UHASSELT

KNOWLEDGE IN ACTION

Faculty of Business Economics

Master of Management

Master's thesis

Risk management and supply chain vulnerability with focus on ICTs.

Aidah Nassali

Thesis presented in fulfillment of the requirements for the degree of Master of Management, specialization Business Process Management

SUPERVISOR :

Prof. dr. Koenraad VANHOOF

2019
2020

UHASSELT

KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

UHASSELT

KNOWLEDGE IN ACTION

Faculty of Business Economics

Master of Management

Master's thesis

Risk management and supply chain vulnerability with focus on ICTs.

Aidah Nassali

Thesis presented in fulfillment of the requirements for the degree of Master of Management, specialization Business Process Management

SUPERVISOR :

Prof. dr. Koenraad VANHOOF

DECLARATION

I declare that this study is my original work and to the best of my knowledge, it has not been published and/or submitted for any other degree award to any other university or institution of higher learning before.

Aidah Nassali
Reference no. 1848517

APPROVAL

This dissertation is submitted for examination with the approval of the following as institute supervisor: Mr. Vanhoof Koen

DEDICATION

I wish to dedicate my work to my parents: the late Mr. & Mrs. Musoke for the tireless support they gave my sisters and I as I was growing up. May their souls rest in eternal peace.

DISCLAIMER

This master thesis was written during the COVID-19 crisis in 2020. This global health crisis has had an impact on the (writing) process, the research activities and the research results that are at the basis of this thesis. There was an impact on the data collection. The field survey could not be done, planned interviews did not take place due to mandatory stay at home government orders. That is why the researcher based this study on already existing literature, research, and previous participant observation.

PREFACE:

I wish to acknowledge my supervisor: Mr. Vanhoof Koen for the professional time he has given me during my study. I also recognize the rest of my lecturers at the University of Hasselt including Ms. Mieke Jans.

To my Hasselt University colleagues: I do want to thank you for your wonderful cooperation. Sharing my thoughts about my work with you has always been beneficial. The research was difficult due to the fact that there is a mandatory stay at home order as a result of COVID-19 the global pandemic sweeping across the globe to date. It has not been easy to use some of the methodology I had anticipated as I was beginning my research end of last year 2019. All in all even when this lock down period of uncertainty took a tall on our wellbeing you still got me motivated.

Others that I cannot underrate are my lovely sisters Jane and Doddie who have played a big role in ensuring that this study is completed in a timely manner; not to forget my guardian Ms. Christine Ssali who has given me emotional support to make my work a success. To you all I say thank you.

ABSTRUCT

This study examined risk management and supply chain vulnerability with emphasis on ICTs. It was prompted by higher uncertainty / risk increases, some of which have resulted in massive losses for companies around the world. Over the years, many companies have steadily evolved from the tradition of competing as business to business, the growing trend to date is that there are global forces leading to integrated supply chains to replace the traditional standard and aim for more efficient trade. This has resulted in greater reliance on ICT to sustain these supply chains, where in certain cases it has adversely affected companies. With this research study, the goal was to determine, why ICTs make the supply chain vulnerable, which ICT areas in particular and what mitigation measures should be put in place to mitigate risks. The researcher used secondary data analysis and participant observation to carry out the study. Face to face interviews were to also be carried out but due to the mandatory COVID 19 lockdown that was not possible. Information was examined through reading the different journals, books, articles and other study material that have been done around this field of study. Observation in the different companies the researcher has worked from in Limburg, Belgium was also used to understand the theories that had been read. The researcher found that much as there are many mitigation measures of risk in the supply chain expressed by different researchers, the company investigated did not fully utilize them. The researcher concluded that despite the existence of risk management approaches companies were not mainly focusing on them but, rather concentrating on continuous global expansion and profit making. Interventions should therefore be put on the risk management implementation through well planned policies, structures and well trained personnel in the different parts of the supply chain in order to coordinate, make more realistic forecasts that enable early detection of problems then provide most probable solutions to reduce the vulnerability.

Table of content

Table of Figures

CHAPTER 1:

1.1 Introduction

To date, the supply chain continues to be a fascinating topic for most of the businesses across the globe. It has been embraced by different companies ranging from small ones to multinational ones with the aim of creating business success. While some already have well established structures to embrace the trend others, are still finding ways of how suitable they can fit in these chains for better market leverage. Companies need to develop organizational skills, work with their suppliers and consumers to face competition by internationalization and globalization of the markets. Supply chain management has therefore become increasingly prominent (Chen & Paulraj, 2004).This study examined risk management and supply chain vulnerability with focus on the different forms of Information communication and technology (ICTs). In this chapter, the researcher gives the background of the study, the statement of the problem, the study objectives and the research questions as well as the significance of the study. This chapter also provides definition of terms used, conceptual framework and the study justification of the study.

