The effect of COVID-19 on supply chain visibility adoption among Small and Medium Enterprises

Akshay Mahesh
a.a.mahesh@tilburguniversity.edu

Enes Öztan
e.oztan@tilburguniversity.edu

Dennis van den Eijnden
d.c.s.j.vdneijnden@tilburguniversity.edu

Tobias von Burg
t.l.vonburg@tilburguniversity.edu

Attila Tonacs
a.a.tonacs@tilburguniversity.edu

ABSTRACT

The COVID-19 pandemic and the subsequent lockdown measures disturbed the orderly flow of global trade and shook the logistic and transport sector along with it. Adapting to the novel situation and preventing forthcoming calamities seem feasible with the implementation of Supply Chain Visibility (SCV) technologies.

In our research, we aim to understand the impact of Covid-19 on the adoption of SCV amongst SMEs within the Netherlands and help SMEs with deciding whether or not to invest in such a technology during the global pandemic.

Throughout the research, we applied a combination of literature review and interviews with experts from different specialization, including Business Process Integration, IT governance and Cybersecurity.

SCV proves to be an adequate solution for enhancing transparency, but the SMEs need to meet some prerequisites before deploying such a technology. A more agile IT governance structure turns out to be essential for SCV. Connecting to a „smart network" of partners improves performance, but it may also involve cybersecurity risks.

Based on our key findings, we suggest that SMEs should look into the requirements, advantages and barriers that we discuss in this paper regarding the implementation of this technology. It is also strongly advised to make a thorough risk assessment before making investment decisions.

Keywords

Supply chain visibility, COVID-19, Small and medium enterprises, Logistics 4.0

INTRODUCTION

Starting from the Hubei province in China, the novel coronavirus (SARS-CoV-2) which causes the disease known as Covid-19 has been spreading all over the world after two months of the outbreak in China. Despite significant efforts, the disease spread quickly putting communities, ecosystems and supply chains at risk. Including those in the Netherlands. The outbreak of the virus is damaging the Dutch economy in a stage-by-stage process. According to research by ABN AMRO Advisory, the transportation and logistics sector shrank in 2020 with six per cent compared to 2019 (Phlippen, Neuteboom, & Klene, 2020). The logistics and transport sector is of great economic importance and makes a significant contribution to the Dutch economy. According to a report of the Dutch bank ING, the logistics and transport sector is responsible for almost nine per cent of the GDP of the Netherlands, which has an added value of € 65 billion. In 2018, the Netherlands was ranked 6th in the Logistics Performance Index. Mainly, the sea freight via the Port of Rotterdam and the air freight via Schiphol is very important for the sector and the Dutch economy (Bode, 2020).

China's role and importance to global trade have grown significantly as they are a primary producer of high-value products and components, a large customer of global commodities and industrial products and the country is a very attractive consumer marketplace. For instance, Wuhan has been a traditional base for manufacturing for decades. Therefore, it can be said that if China "the world's factory" is impacted, global supply chains are impacted. According to a Deloitte report, Covid-19 may be a catalyst for (some) companies to revisit their global supply chain strategy. For logistics and transportation companies, one way to respond is to enhance materials visibility. By means of Supply Chain Visibility (SCV), companies can get visibility

to the status of their shipments, inventory at the supplier The classical supply chain will be replaced by a network location, supplier production schedules, and supplier shipment status which will help them to predict supplier shortages and respond accordingly. SCV became especially important during Covid-19 as it can help companies to reduce risks and costs. These companies can conduct scenario planning on how disruption will affect them and their suppliers and proactively determine alternative sources and strategies. However, this requires a change of the traditional supply chain into a network of companies.

PROBLEM STATEMENT

The impact of Industry 4.0 is also visible in the logistics and transport sector. Logistics 4.0 can be defined as followed: "Logistics 4.0 is the logistical system that enables the sustainable satisfaction of the individualized customer demands without an increase in costs and supports this development in industry and trade using digital technologies" (Winkelhaus & Grosse, 2019, p. 21). The basis of Logistics 4.0 is formed through a smart supply chain. Therefore, Supply Chain 4.0 plays an important role for Logistics 4.0. The digitization of logistics such as digital supply chains, autonomous decisions and logistic activities as self-propelled vehicles are examples of logistics 4.0. Especially the flow of products and information in the supply chain is becoming smarter and more autonomous. Smart containers, smart packaging and wireless transport systems are contributing to more information within the supply chain. These technologies and information will contribute to a better overview and better monitoring of the flows, which could lead to better decision-making on the effectiveness of the SCM (Bukova, Brumercikova, Cerna, & Drozdziel, 2018)**.**

An upcoming trend in Logistics 4.0 is SCV. According to Somapa et al. (2018), SCV refers to "the extent to which actors within the supply chain have access to the timely (real-time) and accurate information that they consider to be key or useful to their operations". In a survey conducted by EY (2020), it was shown that only 6% of the respondents had trust in their systems and capabilities for end-to-end SCV. Taken together, the results of the survey suggest that there is a major gap between the actual capabilities of organisations and the value of SCV. However, COVID-19 has boosted the investments in SCV. Investing in SCV is important because "it reduces risk and costs, better alignment of supply with demand and increases speed and agility" (Steinberg, 2020)**.** Since there is a lot of uncertainty at the moment, many companies invested SCV to have a firmer grip on the situation (Steinberg, 2020). However, with these innovative technologies, there is a risk of suffering from the "shiny toy" syndrome. According to EY (2020), the shiny toy syndrome is defined as followed: "focusing on adopting the latest technology without a clear business case".

The key players in the international market like UPS, DHL and Kuehne + Nagel are experimenting with these IT-based integrated logistics solutions. These international companies are progressive in the market. However, previous studies on supply chain visibility have not dealt with the consequences for small and medium-sized enterprises (SMEs). For SMEs investing in SCV, during the COVID-19 crisis, brings risks. This indicates a need to understand the impact of COVID-19 on the importance of SCV for SMEs.

The main aim of this study is to investigate the impact of Covid-19 on the adoption of SCV amongst small-medium enterprises (SMEs) within the logistics sector in the Netherlands, and the additional requirements, advantages and risks that come with it. Thus we investigated the environment before Covid-19 and compared it to how the disease influenced the adoption during the pandemic. The knowledge created will provide insight on whether it is beneficial (or not) for SMEs to implement SCV, thus creating a body of knowledge for other companies to reflect on their own company whether such a technology could be relevant. Furthermore, it generates knowledge about what is required to implement it, what the best delivery model is, and how to secure it.

