE, London.
- Whitaker, B. (2020) SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments, *CBS News*, 14 February. Available at: <https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/>.

- White, S.M. (2015) Systems theory, systems thinking, in *2015 Annual IEEE Systems Conference (SysCon) Proceedings*, IEEE, pp. 420–425.
- Williams, C. (2014) Security in the cyber supply chain: Is it achievable in a complex, interconnected world?, *Technovation*, Vol. 34(7), pp. 382–384.
- Wilson, C. (2013) Semi-structured interviews, in *Interview Techniques for UX Practitioners: A User-Centered Design Method*, 1st Edition, pp. 23–41.
- Wong, L.W., Lee, V.H., Tan, G.W.H., Ooi, K.B. and Sohal, A. (2022) The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities, *International Journal of Information Management*, Vol. 66, 102520.
- Wong, T.C., Ngan, S.C., Chan, F.T. and Chong, A.Y.L. (2012) A two-stage analysis of the influences of employee alignment on effecting business–IT alignment, *Decision Support Systems*, Vol. 53(3), pp. 490–498.
- Xu, X., Sethi, S.P., Chung, S.H. and Choi, T.M. (2022) Reforming global supply chain operations management under pandemics: The GREAT-3Rs framework and research agenda, National Taiwan University. Working paper.
- Xue, L., Zhang, C., Ling, H. and Zhao, X. (2013) Risk mitigation in supply chain digitization: System modularity and information technology governance, *Journal of Management Information Systems*, Vol. 30(1), pp. 325–352.
- Younis, H., Sundarakani, B. and Alsharairi, M. (2022) Applications of artificial intelligence and machine learning within supply chains: Systematic review and future research directions, *Journal of Modelling in Management*, Vol. 17(3), pp. 916–940.
- Zacharia, Z.G., Sanders, N.R. and Nix, N.W. (2011) The emerging role of the third-party logistics provider (3PL) as an orchestrator, *Journal of Business Logistics*, Vol. 32, pp. 40–54.
- Zeadally, S., Yu, B., Jeong, D.H. and Liang, L. (2012) Detecting insider threats: Solutions and trends, *Information Security Journal: A Global Perspective*, Vol. 21(4), pp. 183–192.
- Zheng, K. and Albert, L.A. (2019) A robust approach for mitigating risks in cyber supply chains, *Risk Analysis*, Vol. 39(9), pp. 2076–2092.
- Zsidisin, G. and Ellram, L. (2003) An agency theory investigation of supply risk management, *Journal of Supply Chain Management*, Vol. 39(3), pp. 15–27.

APPENDICES

Appendix A – Semi - Structured Interview Questionnaire

Demographic Information

1. Age:

☐18-25 ☐26-35 ☐36-45 ☐46-55 ☐56 and above

2. Gender:

☐Male ☐Female ☐Prefer not to say

3. Job Title:

4. Department:

5. Years of Experience in the Logistics/Supply Chain Industry:

☐Less than 1 year ☐1-3 years ☐4-6 years ☐7-10 years ☐More than 10 years

6. Educational Background:

☐High School Diploma

☐Associate Degree

☐Bachelor's Degree

☐Master's Degree

☐Doctorate

Other (Please specify):

7. Company Size (Number of Employees):

☐Less than 50 ☐50-100 ☐101-500 ☐501-1000 ☐More than 1000

8. Type of Service Provided by Your Company:

☐Transportation ☐Warehousing ☐Distribution ☐Freight Forwarding ☐Supply Chain Management

Other (Please specify):

9. Geographic Region of Operations:

☐North America

☐South America

☐Europe

☐Asia

☐Africa

☐Australia

Other (Please specify):

INTERVIEW QUESTIONS

About Technology Use and Stakeholders

1. What technology and software do you use to ensure flow during the operation process?

1.1. Can you explain to what extent these technologies are used and in which supply chain partners they are integrated, on a sectoral basis without naming the company?

1.2. Is there a connection between the technologies and software you use and those used by stakeholders? If they are independent, from which stakeholders do you receive information and to which stakeholders do you transmit it?

2. How is information (data) entered into the systems during the operation process, how is it shared, how does it stay in flow? Can you tell us about your general operation process?

3. How secure are the technologies and software used in the industry, and what risks are there?

4. Who are your supply chain partners? Can you explain on a sectoral basis without naming companies?

5. What information is shared with which stakeholders during the operation process?
What information is conveyed to you from which stakeholders?

5.1. To which other stakeholders in the chain does information shared with one stakeholder reach?

5.2. What information and data received from stakeholders are kept in your systems? How long is it stored?

About Cybersecurity

6. Can you explain your understanding and definition of cybersecurity in the context of the sector, your company, or third-party logistics (3PL) providers?

7. How important is cybersecurity in the 3PL sector? How does ensuring cybersecurity affect the sector, your company, your operations, and your partners, and to what extent?

7.1. We know that cybersecurity is weaker and the risk of attacks is higher in developing and underdeveloped countries. Who are the stakeholders in cooperation in operational activities in these countries, how is information shared, and what security measures are taken? What cybersecurity threats might be encountered, is the risk higher compared to other operations, what are the possible effects of an attack, and what strategies should be applied against these threats? Can you explain?

8. Can you evaluate the current state of cybersecurity in the sector or your company?

9. How do you ensure cybersecurity?

9.1. What measures do you take within the company?

9.2. How is cyber security ensured in the process of sharing information and data outside the company, that is, with stakeholders?

About Cyberattacks

10. What are the potential cyberattacks in the sector? What are you hearing about the issue in the industry?

11. If a cyberattack occurs in the 3PL sector, who would be affected and how?

11.1. What kind of threats and effects does any cyberattack on your systems or a 3PL company in the industry pose?

11.2. In your experience and observations, what are the immediate and long-term effects of cyberattacks on supply chain resilience?