1.2 Background of the study.

In most parts of the world, governments have put an emphasis on companies to develop strong supply chains to sustain trade (Gupta, Dasgupta, & Gupta, 2008). A high investment in information communication and technology (ICT) has been made to archive this, which involves modern technology such as electronic mail, video conferencing, facsimile, and telephone conferences (Vu, 2005). ICT correspondence deals with digital data storage, retrieval, and manipulation. ICT communication uses ICT devices to link corporations, individuals and organizations. This pattern, however, has faced several risks that need high investment to make it sustainable exposing some businesses to bankruptcy. For instance, the failure of Blackberry mobile phone company to adopt to the new technology of quick touch screen mobile phones such as iPhone led to its collapse after a huge investment of over 50 million dollars in 2011. It did not adequately improve its ICT to respond to the changes within its supply chain. Hence making it more of a shadow company to date (Youssef & Haj Youssef, 2013).

1.2.1 Historical background

In the early years, trade can be traced back roughly 2.6 million years ago during the Stone Age; stone tools were used for hunting during this era, and people were self-sufficient. They traveled in search of food, shelter and trading was carried out on a relatively smaller scale, within small communities for short distances. At that time, there was no idea of agriculture and merchants (Palaeolithic stage of the stone age) (Chavaillon, Chavaillon , Hours, & Piperno, 1979). The first long distance trade began between 17000BC and 900BC, and obsidian was used as currency before metals were brought on board in Mediterranean areas (Merrick & Brown, 1984) .

By 900 BC, agriculture had commenced in fixed domestic areas. Planting of crops, as well as animal rearing begun and had become the norm (Marshall, 1990). This led to neighborhood development in fixed homesteads. With agriculture and new farming techniques, there was more food surplus which the different communities used to sell among each other for other valuable goods in form of barter System (Marsall, Barthelme, & Stewart, 1984). With time, trade spread across different communities where there was not only surplus food being exchanged but also agricultural tools (tools made from stone) and trades of crafts (Knapp, 2013). Given the growth of these activities there came into being a new social class of merchants. These would move for many miles on foot and using animals such as camels, carriages with dogs and horses to trade with other groups (Feldman & Sauvage, 2010). In that time, commodities being traded were standardized in the form of livestock, salt, metal, oil, textile and rare stones.

People begun populating other parts of the world over the next few centuries including Indus Valley, Jordan, Ireland, Anatolia, Scotland, North America, Nigeria, Turkey, Norway, Italy, Europe, Egypt and so on. Ornaments (Gold & Copper) came into being and were in immense demand all over the world (Feldman & Sauvage, 2010). On the basis of the inhabitant zone, these cultural groups of people began accommodating areas on the basis of the availability of natural resources (Katz, 2020). New objects were made with an aesthetic value and not just a function.

With the gradual evolution of trade between communities to communities, then cities to cities, countries to countries and continents to continents it can no be underestimated that strong organizations such as the general agreement of terms of trade ("WTO | Understanding the WTO - The GATT Years," n.d.) that was revised to world trade organization
("WTO | Understanding the WTO - The GATT Years," n.d.) have facilitated such connections by forming coalitions and playing a key role in developing the supply chains that we are evidencing to date.

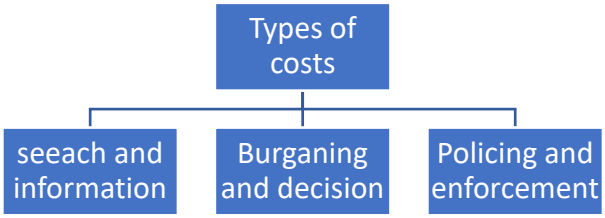
1.2.2 Theoretical background.

Although there are many theories that can be used to define the supply chain, this study will mainly focus on three theories which are the Transaction theory, System theory and Network theory which is the main guiding theory in this study.

1.2.2.1 Transaction theory.

Transaction theory may be used to identify vulnerability at every stage of the supply chain in order to be able to manage risks appropriately. Transaction theory defines governance structures as based on the net effects of internal and external transactions, rather than as external contractual ties (i.e. with shareholders) (Bahli & Rivard, 2003). The early studies of Dow, (1987) had given little attention to internal operations of organizations. External factors were emphasized and some of the transaction costs were for research and information, bargaining and decision and policing and enforcement (Pitelis & Pseiridis, 1999).