Relevance

This research is particularly important because it focuses on the SMEs, which together account for almost 99% of the companies in the Netherlands, according to CBS (2020).

OBJECTIVE

As COVID-19 caused uncertainty throughout the whole world, the logistics sector has shown great interest in investing Supply Chain Visibility (SCV) technology to gain more control over the supply chain. Our research objective is to understand the impact of Covid-19 on the adoption of SCV amongst SMEs within the Netherlands and help SMEs with deciding whether or not to invest in SCV during the global pandemic.

While there is literature on investing in technology during uncertain times, SCV technology is still quite new and business owners and professionals within SMEs are not sure if they should invest in this new technology, especially in uncertain times. With this paper, we want to give logistics professionals within SMEs insight in SCV technology to help them assess whether or not to invest in SCV technology.

Research question: what is the effect of Covid-19 on the adoption of SCV among SMEs in the Netherlands, and what are the consequences?

APPROACH

The study was conducted in the form of interviews with experts regarding business process integration, IT governance, cybersecurity, and crisis management with secondary data being gathered through analysing literature. The interviews were conducted with Francesco Lelli (business process integration expert), Carol Ou (IT Governance expert), Joris Hulstijn (Cybersecurity expert), and Kenny Meesters (Crisis Management Expert). The interviews are transcribed and can be found in Appendix 1. The gathered secondary data mostly consists of existing literature found via Google Scholar, EBSCO Webhost, Academia, and Tilburg University's library.

As our research objective states, we investigate the impact of the unanticipated disruptions in the global value chains – linked to the COVID-19 pandemic - on the adoptions of Supply Chain Visibility (SCV) technologies in small and medium enterprises (SMEs) in the sector of logistics and transport, and the consequences of the adoption of SCV.

To analyse the decisions, processes and the arising risks these firms have to face when implementing such a system, we mostly base our research on a combination of literature review and interviews with experts from different specializations. The main advantage of this method is that we can easily unfold the attitude of company leaders towards these technologies and we can detect possible motives behind their decisions. We can also find more about the future implications of the use of these technologies or we can forecast the probability of in-company resistance by employees or stakeholders.

We have collected our data from archives of journals, which were mostly retrieved from the internet and the library.

ANALYSIS

In the consecutive sections, the transportation and logistics industry of the Netherlands is analysed with special attention to the Dutch SMEs operating in the sector and the implications of possible SCV investments. In our analysis, we take a glance at the overall shape of the sector pre- and post-COVID-19, highlighting the main impacts of the pandemic and the subsequent restrictions on the industry. Following that, we focus on the implementations of SCV technologies within SMEs, which we consider as a possible solution preventing disruptions in future. We approach this subject with the methods offered by IT Governance and Strategic Sourcing, Business Process Integration and Cyber Security.

IT Governance and Strategic Sourcing

Situation pre-Covid-19

Effective utilization of IT Governance is crucial to managing the effectiveness of IT investments. While most of IT governance literature focuses on large companies, Rudenko (2012) states that within small enterprises there is a lack of formalized IT governance structure and that most medium-sized enterprises use the COBIT framework to structure their IT governance.

Consequences of Covid-19 for IT governance within the sector

While IT Governance has been relevant for a long time, the current situation with COVID-19 gives organizations even more urgency to have an effective and efficient IT Governance structure. During times of crisis, introducing an agile governance structure can be used to deploy new technologies faster than usual. Introducing an agile governance structure means focusing on quick software development, decision making pushed to lower levels within the organization and an emphasis on speed (Janssen & van der Voort, 2020)

Guidelines to govern IT investments

To analyze how the introduction of new technology can be best governed, we will apply the Weill & Ross framework (2004) to Dutch companies introducing SCV technology.

Traditionally, IT Governance is composed of five different decision domains. Namely, IT principles, IT architecture, IT infrastructure strategies, Business application needs and IT investments. The deployment of SCV in an organization would fall under the category of 'Business application needs'. When assessing the introduction of supply chain technology within the company, there are several questions the decision-makers need to consider. These questions are:

- What are the market and business process opportunities for SCV?
- If we start a pilot with SCV, when will it be considered successful?
- If we choose to introduce SCV, who will become responsible for managing the introduction of the technology?
- What impact will the introduction of SCV have on our IT infrastructure?

These questions should be answered before utilizing an SCV pilot in order to ensure the right governance. Besides answering these questions, the organization should also formalize the decision-making process for all IT investments. Within the domain of IT governance, there are five main decision making governance archetypes. Namely, business monarchy, IT monarchy, federal, IT duopoly and feudal. Ross & Weill (2004) argue that business application investment decisions should be made through a federal governance archetype. In a federal system, C-level executives and business representatives of all operating groups make investment decisions together with the IT department. This seems like a fitting approach for the introduction of SCV as input from the business is needed to understand the business need and the IT department needs to be involved in the decision-making process to have a critical view of the possibilities and risks that come with the introduction of new technology.

Once the companies have a good understanding of the need for the SCV technology and have established a federal archetype to make the decision, they should know how they will govern the technology once it is implemented in the organization. In order to establish effective governance, they should have a great understanding of the strategic driver, key metrics, key IT governance mechanisms, IT infrastructure, key IT principles and governance.

As SCV technology is still an upcoming technology, executives need to ensure that they have a good understanding of the possibilities within their current IT infrastructure and IT capabilities. Once they have a good overview of the internal possibilities, SMEs who are interested in this technology should decide which parts of the technology they want to develop, host and maintain within the organization and which parts they want to outsource to other companies. Once this is clear, the right governance structure should be developed in order to ensure that the outsourced services are managed effectively.

Regarding the changing dynamics of the sector through Covid-19, we advise SMEs within the logistics industry to manage their IT governance through the provided guidelines by Weill & Ross (2004) in combination with an agile mindset to be able to introduce new technologies with the necessary speed.

Business Process Integration

Situation pre-Covid-19 – 2018

Before Covid-19 affected the Dutch market, the financial forecasts were positive. Import and export were important for the transportation and logistics industry, and both were predicted to grow further in 2019. According to a report by ABN Amro (2018), the expected growth in the logistics industry was predicted at 1.5%. In November 2018, a total of 391,000 jobs (which is five per cent of the total jobs in the Netherlands) was within the transportation and logistics sector. In the second quarter, there was more demand than supply of workforce, partly because of the ageing of the labour market. The increase in transportation led to more emissions and the sector was planning to invest in smart loading and unloading locations, electric vehicles and smart planning of routes.

The threats that the logistics sector faced were: high staff shortages that would hinder growth, Brexit and its consequences regarding additional customs formalities and sustainability that could not be ignored.