12. Have you ever experienced a cyberattack, do you know any examples from the industry, what are your observations?

13. Which operational processes are more vulnerable and fragile to cyberattacks?

14. What kind of problems occur in the flow of a 3PL company in a situation where information leaves the system or is stolen during the operation process? What happens in a 3-week period when systems are attacked and access to information is cut off in a 3PL company, as in the Maersk example? (You can explain through your own company)

14.1. If the X information you received from any partner A is stolen during the operation, how will the partner A who provided the information be affected?

15. We have been seeing an increasing number of cyberattacks lately. Is there a side of cyber security that cannot be prevented on a company and sector basis, as in the Maersk example?

About Situation and Precautions Before and After Cyberattack

16. Have you taken precautions against cyberattacks that have occurred or may occur even if you have not experienced them? Can you explain what to pay attention to in this process, what precautions should be taken, what should be done in the sector?

17. In case of a cyberattack scenario, what do you do to prevent the attack completely or keep the damage to a minimum? Can you explain what should be done in the sector?

17.1. How can the entire system be recovered and improved after a possible cyberattack, and what difficulties would arise in this process?

18. What are the biggest challenges your company and the industry face in implementing effective cybersecurity measures? What factors negatively affect cybersecurity efforts in the industry (such as budget constraints, lack of expertise, or technological limitations), and how do they affect it?

19. How do you evaluate the cybersecurity level of your stakeholders? What are your evaluation criteria and can you evaluate the importance of stakeholders in this context?

20. How is collaboration done with other organizations in the supply chain (suppliers, logistics providers, retailers) to solve cybersecurity issues in the industry? Can you explain the role and importance of stakeholders?

About the Future of Cyber Security

21. How do you see the future of cybersecurity?

21.1. Will it be more risky?

21.2. What steps do you believe your company, 3PL companies, other actors and the industry as a whole should take to improve cyber security and supply chain flexibility in the future, and what are their duties?

Appendix B – Semi-Structured Interviews’ Participant Consent Form

PARTICIPANT CONSENT FORM

I have read the participant information form prepared for the master's thesis titled "**Enhancing Cybersecurity in Logistics Services: A Study on Third-Party Logistics (3PL) Service Providers,**" conducted by Barış Can GENÇ, a graduate student in the Logistics Management Master's Program at İzmir University of Economics, under the supervision of Assoc. Prof. Dr. Aysu GÖÇER, a faculty member in the Logistics Management Department.

I voluntarily agree to participate in this research. Additionally, I permit the use of all data I provide during the interview study for scientific purposes.

Name and Surname:

Date:

Signature:

Appendix C – Semi-Structured Interviews’ Participant Information Form

PARTICIPANT INFORMATION FORM

Dear Participant,

With the advent of Industry 4.0, technological advancements have brought about revolutionary operational developments in supply chain and logistics operations while also introducing cybersecurity risks. According to research, supply chain and logistics operations, which are among the world's largest industries, are the number one target for attackers. Statistics show that 60% of supply chain-focused cyber attacks are centered on suppliers and third-party logistics providers (3PL). Today, companies mostly outsource their logistics operations to 3PLs, and since 3PLs are intermediary links in the supply chain, a potential attack poses security threats and serious risks to the entire supply chain, making 3PLs highly significant in this context. The aim of this study is to investigate how cyber attacks targeting third-party logistics (3PL) service providers impact the overall efficiency and resilience of the supply chain, identify effective mitigation strategies, and explore the impacts of implementing these strategies.

In the semi-structured interview, we will explore how cyber attacks on third-party logistics (3PL) service providers affect the overall efficiency and resilience of the supply chain. This research aims to gather information about the nature of these impacts, understand how organizations manage such disruptions, potential risks, their experiences, and responses. Your expertise and experiences in the sector are invaluable for shaping this master's thesis and contributing to the logistics industry.

In this study, you will participate in an interview consisting of semi-structured open-ended questions. During the interview, I will generally ask about the 3PL sector, your experiences, and observations.

Your personal information and the identity of your organization will not be shared with third parties or disclosed in the thesis and publications. The interview **will not include** questions aiming to reveal the content specific to your firm.

The answers provided will be used solely for academic purposes, and no actions or content that could harm you or your organization will be created.

Thank you in advance for your participation in our study.

Sincerely,

Barış Can GENÇ
Izmir University of Economics
Master's Student in Logistics Management

APPENDIX D – Ethical Approval

SAYI: B.30.2.İEÜ.0.05.05-020-390

04.09.2024

KONU : Etik Kurul Kararı hk.

Sayın Doç. Dr. Aysu Göçer ve Barış Can Genç,

“ENHANCING CYBERSECURITY IN LOGISTICS SERVICES: A STUDY OF THIRD-PARTY LOGISTICS (3PL) SERVICE PROVIDERS” başlıklı projenizin etik uygunluğu konusundaki başvurunuz sonuçlanmıştır.

Etik Kurulumuz 03.09.2024 tarihinde sizin başvurunuzun da içinde bulunduğu bir gündemle toplanmış ve Etik Kurul üyeleri projeleri incelemiştir.

Sonuçta 03.09.2024 tarihinde **“ENHANCING CYBERSECURITY IN LOGISTICS SERVICES: A STUDY OF THIRD-PARTY LOGISTICS (3PL) SERVICE PROVIDERS”** konulu projenizin etik açıdan uygun olduğuna oy birliğiyle karar verilmiştir.

Gereği için bilgilerinize sunarım.

Saygılarımla,

Prof. Dr. Murat Bengisu
Etik Kurul Başkanı