Figure 1:Transaction theory external costs



Source: Transaction costs versas resource value (Pitelis & Pseiridis, 1999)

Basing on the theory, the above figure shows that external transactions contain different types of costs which will accumulate especially in the search and information for new suppliers, bargaining and decision to buy components, policing and enforcement to monitor the quality of products bought. This approach as we shall further analyze creates little room for trust among key stakeholders of businesses (Hindmoor, 1998) and yet such trust is needed to help integrate the supply chain and reduce its vulnerability.

While on the other side, Williamson (1986) further expanded the application of transaction theory by highlighting its role in vertical integration and trust in organizations. Within the organization the following was the focus:-

- Asset specificity: Amount the manager will gain personally.
- Certainty: Otherwise being caught.
- Frequency: Endemic nature of such action within corporate culture.

The degree of influence of the three variables contributes to an objective assessment of how much monitoring and control senior management require to run businesses. Opportunistic conduct may have serious effects on corporate finance and policy, thereby restricting future investors. Therefore, companies structure themselves to mitigate as much as possible the effect of bounded rationality and opportunism (Silverstein, 2020) hence reducing supply chain vulnerability and enhancing risk management approaches.

Given such elements of the transaction theory, there is evidence that most of them affect the supply chain positively or negatively. Whether we look at the supply chain, as a network or as an integrated mechanism, the transaction costs describe the vertical relation and convergence of different elements of the organizational supply chain, from second and first tier suppliers and from first tier suppliers to customers. Transaction theory applies in four dimensions to the organizational supply chain: commitment, control, issue and gain. Effort to "develop and sustain the relationship" with suppliers; cost of "monitoring supplier performance;" problem solving in business relationships; and supplier involvement in "opportunistic conduct"(Ghauri & Hassan, 2014) .

In relation to ICTs, while transaction theory focuses on people's actions to influence costs through controlling, close supervision and policing to maximize efficiency (Williamson, 1986) the digital era that is prevailing today puts more emphasis on management of supply chain integrating systems. Such systems include but not limited to enterprise resource planning, marketing online platforms, online banking all of which switch the focus of risk management from analyzing the safety of individual transactions to a more holistic approach of managing the risk of the whole supply chain from the source to the ultimate end user (Zsidisin & Henke, 2019). Therefore it can be argued that much as transaction theory over years dating back from the analogue era is the core of managing risk especially within organizations the digital era requires a much broader risk management approach as will be discussed in the next chapters.

1.2.2.2 Network theory

Network theory is another relevant one to risk management and supply chain vulnerability regardless of which type of business it may be. Network perspective – also described in the literature as network theory (K. Lavassani, Movahedi, & Kumar, 2008) – is mainly concerned with value generation through inter-organizational relations. From this point of view, the Network viewpoint has resource-based similarities. Whereas the resource-based view focuses on dyadic relationships, network viewpoint also takes multi-party relationships into consideration (McNichols, Brennan, & Middel, 2006). When the network increases in complexity, variety and diversity, so does its efficacy (Child & Mansfield, 1972). The organization, however, is expanding the supply chain networks to include more diverse professional and geographical areas.

The networks perspective has been used in particular industries or countries for business and global supply chain studies (K. M. Lavassani & Movahedi, 2010a). With such a perspective stronger collaborations have been established throughout supply chains although at the same time challenges of supply chain management can not be ruled out due to the varied factors such as geographical locations of the players. Markets are seen in the network theory as a web of relationships between various entities including, for example, customers , suppliers, or manufacturers (Coviello & Munro, 1995). Companies that are now participating in networks are considered to gain profit, not through achieving their own goals, but through the network's business relationships and alliances (Gulati, Nohria, & Zaheer, 2000). This theory therefore supports the importance of networking within the supply chain but once not appropriately applied may lead to supply chain vulnerability and the undermining of risk management across the chain.

1.2.2.3 Systems theory

Systems theory having been considered in this study also plays a big role in highlighting the importance of coordination of activities, resources and human capital throughout the supply chain.

Von Bertalanffy (1950) made a seminal contribution during the primary study of the advancement of systems theory. The contributions Bertalanffy (1950) made to scientific research were mainly from the perspective of physics and biology. For example, in his paper published in 1950 – while he was a professor at the University of Ottawa – Bertalanffy (1950) analyzed the view of the open system of living organisms in contract to them being in closed systems.