Consequences of Covid-19 for the sector

Major risks according to ING's sector banker transport & logistics Machiel Bode (2020), are that companies, in the short-term will have liquidity issues, and on the long-term will face insufficient resistivity. The first issue is related to unavailable inventories, sudden reduction (or increase) in demand from customers, where the lost revenue represents a permanent loss rather than a timing difference and that is putting pressure on working capital and liquidity. The second issue is related to the staff shortages that were mentioned before, companies face difficulties in replacing the workforce when ill (and in quarantine) for instance.

In the first weeks of the government measures, citizens were often buying extra groceries to stock up. This led to a twofold or threefold of required transportation (Ramdjan, 2020). This led to transportation companies to extra vehicles and extra chauffeurs. Furthermore, many European countries have introduced additional border checks as prevention, leading to longer waiting times (Ramdjan, 2020).

Opportunities

Change of Processes

The influence of the Internet of Things (IoT) and mobile connectivity had influenced the industry before Covid-19, but that trend will continue significantly (Bode, 2020). The classical supply chain will be replaced by a network in which everyone can act on behalf of the others. All capacity, supported by algorithms, internet and smart ICT applications will be used to deliver products to the customer. This requires

transparency, where SCV could add value, as all participants can view the exact status and location of a product. Thus, this requires a significant change in processes. Working together in this "smart network" requires working together even more than before, but these embedded processes lead to substantial business advantage (Vervest, van Heck, & Preiss, 2008).

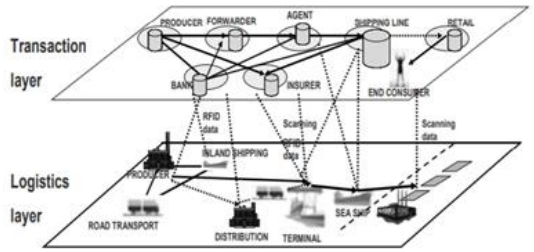

FIGURE 1 - The Traditional Business Network Approach, source: (Vervest, van Heck, & Preiss, 2008).

With regards to the processes, this implies that linking partners is based on linking processes, still allowing individual execution according to those processes; companies act individually according to the joint rules of the network (Vervest, van Heck, & Preiss, 2008). The network separates the process from execution. Such a network shares the processes required to achieve delivering the products to the customer allowing each participant to execute in its own way according to this logic. This means that to be a member of the network, an organization must be able to absorb the shared logic and execute accordingly (Vervest, van Heck, & Preiss, 2008). Schmidt (2020) agrees that the transportation and logistics industry needs innovation and flexibility. According to Schmidt (2020), partnerships are the most important factor, benefitting coordination and optimisation. Furthermore, the industry should digitalise, as Covid-19 showed that manual and/or paper processes are outdated. Digital processes allow for more (short-term) flexibility (such as last-minute changes due to bad weather).

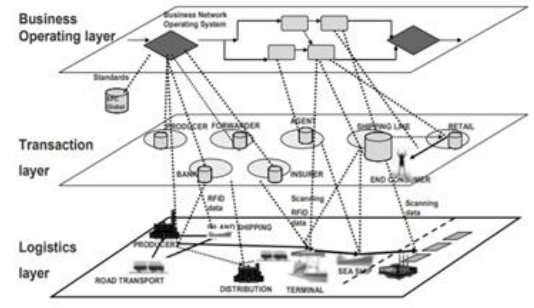

FIGURE 2 – The New Business Network Approach, source: (Vervest, van Heck, & Preiss, 2008).

Change of services, environment and market

The global economy before Covid-19 was highly dependent on China. The crisis made it difficult to rely on the transportation of products from China to elsewhere. Currently, companies are seeing greater value in storing inventory in strategic locations from where it can be easily accessed and delivered to customers (The Economist Intelligence Unit Limited, 2020). Such a location characterises as a low-risk location, close to the market, and has a strong political, economical and infrastructural environment. According to a graph by the Eurasia Group, the Netherlands is a top performer on these factors. According to panellist Bart Kuipers, port economist at Erasmus University, the Netherlands could become a "logistics hub" to distribute China-based production, thus will significantly increase the economic value of the sizable Dutch transportation and logistics sector (Caluwe, 2020).

Challenges

Challenges for Dutch SMEs according to Fottner (2020) are that the increasing digitalisation requires significant improvement of the physical processes such as order picking, sorting, and dividing products; which requires (large) investments. For this (and for the smart network) an improvement of flexibility and adaptability is required; which can be difficult. Furthermore, the collaboration of human capital and machines within industry 4.0 should become the "new normal" to (Fottner, 2020). Further challenges are those that were present pre-Covid-19, such as high staff shortages, ageing of the labour market and Brexit.

Cybersecurity

New technologies continue to change how organizations complete. SCV uses a lot of new technologies of the Industry 4.0, such as big data, cloud computing, artificial intelligence (AI), internet of things (IoT) and RFID and NFC sensors. This emerging trend is also called "logistics 4.0". According to Steinberg (2020), these technologies could reduce risks and costs, better alignment of supply with demand and an increase of speed and agility. The reliance on organizations in data and data processing is becoming more and more important (Duc & Chirumamilla, 2019). This could lead to new risks for the organizations, for example, cybersecurity risks. Previous studies who identified supply chain risks have not dealt with the role of technologies related to Industry 4.0. The new possible cybersecurity risks of SCV for SME's within the Dutch logistic and transport sector will be discussed in this section. Furthermore, the risks of a

connected supply chain will be analyzed. Finally, possible solutions to mitigate these cybersecurity risks will be provided. The extended analysis is provided in Appendix 2.

Identify risks of logistics 4.0

Industry 4.0 is an umbrella term for technologies that are used for automation and data exchange in the manufacturing sector. Figure 3 shows an overview of the nine technological pillars of Industry 4.0. Logistics 4.0 operates under the same principles as Industry 4.0. However, cloud computing, IoT and RFID technologies are mostly used within logistics 4.0. Implementing these new technologies involves risks and possible direct cyber-attacks.