Before the 1950s his research was mostly from the perspective of biology, which led to the development of the theory of the organism system.
He suggested that the living organisms were highly organized with minimum interruptions and that this principle should further be investigated scientifically to the benefit of other systems. His research, after the 1950s, was mainly about the advancement of science's methods, which contributed to the creation of general system theory. Bertalanffy (1950) questioned classical modeling, based on a quantitative view of the processes, arguing that the time factor affects these open systems. To understand these open systems, therefore, a dynamic view of the systems is required (K. M. Lavassani & Movahedi, 2010b).

The early system theory was implemented in supply chain management and especially in the logistics context. (Gripsrud, Jahre, & Persson, 2006). They claim that during the time from the 1950s-1970s the neoclassical economic theories were dominant. The emphasis during this time was one "absolute cost" and one "trade-off". However, since the 1970s the system theory has been dominant in understanding the context and operation of the supply chain of organizations. The post 1970s era itself is witnessing a shift in focus. Although the cost-service balance as well as trade-offs were the subject of attention until 1985, the theory's emphasis was changed around 1985 to explain efficiencies and process function until to date. Interrelations exist between all elements and constitute a society (Manning,1967). it is with no doubt that under rating such system theory approaches to management of supply chain can easily render it vulnerable hence increasing risks especially in this era of technology.

1.3 Conceptual Background

This study was guided by two concepts: Risk management and supply chain vulnerability with focus on ICTs. These concepts have a range of definitions depending on the source and perception of people as a whole. Before going into the details of these two concepts it is important that we familiarize ourselves with what risk actually is and how it all begun over years.

Risk is a multi-dimensional construct in which a single concept may not be sufficient in all circumstances (Zsidisin, 2003). The word may derive from the early Italian word Risicare (Bernstein, 1996), the Arabic word risq, or the Greek word risicum (Norrman & Lindroth, 2004). Different people also have different perception of risk depending on their view on risk.

Historically, the risk study can be traced back to the early 17th century when famous mathematicians like Blaise Pascale and Pierre de Fermat (Devlin, 2010) tried to apply mathematics to gambling. During this study probabilities were applied to estimate likelihood of occurrences at that time. However, views of risk have changed tremendously over the years especially with advancement in technology and movement to globalization (Khan & Burnes, 2007). The actions we do dare to take, which depend on how free we are, guide us in making choices and, are what the story of risk is all about (Bernstein, 1996). The value of preference is explicit in this definition and the notion of negative and positive aspects of risk is implied. While the negative connotation of risk permeates most managers' thoughts and feelings (March & Shapira, 1987), some scholars emphasize the dichotomy of risk (Khan & Burnes, 2007).
However, once again the negative effects caused mainly by technological progress sometimes outweigh the positive when it comes to an organization's risk perspective (March & Shapira, 1987).

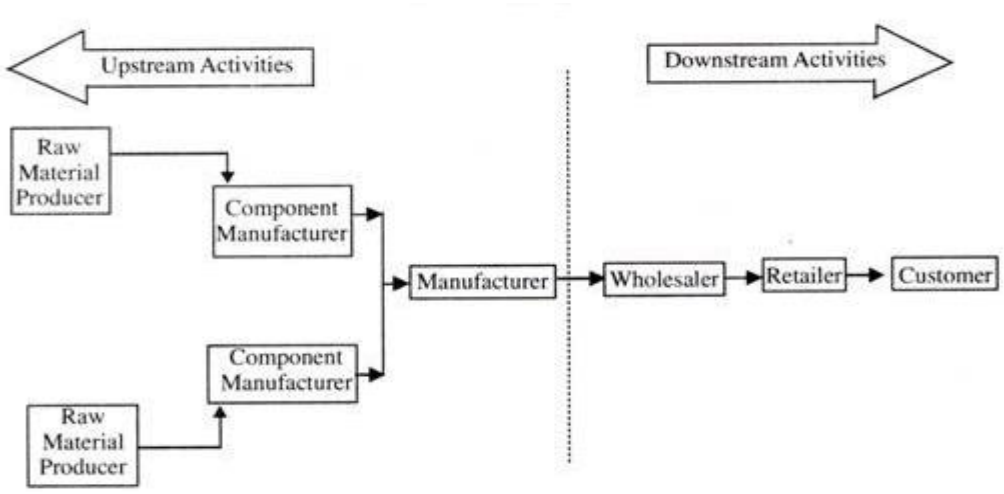
Basing on the above, It can be argued that knowing the mere meaning of risk is not sufficient on its own in solving the impact that it creates in today's world. That is why this study further explains risk management in order to be able to form a good basis in mitigating supply chain vulnerability and drive organizations' prosperity.

Risk management is the culture, processes, and structures aimed at efficiency (Stanton & Webster, 2014). Managing future risks and adverse effects (Kleindorfer & Saad, 2005). In decision making and risk management procedures, a person's risk tendency plays a fundamental role (Rahman & Kumaraswamy, 2002).

However, much as there are different risk management terms, researchers appear to agree that risk management requires risk mitigation practices and acts. Risk described in the Supply Chain is as "the management of the supply chain risk through collaboration or coordination among supply chain partners to ensure profitability and continuity" (Tang, 2006).

A supply chain is the flow of materials and information upstream from the source then downstream towards the ultimate user or customer (Lysons & Farrington, 2006).

Figure 2: Typical supply chain.



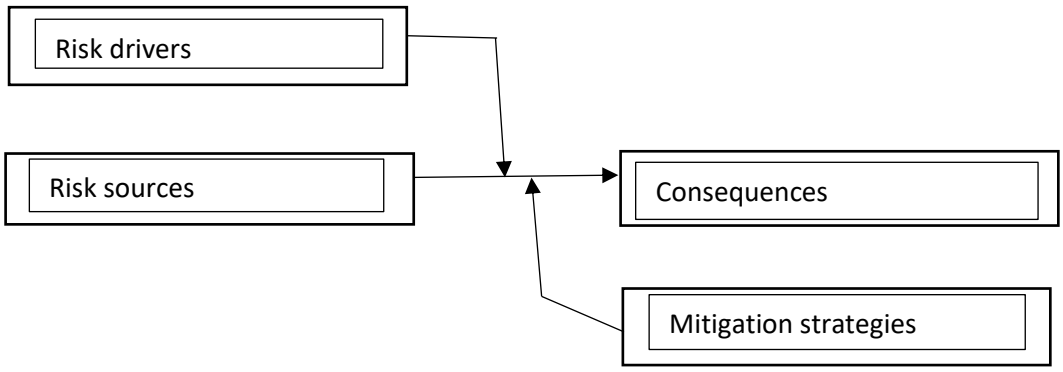
Source: The purchasing and supply chain management (Lysons & Farrington, 2006)

"Supply chain risk management is to collaborate with partners in the supply chain, apply risk management process tools to deal with risks and uncertainties caused by, or impacted on logistics related activities or resources" (Norrman & Lindroth, 2004).

To date, supply chain risk management suffers from the lack of a clear and adequate quantitative measure for supply chain risk that respects the characteristics of modern supply chains" (Heckmann, Comes, & Nickel, 2015). And, because of that some researchers have identified different criteria through which risks in the supply chain can be identified.

Some of these criteria include the four relevant risk constructs;- Supply chain risk sources, supply chain risk drivers, supply chain risk consequences and supply chain risk mitigation strategies (Jüttner, Peck, & Christopher, 2003).

Figure 3: The four risk constructs in the supply chain.



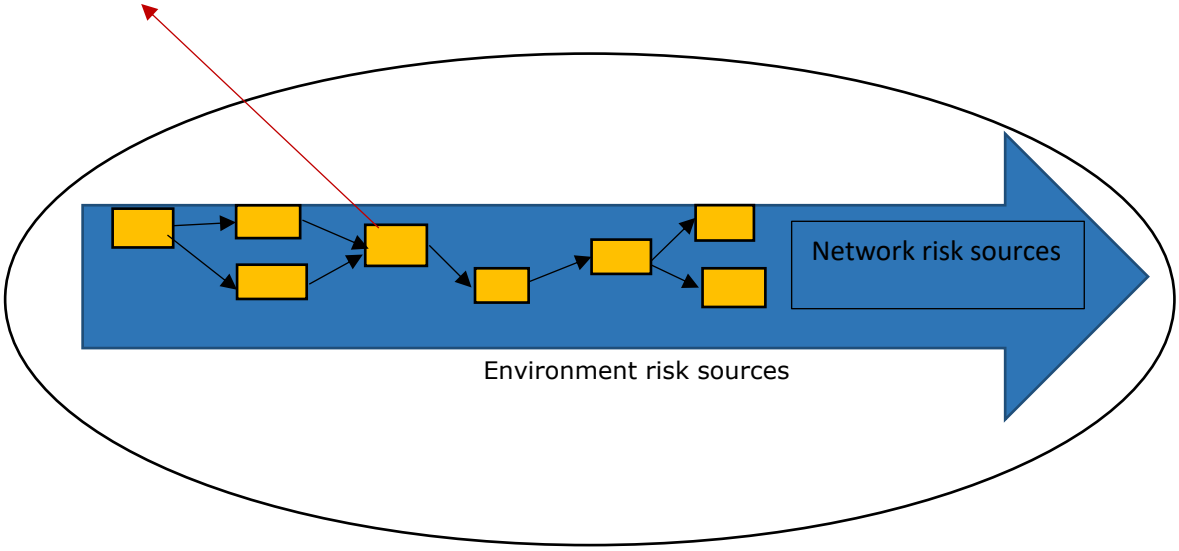
Source: Basic construct of SCRM (Jüttner et al., 2003).