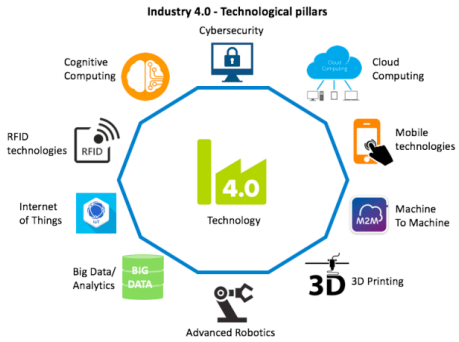

Figure 3 Technologies Industry 4.0 (Saturno, Pertel, & Deschamps, 2017)

However, *a fully integrated and connected supply chain is as strong as its weakest link*. Because all devices, gateways and servers, within a chain, are connected with each other. This increases security risks due to the wide environments these logistics 4.0 applications touch (Dingee, 2019). When all actors within a supply chain are connected, the possible cybersecurity risks will increase and embrace further in the network (Pandey, Singh, Gunasekaran, & Kaushik, 2020). According to Pandey et al. (2020), the following cybersecurity risks will occur in a connected supply chain; *Partners trust, product specification fraud, poor protection of cargo in transit, unauthorized access, information theft and counterfeit products.* This study will analyze the above risks, which occur because of the risks and direct attacks of the new logistics 4.0 technologies. These risks will be analyzed in the risk assessment in table 1.

Risk assessment

It is important for SME's that the possible cybersecurity risks of a connected supply chain are clearly mapped out. For this reason, a risk assessment has been made to understand the impact and the likelihood of cybersecurity risks. Every cybersecurity risk has been analyzed on the possible impact and likelihood that the cybersecurity risk will occur. This has led to a score per risks, which eventually will be categorized into a low, medium or high-risk level for the organization. The results of the risk assessment are shown in table 1. The motivation of the choices is provided in Appendix 2.

Solutions

The identified risks occur within the whole supply chain. The supply chain can be divided into three sectors: upstream, focal firm and, downstream.

Table 1 Risk Assessment

	Technologies	Risks	Security concerns	Likelihood (1-5)	Impact (1-5)	Overall Risk (1-25)	Risk Level*
R1	Weakest link	Partners trust	Confidentiality	4	5	20	High
R2	IoT	Product specification fraud	Integrity	3	4	12	Medium
R3	IoT	Poor protection of cargo in transit	Integrity	2	5	10	Medium
R4	IoT, CC, RFID	Unauthorized access	Integrity	3	3 (internal/external)	9	Medium
R5	Weakest link, IoT	Information theft	Confidentiality	2	4	8	Low
R6	Weakest link	Counterfeit products	Integrity	2	2	4	Low

*Low 1-8, medium 9-17 and high 18-25

Table 2 Measures for mitigating cyber risks

	Risks	Cyber security measures for mitigation
R1	Partners trust	Network audit (Windelberg, 2016)
		Supplier audit (Windelberg, 2016)
		Confidentiality agreements (Tran, Childerhouse, & Deakins, 2016)
R2	Product specification fraud	Event logging
R3	Poor protection of cargo in transit	Vulnerability checks
		Monitor network traffic
R4	Unauthorized access	Access control
		Event logging
R5	Information theft	Authentication processes
R6	Counterfeit products	Information sharing

In each sector, different risks apply. In the upstream supply risks, in the focal firm operational risks and downstream demand risks (Pandey, Singh, Gunasekaran, & Kaushik, 2020). For example, partner risk (R1) occurs in the upstream or downstream of a supply chain. Hence, this risk is a supply- and demand risk. However, unauthorized access (R4) can occur throughout the whole supply chain. Thus, for each sector, different risk mitigation strategies apply. Furthermore, risk mitigation strategies are divided into three phases. The three phases are, pre-attack, trans-attack and post-attack. Besides, "the risk mitigation typically depends on the type of cyber-attack, impact of the attack and resilience of the organization" according to Ghadge et al. (2020, p. 11). Risk mitigation measures need requirements. Ning & Liu (2012) suggest that the security requirements elements include the CIA (Confidentiality, Integrity and, Availability Triad, authority, non-repudiation, and privacy. However, according to the PAS 555 (2013), it is important to "emphasizes that technical measures alone are not enough, effective outcomes encompass people and behaviours, physical and equipment security, as well as governance, leadership and culture". From this information the measures for mitigating cyber risks are determined, see Table 2. The motivation of the measures is provided in Appendix 2.

Conclusion

In this report, we described the risks and how those risks can be mitigated. However, as with most risk management situations, after implementing these measures there will still be risks that Dutch SMEs can face when implementing SCV within their organization. Supply chain visibility is still a fairly new technology which means that there probably will be more innovations in the future, which will bring new risks with them. To ensure resilience within the whole supply chain and to be aware of new threats, we propose that supply chains that make use of SCV conduct a cybersecurity assessment for the whole network, every six months.

DISCUSSION

To interpret the results, laid out in the previous sections, we loosely followed the SWOT framework to identify the different success factors and barriers SMEs have to face, when undertaking SCV implementations. The well-known SWOT framework is serving as a logic base to cross-examine all the findings we had on the implementation of SCV technologies in SMEs, analysed in the three different perspectives.

SWOT is considered a reliable model for strategic planning, which is used in the preliminary stages of the decision-making process. SWOT is useful for providing insight into internal and external factors (internal: strengths, weaknesses, external: opportunities, threats) companies have to face when launching a project like SCV.

One of the strengths of SMEs essential for SCV is that they are likely to operate in more agile organizational structures than their larger competitors. Agile IT governance is a key element of deploying new technologies and quicker software development. Introducing a more agile IT governance can be more effective in an organization where the overall decision-making processes are

pushed to lower levels.

Among the main weaknesses of SMEs, we can mention the permanent loss of income due to the sudden reduction in demand from customers during the pandemic, which is a serious hindrance when a company wants to invest in new technologies. SMEs usually have less overall resources and they are operating with less safety margin than large companies. The insufficient financial background leads not only to serious competitive disadvantages, but it makes it difficult or even impossible for SMEs to venture in projects involving new and risky technologies.

As stated in the IT governance section of the analysis most SMEs lack formalized IT governance structures, which also implies the lack of expertise with the governance of large scale technological investments, like SCV. The lack of high-profile IT personnel can also add up to the weaknesses of SMEs when it comes to SCV. Experts of industry 4.0 technologies are hard to find and they are expecting high wages. Many large companies were investing a lot in SCV before the pandemic, thus having now considerable know-how and expertise. Notwithstanding their capability to offer higher wages and thereby sucking up the human capital, essential for SMEs to implement and operate their technology.