Risks are further distinguished within the environment, supply and demand on one hand and sources of risk to process and control on the other. Economic risks are external to supply chains, and supply and demand risks are internal.

Her description of sources of environmental risk involves external uncertainty including financial, economic, and social uncertainties (Jüttner, 2005).

Ponis (2010) categorizes risk in form of organizational risk source, network risk sources and environmental risk sources.

Figure 4: Categories of risk in the supply chain network.



Source: Managing risk in virtual enterprise network (Ponis, 2010).

Supply risk is the transportation or significant and/or disappointing inbound goods and services failures (Zsidisin, 2003). While Svensson (2002) describes the risk of demand associated with outbound logistics flow. Apparently these two factors intersect as the risk source from the environment where supply and demand risk is the norm.

Risk sources can be classified according to the flow of supply chain products, funds and information. The way these flows are organized in turn will provide another source of risk. Four risk factors are then identified: physical risk, financial risk, knowledge risk and organizational risk (Waters, 2011).

Norrman and Lindroth (2004) claim that only taking business risks (e.g. political, legal, currency) is not appropriate when the supply chain prospect is of significant interest. They also note the value of a holistic view of chain partners, and concentrate more attention on operational logistics and supply chain management. Operational events (e.g. truck crashes) have a greater chance and less effects, while operational disasters (e.g. earthquakes) are vice versa. Authors argue that strategic risks are unknown, and thus difficult to resolve.

Jüttner et al. (2003) describes supply chain vulnerability as the propensity of risk sources and risk drivers to outweigh risk-mitigating strategies, thus causing adverse supply chain consequences and jeopardizing the supply chain's ability to effectively serve the end customer market.

Information communication and technology (ICT) is the digital processing and utilization of information by the use of electronic computers. It comprises the storage, retrieval, conversion and transmission of information. (Hayes & Whitebread, 2006). ICTs (information and communications technology – or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. ICTs are often spoken of in a particular context, such as ICTs in education, health care, or libraries. The term ICT is widely used as a synonym for computers and computer networks, although now it also includes other technology such as television and telephones in the delivery of knowledge (Hayes & Whitebread, 2006).

It is with no doubt that the reliance on ICT global supply has led to stronger economies due to the speed and efficiency through which businesses are being carried out. However this success has been accompanied by supply chain vulnerability that has led to high risks some of which have materialized leading to supply chain disruptions, great loses hence necessitating much investment in risk management (Zhao, Liang, & Zhao, 2011).

1.4 Contextual background

Limburg is one of the main logistics hot spots in the heart of Europe. It has been of great interest for this study due to the fact that it is strategically located east of Antwerp (80km) which serves as a gate way to Europe and the rest of the world.
Limburg is a province found in the North east of Belgium in the Flanders part of the country where Dutch is the main language. It sits to the west of the Meuse River. South of it is the Wallonia province of Liege, with which it also has historical ties. To the North is the Limburg the Netherlands province with which they border river Meuse. Then in the west is Flemish Brabant. Limburg Province has an area of 2,427 km (937 sq mi) consisting of three districts with 44 municipalities. Among these municipalities are the present capital Hasselt, Sint-Truiden, Genk and Tongeren, the province's only Roman city, and considered Belgium's oldest city. As of January 2019, the population of Limburg was 874.048 (Knippenberg & Markusse, 2012). The multi-modal access (by road , rail, water and air) and the availability of cost-effective support services (transportation, customs, ICT, logistics infrastructure and skilled workers) make Limburg a logistics hotspot. It cannot be under estimated that modern technology serves as a gist to keep this network of sectors enable the supply chain a success.

Many international companies such as Nike already invested in Limburg and Antwerp through global and European distribution centers or their European distribution operations outsourced to one of the main logistics players. That, coupled with the proximity of large European hubs such as TNT in Liege and UPS in Cologne, is why Cushman & Wakefield places Limburg at the top of the list of logistical hotspots until at least 2019 https://www.locateinlimburg.be/en/key-sectors. So given the nature of its businesses and proximity Limburg plays a big role in the global supply chain and has a some examples of players whose vulnerability has been witnessed and hence calls for more attention on risk management.

1.5 Statement of the problem

The continuous collaboration among businesses that have been established has created strong supply chains. As a result, there has been growth of small, medium and multinational companies such as Nike which doubled its profits and registered 7% increased sales in 2019 (Jiang, 2019). Other companies that have been successful include Ageas, KCB bank, Proximus group. One of the most notable areas that these companies have been characterized with is the huge investment in is ICT. Some of these popular ICT investments are in form of ERP systems such as SAP Hana, Sage Intacct, Oracle, IQMS, media communication, marketing among others. This has resulted in increased online sales, trace and tracking of shipments within the supply chain, modern storage facilities that enable quick replenishment of stock, online banking, teleworking the list is endless.

Although success of the supply chain systems integration has been noted in the different companies across Limburg there are also challenges that have come along in managing risk and supply chain vulnerability.
With that short background, it is evident that such global trends of the Supply chain integration have resulted in supply chains that are more vulnerable to disruption, leading to an increasing need to invest in risk management. Without risk management, supply chain vulnerability may result in greater impact of disruptions resulting in high costs and failure to meet customer demand hence collapse of businesses (Zsidisin & Henke, 2019).

1.6 General objectives

This study intended to examine risk management and supply chain vulnerability with focus in ICTs.

1.6.1 Specific objectives

This study aimed to achieve the following:-

1. To access which ICT areas make the supply chain vulnerable.
2. To examine why ICTs make the supply chain vulnerable.
3. To emphasize what should be done to mitigate supply chain vulnerability with focus on ICTs.

1.7 Research Questions

1. Why do ICTs make the supply chain vulnerable?
2. Which ICT areas make the supply chain vulnerable?
3. What should be done to mitigate supply chain vulnerability with focus on ICTs?

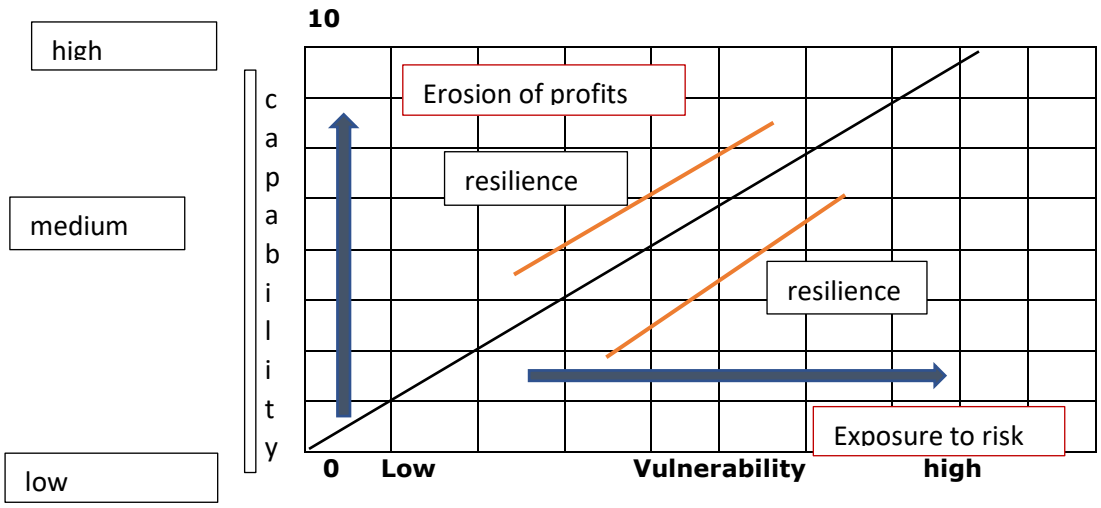
1.8 Methodology

The research was to be conducted using secondary data, literature review, participant observation and interviews. But, due to COVID-19 stay at home orders some of these methods could not be fully applied especially interviews. That is why the researcher based the study findings on already existing literature, research studies and earlier participant observation.

1.9 The conceptual framework.

The conceptual framework clearly links the independent and dependent variables as shown below. The Independent Variable (IV) which is supply chain vulnerability demonstrates the different levels of risk management capability which would be required control. (DV).