As for the opportunities, successful adoption of SCV technology can offer to SMEs, we can mention that the connection to "smart network" leads to better optimization of the processes, more effective cooperation and transparency. Utilizing this, the customer receives a far better service, accomplished through these faster and more flexible networks. This can lead to a substantial business advantage for SMEs, which otherwise would be hard to establish in an industry dominated by larger players. Before implementing SCV the physical processes also need to be improved. This is an opportunity for SMEs to optimize these processes, further improving their competitiveness

If the Netherlands becomes a logistic hub for China in the foreseeable future it will generate higher demand for the services of SMEs as well, which is a huge possibility to improve on their financial status. However, it also leads to intense competition, in which only a well-equipped and the digitally transformed company could prevail. This further emphasizes the importance of SCV in SMEs.

The greatest threats SMEs have to face when implementing SCV technology can be found around the job market and it is the inadequate supply of professional personnel and technologists of industry 4.0. Successful cybersecurity operations are also dependent on high-skilled employees. As it is stated in the Cybersecurity risk analysis, connecting to smart networks of logistics also poses concerns on choosing the trusted partners and the formation of reliable partnerships

CONCLUSION

This paper intends to show the impact of Covid-19 on the adoption of SCV, and the additional requirements, advantages and risks that come with it. It shows that pre-Covid-19, the transportation and logistics industry was stable and the financial predictions were positive, but it was lacking formalised IT governance structure. Covid-19 affected the adoption of SCV because China, "the world's factory" was significantly impacted. The crisis made it difficult to rely on the transportation of products from China and made it difficult to plan; Thus, companies want to invest in more transparency to be knowledgeable about every aspect of the inventory and shipped goods for their planning.

Adopting SCV requires companies to rethink their IT governance and introduce an Agile structure that allows for flexibility in decision making. This is required to deal with this relatively new technology. Furthermore, to gain the maximum performance, the classical supply chain will be replaced by a "smart network" where businesses collaborate on a large scale. However, the downside is that SVC and collaboration in smart networks introduce additional security risks, which companies have to consider.

A risk that increases as a result of SCV adoption, is data vulnerability. Data storage on cloud servers introduces limited control of data (as data is put-on third-party servers). Moreover, the use of IoT allows companies to trace every step through sensors, however, it could also allow intruders access to the (sensitive) data and the intruders could also sabotage the devices to disrupt the business network. Working together in a network introduces the risk of a weak link in the network. Partners with malicious intent could steal confidential information and counterfeit products, competitors and partners.

Thus, although the adoption of SCV increased due to Covid-19, it is recommended that companies look into the requirements, advantages, barriers, and increased security threats discussed in this paper to assess whether adoption. We suggest companies make a risk assessment to make a well-determined decision.

REFERENCES

ABN Amro. (2018). *Aan uitdagingen geen gebrek in de logistieke sector.* Amsterdam: ABN Amro.

Birkel, H., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management*, 39-61.

Bode, M. (2020). *De impact van corona op transport en logistiek - ING - Kennis over de economie*. Opgeroepen op October 14, 2020, van ing.nl: https://www.ing.nl/zakelijk/kennis-over-de-economie/uw-sector/transport-en-logistiek/trends2020-transportenlogistiek-corona.html

Bukova, B., Brumercikova, E., Cerna, L., & Drozdziel, P. (2018). The Position of Industry 4.0 in the Worldwide Logistics Chains. *LOGI – Scientific Journal on Transport and Logistics*, 18-23.

CBS Statline. (2020). *StatLine*. Opgeroepen op October 14, 2020, van mkbstatline.cbs.nl: https://mkbstatline.cbs.nl/#/MKB/nl/

Dingee, D. (2019, January 23). *IoT, Not People, Now the Weakest Link in Security - DevOps.com*. Opgeroepen op September 27, 2020, van DevOps.com: https://devops.com/iot-not-people-now-the-weakest-link-in-security/

Duc, A. N., & Chirumamilla, A. (2019). Identifying Security Risks of Digital Transformation - An Engineering Perspective. *Digital Transformation for a Sustainable Society in the 21st Century*, 682-693.

Ghadge, A., Weiß, M., Caldwell, N., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*, 223-240.

Janssen, M., & van der Voort, H. (2020). Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic. *International Journal of Information Management*, 1-7.

Nikolov, N., & Rudenko, O. (2012). IT Governance Approaches in SMEs: A Literature Review. 1-7.

Ning, H., & Liu, H. (2012). Cyber-Physical-Social Based Security Architecture for Future Internet of Things. *Advances in Internet of Things*, 1-7.

Pandey, S., Singh, R., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, 1-27.

PAS 555. (2013). *Cyber security risk - Governance and management - Specification.* London: The British Standards Institution.

Phlippen, S., Neuteboom, N., & Klene, N. (2020). *Invloed coronacrisis op Nederlandse economie.* Amsterdam: ABN Amro.

Ramdjan, A. (2020, March 27). *Logistieke uitdagingen tijdens COVID-19 crisis | PTV Blog*. Opgeroepen op October 14, 2020, van blog.ptvgroup.com: https://blog.ptvgroup.com/nl/transport-en-logistiek/covid-19-uitdagingen/

Rudenko, A. (2019). IT Governance Approaches in SMEs: A Literature Review. *Information Management*, 1–7. https://www.academia.edu/7759565/IT_Governance_Approaches_in_SMEs_A_Literature_Review

Saturno, M., Pertel, V., & Deschamps, F. (2017). Proposal of an automation solutions architecture for Industry 4.0. *24th International Conference on Production Research*, 1-7.

Schmidt, S. (2020, May 18). *5 lessen voor in de logistiek na de COVID-19 crisis | PTV Blog*. Opgeroepen op October 14, 2020, van blog.ptvgroup.com: https://blog.ptvgroup.com/nl/transport-en-logistiek/covid19-logistieke-lessen/

Somapa, S., Cools, M., & Dullaert, W. (2018). Characterizing supply chain visibility - a literature review. *The International Journal of Logistics Management 29*, 308-339.

Steinberg, G. (2020, June 11). *COVID-19: Why real-time visibility is a game changer for supply chains | EY - Global*. Opgeroepen op September 22, 2020, van EY: https://www.ey.com/en_gl/consulting/covid-19-why-real-time-visibility-is-a-game-changer-for-supply-chains

Tran, T., Childerhouse, P., & Deakins, E. (2016). Supply chain information sharing: challenges and risk mitigation strategies. *Journal of Manufacturing Technology Management*, 1102-1126.

Vervest, P., van Heck, E., & Preiss, K. (2008). *Smart Business Networks.* Rotterdam: SBNi.

Weill, P., & Ross, J. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. *International Journal of Electronic Government Research*, 63-68.

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure*

Protection, 4-11.

Winkelhaus, S., & Grosse, E. (2019). Logistics 4.0: a systematic review towards a new logistics system. *International Journal of Production Research*, 18-43.

APPENDIX 1 – INTERVIEWS WITH EXPERTS

Francesco Lelli

Questions:

We want to research whether businesses have to rethink their business model and have to think on the longer term before investing lots of money. Good research?

Depends on the company, because each company is unique. Some companies stick to a standard. You have to see how much of a structure it has to change. Bring expertise in house, hiring and rent are two biggest cost in a company. 80% of the budget.

Do you think Supply Chain Visibility is worth it for SMEs?

What if you could rent this business model? Like an outsourcing model, its more efficient. External solution. You are building a saas solution and offer this to a small company. Problem is that small companies don't have the knowledge of the saas solution. Think about how you can deliver this functionality to the small companies. For example the software as as solution. Don't look at just the adoption of giving a software.

Why it worked? It was not designed for Covid? Why additional visibility worked in Covid times. How does this works for the long term for medium sized companies. What are the benefits. New technology, how do I use it. How does it change my process? Understand who you are.

What are the main disadvantages of SCV?

Transparency foster competition is good, but price move towards an optimum. Consequently you have less margin when you have an optimum price.

Challenge in quality rate, competition foster too much to cost reduction which could lead to less quality. Margins is key.

Should we specify to a particular group e.g. SMEs

Should we specify in ocean freight, air freight. You want something relative special. You choose a company in a sector and choose a level of standard. So you are choosing for example a company that is specialized in a product with ocean freight.

Do you have experience, case studies about logistics companies that made such investments

You will find a lot of this in google scholar. Saas solution for new technology. Plenty of report in covid, search on that.

Joris Hulstijn

[Explanation of topic], what do you think about the topic?

The Netherlands is ahead in SCV. The idea was SCV is a problem, because the market is fragmented. The rate of IT in that sector is relatively low. EDI in 1990's only for larger companies. SCV usage it is based of the sector. Government role: role for regulation. Network problem. E.g if you have an iPhone but all your friends have an android.

How are we going to deliver this solution.

Initiative BPM and .. conclusion overhyped, research has been done.

Technology push. The general argument of SCV is that if you have a good SCV … Kuehne nagel has everything door to door. Once you have SCV, all the companies together have a SCV. Same standards for data and same network. All the members have SCV then. (port base, official system used by port of Rotterdam. Use this system for your case)

Impact of the pandemic -> Shift to e-commerce, delivery at home. How this pandemic will slow down or fastening this technology. Good thing about SCV there is a good combination possible with cybersecurity. Supply Chain Resilience is a very important topic. Heilding article. If they are dependent on eachother, it will be a risk.

Regulations: HS code; well known standard for goods description. Different in countries/regions.

Carol Ou

Q&A with Carol Ou

Does it require that small businesses rethink their business strategy?

Thus their alignment

Really depends on what the company wants. Fresh food from the store, our online system for example: Pick up the food in package in AH. Ask the consumer for information, logistics package, all this information should be gathered and the consumer. Why SCV change of Covid? Think about this question.

ITG is related to technology. **Try to defend which direction the ITG arrangement will change.**

What are the main disadvantages with regards to the business model?

Resistance will be the main disadvantages. You need to analyze BPI. People are reluctant to change towards the organization. Biggest problem in ITG. IT investment, why do you want to invest in one particular technology? Internal organizational debate.

Kenny Meesters

Explanation of paper

Challenge for you for a paper that adds a value, is to find a good research question. My question to you would be: what are you trying to prove? Uncertainty , hard to invest in long term solutions. Is that a fastening or slow down the innovation? The needs or success factor has changed, difference between big and small companies.

Are we doing this now because it is an opportunity, or you don't want to go backwards. Maybe the reasons are different. Now you go all in, because it is a must have.

Was a country like the Netherlands prepared for such a crisis?

Netherlands and Europe were not prepared for this crisis. Delft faculty TNL are working on disruptions in logistics on a daily basis. Even for the Brexit. Development countries, for them disruptions happen normally. They are used to disruptions. They have less dependencies. That's the problem with complex systems, every buffer is taken out because of efficiency. Are we able to rapidly respond to this.

What are the Risks of SCV?

Privacy, attacks, do we become dependent on it? Because what if the power doesn't work. The ability to deal with these consequences. Frederik Veneman. His thesis. In a crisis people can adapt, but time is limited to learn new things. Switch between, scale up or down or relocate resources. Use the things you normally do on a daily basis. Adapting is key.

What about RESILIENCE ?

How should logistics companies prepare for a possible rebound of the COVID-19 in your opinion? E.G. availability suppliers, agility. In many industries, supply chain visibility programs are aligned with disaster recovery plans (crisis management?)

APPENDIX 2 – EXTENDED CYBER SECURITY ANALYSIS

New technologies continue to change how organizations complete. Supply chain visibility (SCV) uses a lot of new technologies of the Industry 4.0, such as big data, cloud computing, artificial intelligence (AI), internet of things (IoT) and RFID and NFC sensors. This emerging trend is also called "logistics 4.0". According to Steinberg (2020) these technologies could reduce risks and costs, better alignment of supply with demand and an increase of speed and agility. The reliance of organizations in data and data processing is becoming more and more important (Duc & Chirumamilla, 2019). This could lead to new risks for the organizations, for example cybersecurity risks. Previous studies who identified supply chain risks have not dealt with the role of technologies related to Industry 4.0. The new possible cybersecurity risks of SCV for SME's within the Dutch logistic and transport sector will be discussed in this section. Furthermore, the risks of a connected supply chain will be analyzed. Finally, possible solutions to mitigate these cybersecurity risks will be provided.

IDENTIFYING CYBERSECURITY RISKS AND METHODS OF CYBER-ATTACKS OF LOGISTICS 4.0 TECHNOLOGIES

Industry 4.0 is an umbrella term for technologies that are used for automation and data exchange in the manufacturing sector. Figure 1 shows an overview of the nine technological pillars of Industry 4.0. Logistics 4.0 operates under the same principles as Industry 4.0. However, cloud computing, IoT and RFID technologies are mostly used within logistics 4.0. Implementing these new technologies involves risks and possible direct cyber-attacks.

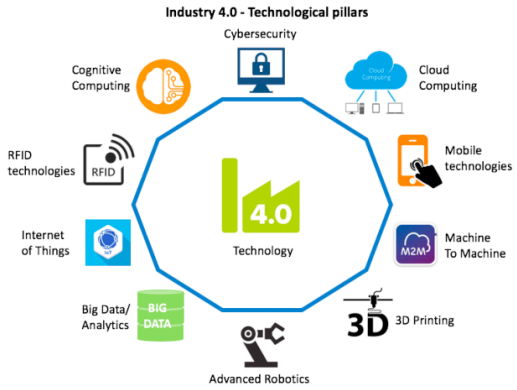

Figure 1 Technologies Industry 4.0 (Saturno, Pertel, & Deschamps, 2017)

First of all, cloud storage is one of the technologies of the logistics 4.0 that is used within the SCV. Organizations are now relying on cloud computing for the storage, processing and analysis of the data from the SCV activities. Cloud computing has a lot of benefits for organizations, for instance affordable costs and easy-to-use. However, the downside of cloud computing is that there can be serious threats to the security of their data. Typical risks of cloud computing are: *Limited control of services, a leak of data, securing API layers* (Duc & Chirumamilla, 2019).

To gather all the information within the supply chain, IoT is used to provide the SCV of the organization. Specifically, rhe use of sensors to track products as part of IoT is relevant for SCV. All the devices, gateways and servers that are connected to each other. As a result of this, the concerns on the security of the IoT within the SCV should be considered. The use of more devices, gateways and servers are new possibilities for cybercriminals. To analyze the cybersecurity risks, a classification of the risks of IoT has been stated. The different cybersecurity risks that companies face consist mostly specific for SCV and are divided into security risks regarding Confidentiality and integrity. As SCV is dependent on reliable data, integrity is the most important aspect of security within the SCV domain. The main risks that derive from the use of cybersecurity are Partners trust and information theft (Confidentiality), product specification fraud, poor protection in cargo transit, unauthorized access and counterfeit products (Integrity).

However, *a fully integrated and connected supply chain is as strong as its weakest link*. Because all devices, gateways and servers, within a chain, are connected with each other. This increases security risks due the wide environments these logistics 4.0 applications touch (Dingee, 2019). When all actors within a supply chain are connected, the possible cybersecurity risks will increase and embrace further in the network (Pandey, Singh, Gunasekaran, & Kaushik, 2020). According to Pandey et al. (2020) the following cybersecurity risks will occur in a connected supply chain; *Partners trust, product specification fraud, poor protection of cargo in transit, unauthorized access, information theft and counterfeit products.* This study will analyze above risks, which occur because of the previous mentioned risks and direct attacks of the new logistics 4.0 technologies. These risks will be analyzed in the risk assessment in table 1.

RISK ASSESSMENT

It is important for SMEs that the possible cybersecurity risks of a connected supply chain are clearly mapped out. For this reason, a risk assessment has been made to understand the impact and the likelihood of the cybersecurity risks. Every cybersecurity risk has been analyzed on the possible impact and likelihood that the cybersecurity risk will occur. This has led to a score per risks, which eventually will be categorized into a low, medium or high risk level for the organization. The results of the risk assessment are shown in table 1. The motivation of the choices are set out below.

Table 1 Risk Assessment

	Technologies	**Risks**	**Security concerns**	**Likelihood (1-5)**	**Impact (1-5)**	**Overall Risk (1-25)**	**Risk Level***
R1	Weakest link	Partners trust	Confidentiality	4	5	20	High
R2	IoT	Product specification fraud	Integrity	3	4	12	Medium
R3	IoT	Poor protection of cargo in transit	Integrity	2	5	10	Medium
R4	IoT, CC, RFID	Unauthorized access	Integrity	3	3 (internal /external)	9	Medium
R5	Weakest link, IoT	Information theft	Confidentiality	2	4	8	Low
R6	Weakest link	Counterfeit products	Integrity	2	2	4	Low

*Low 1-8, medium 9-17 and high 18-25

Motivation of the choices

As a result of the risk assessment, it can be concluded that the trust in the partners within the supply chain can be seen as the highest risk for the SCV of SME's. In SCV, every partner within the supply chain network is linked with each other. A weak link within the supply chain could lead to some serious problems for an organization. It follows that if one of the partners has a weak spot within their cybersecurity, the information of the whole supply chain could be stolen. The likelihood that this security concern could happen is high, because there are multiple partners within the supply chain that could have a security problem. Since SCV ensures a lot of real time information about the supply chain, this could have a serious impact on a SME. The security concern of R1 is the confidentiality of the information stored within the supply chain. A successful attack of a cybercriminal could affect the disclosure of important information, which should only be available to the authorized individuals. Thus, due to a high likelihood and high impact of R1, a high risk level is assigned to R1.

Furthermore, other typical supply chain visibility risks within the logistics and transportation sector are product specification fraud (R2) and poor protection of cargo in transit (R3). These risks could have a high impact on the supply chain of a specific sector, because it could lead to unreliable information about the product or possible security problems of the cargo. According to Clark & Wilson (1987), a major goal of commercial data processing is to ensure integrity of data to prevent fraud and errors. The sensitive information of the organizations should not be modified or destruct in such a way that assets or information are lost or corrupted. As a result of the SCV, there is a lot of information available about the products within the supply chain. This occurs in new security risks that could infringe the integrity of the information. The impact of possible attacks on the integrity of the products or the physical products could have a huge impact on the organizations. The general cybersecurity risk of an unauthorized user access (R4) could infringe the integrity as well. An unauthorized user who gets access to the information could be an internal or external individual. In both situations, the unauthorized user has access to sensitive information of the organizations. Since the low likelihood that the R2, R3 and R4 will occur, a medium risk level has been given. However, SME's should take these risks into account because of the possible high impact level. The last two risks are information theft (R5) and counterfeit products (R6), which could have an impact on the confidentiality (R5) and integrity (R6) of the information. These are low level risks, because of the low impact and likelihood that these risks will occur.

SOLUTIONS

The identified risks occur within the whole supply chain. The supply chain can be divided in three sectors: upstream, focal firm and, downstream. In each sector different risks apply. In the upstream supply risks, in the focal firm operational risks and downstream demand risks (Pandey, Singh, Gunasekaran, & Kaushik, 2020). For example, partner risk (R1) occurs in the upstream or downstream of a supply chain. Hence, this risk is a supply- and demand risk. However, unauthorized access (R4) can occur throughout the whole supply chain. Thus, for each sector different risk mitigation strategies apply. Furthermore, risk mitigation strategies are divided in three phases. The three phases are, pre-attack, trans-attack and post-attack. In addition, "the risk mitigation typically depends on the type of cyber-attack, impact of the attack and resilience of the organization" according to Ghadge et al. (2020, p. 11). Risk mitigation measures need requirements. Ning & Liu (2012) suggest that the security requirements elements include the CIA (Confidentiality, Integrity and, Availability Triad, authority, non-repudiation, and privacy. However, according to the PAS 555 (2013) it is important to "emphasize that technical measures alone are not enough, effective outcomes encompass people and behaviors, physical and equipment security, as well as governance, leadership and culture". From this information the measures for mitigating cyber risks are determined, see table 2.

Table 2 Measures for mitigating cyber risks

	Risks	**Cyber security measures for mitigation**
R1	Partners trust	Network audit (Windelberg, 2016)
		Supplier audit (Windelberg, 2016)
		Confidentiality agreements (Tran, Childerhouse, & Deakins, 2016)
R2	Product specification fraud	Event logging
R3	Poor protection of cargo in transit	Vulnerability checks
		Monitor network traffic
R4	Unauthorized access	Access control
		Event logging
R5	Information theft	Authentication processes
R6	Counterfeit products	Information sharing

In the post-attack phase the risk mitigation strategy has to focus on prevention of the potential risks. The trust in the partners (R1) within the supply chain can be seen as the highest risk for the SCV of SME's. A weak link within the supply chain could lead to some serious problems for an organization. It follows that if one of the partners has a weak spot within their cybersecurity, the information of the whole supply chain could be stolen. Hence, trust is a crucial factor within a supply chain. High trust and optimal information exchange between organizations within a supply chain are hard to achieve (Birkel & Hartmann, 2019). To validate the cybersecurity of potential partners, network audit, supplier audit and confidentiality agreements can be executed (Windelberg, 2016) (Tran, Childerhouse, & Deakins,

2016). Secondly, product specification fraud (R2) and poor protection of cargo in transit (R3) are potential risks. To prevent or mitigate these risks event logging, vulnerability checks and monitoring network traffic helps. Unauthorized access (R4), information theft (R5) and counterfeit products (R6) can be caused by various attacks. For example, DoS attacks, spoofing, phishing, etc. Because of the various types of attacks, it is difficult to have a cyber security measure for every attack type. However, to mitigate these potential attacks access control, event logging, authentication processes and information sharing can contribute. Lastly, it is important that employees have continued education on the potential cyber security risks. Employees can then prevent potential attacks and recognize them at an early stage.

In the trans-attack phase the risk mitigation strategy have to focus on the anticipation of the attack. In this phase an organization has to identify quickly attacks and make decisions to minimize the potential damage. Monitoring the network traffic and event logging helps to identify an attack in an early stage. In the post-attack phase the risk mitigation strategy have to focus on recovery and the resilience of the organization. According the PAS 555 standard (2013) resilience is "the ability of assets, networks and systems to anticipate, absorb, adapt to and/or recover from disruptive event or incident". There are two kinds of resilience: business resilience and resilience preparedness. Business resilience focuses on the degree of resilience and risk appetite. While resilience preparedness focuses on anticipation, assessment, prevention and preparation for recovery after an incident (PAS 555, 2013). Cyber security measures that improve the resilience are recovery and back producers (Windelberg, 2016).

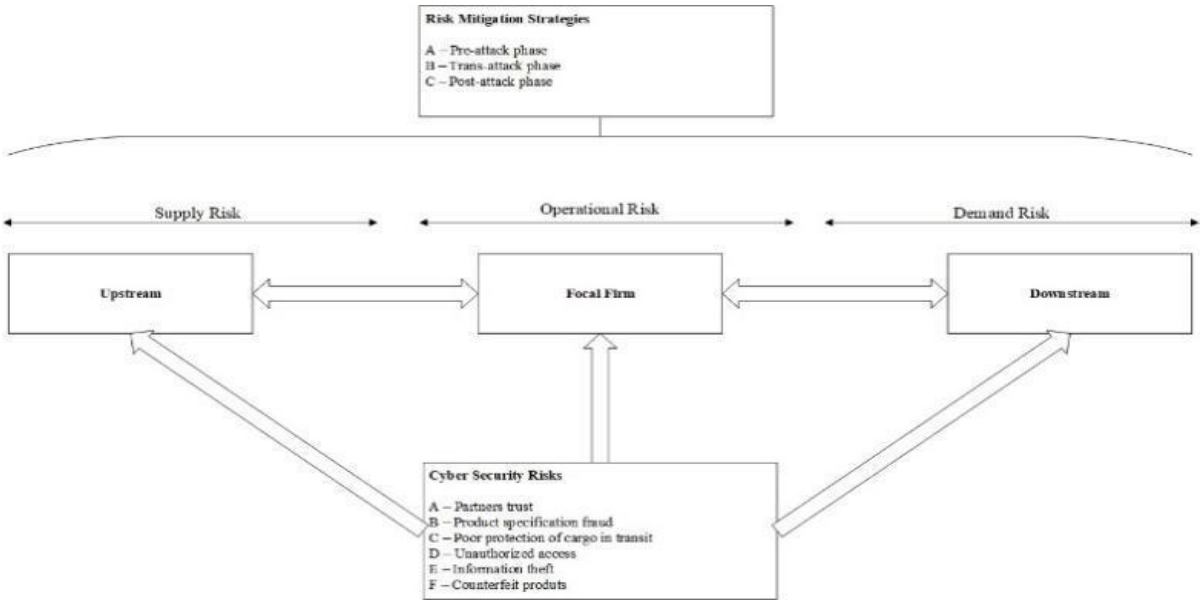

Figure 2 Adjusted framework for cyber security risks and mitigation strategies (Pandey, Singh, Gunasekaran, & Kaushik, 2020)

CONCLUSION

In this report, we described the risks and how those risks can be mitigated. However, as with most risk management situations, after implementing these measures there will still be risks that Dutch SMEs can face when implementing SCV within their organization. Supply chain visibility is still a fairly new technology which means that there probably will be more innovations in the future, which will bring new risks with them.

As we look at the current risks analysis however, we can state that most SMEs within the Netherlands will have a baseline of cybersecurity measurements that they can apply within their organization. The main factor that is not included in the risk assessment is the resilience of organizations. Besides implementing the measures we suggest, also like to advise companies that make use of SCV within their organization to test how fast they are "up and running" after an attack happens. While taking measurements are a good step forward, being resilient when a breach does happen remains critical. To tackle the fact that innovative technologies, new cybercrime possibilities and resilience of the organizations will remain a threat, we propose a situation in all companies who are involved in a supply chain in which SCV is adopted to do a cybersecurity assessment at least every six months. By assessing all the companies in the supply chain, there will be a helicopter view of the whole supply chain and if there are any companies who are especially vulnerable, it will show during this assessment. We suppose that this also could work preventively as companies would not want to be the weakest link within a supply chain.