Figure 5: Conceptual framework



Source: Pettit, Fixsel and Croxton, 2010.

From figure 5 it can be seen that the higher the vulnerability of the supply chain the more risky it becomes for the business at hand, resulting in a push for more investment in risk management capability. It should be noted that companies which go to extreme investment in risk management capability end up losing more profits instead. Therefore, a balance has to be done between the risk or vulnerability and ways of managing capability to attain appropriate resilience and retain realistic profits.

1.10 Significance of the study.

The research was undertaken to examine risk management and supply chain vulnerability with focus on ICTs. It is anticipated that the focus of this study will contribute to the already existing research on ways of improving the timely identification of the vulnerability of the supply chain and the different ways through which risk can be managed. The in-depth discussion of what the different researchers in this field have so far found out will be useful to business owners, managers and partners in the different organizations to design tailor made risk management techniques using modern ICTs. It is anticipated that this study will be of great use especially to small and medium enterprises (SME) that are expanding their supply chain network with the aim of increasing economies of scale and strengthen stable growth in the market.

CHAPTER 2:

2.1 Literature review

This chapter provides the review of literature that was used in relation to risk management and supply chain vulnerability with focus on ICTs as per the identified themes and objectives. This review basically indicates the different literature that is available and supports this study as well as showing some gaps that may justify supply chain vulnerability.

2.1.1 Theoretical review

The following literature reviewed the theories that were expressed in chapter 1. This review identified the existence of the gaps between then when these theories had just been found and now when businesses rely more on modern technology and globalisation. Some of these gaps explained the magnitude of existence and persistence of supply chain vulnerability which aided appropriate management initiatives to cub risks. The theories the researcher already focused on in chapter 1 are the Transaction theory, Network theory and System theory.

2.1.1.1 Transaction theory

As earlier stated transaction theory is defined by the different researchers depending on their findings. It is a theory that defines governance structures as based on the net effects of internal and external transactions, rather than as external contractual ties (Bahli & Rivard, 2003). Unlike agency theory which advocates for assigning of duties and responsibilities to someone else to carry out a transaction, transaction theory supports business structures that promote doing it within or by yourself (Williamson, 1986). (Williamson, 1986) assumed that there are three internal variables upon which transaction theory costs are rated and these are:-

- Asset specificity that throws light on the amount a manager will personally gain.
- Certainty or trust or otherwise being caught.
- Frequency of carrying out internal transactions that drive costs upwards.

Analyzing the above variables it is true that (Williamson, 1986) greatly supported risk management within organizations. But, it can also be argued that to date the supply chain is both inward and outward oriented (Waters, 2011). There is a higher degree of trust between organizations within the supply chain integrations unlike that of the transaction theory.

Therefore, in order to bridge the gap of the level of trust in transaction theory which may pause a threat to the vulnerability of the supply chain, modern technology has led to the automation of most of these earlier transaction costs. Although this is has led to other completely new costs as will be discussed in chapter 3.

Meanwhile other researchers emphasized close monitoring of external transaction costs mainly in research and information, bargaining and decision and policing and enforcement (Pitelis & Pseiridis, 1999):- see illustration in figure 1.

a. Search and information:- This relates to costs incurred in deciding whether a requested product is available on the market with the lowest price, relative value and functionality of the product, possible operating costs of continuous use of the product and other relevant fields. In most businesses the operational costs that can be embedded in the search of information may include hiring of marketing specialists, transport costs to go to the field and look for sources of good products or services. Many times international travel for conferences could not be ruled out leading to high operational costs among others. To date, especially in developed countries like Belgium, modern technology of searching online platforms, arranging virtual meetings and closing sales deals in a timely manner has changed the game of trade hence reducing search and information costs (Messenger & Gschwind, 2016). Other modes of searching for information in real time are through use of smart phones where for example product bar codes can be scanned to get detailed background of composition and performance (Kato, Tan, & Chai, 2010), human resource can be recruited through click away platforms such as LinkedIn. The convergence of social media as a whole including WhatsApp, Tweeter, Facebook among other platforms also allows the different players in the supply chain to look at multichannel online sources of information in quicker and different way.

The ways in which transaction theory portrays the need to closely supervise external costs especially search and information while acquiring products or services shows that there is a gap between then and now. The speed at which modern ICT is driving costs is quite different hence requiring different risk management approach as we shall see in chapter 3.

b. Bargaining and decision:- This relates to costs required to reach an appropriate arrangement with the other party in the deal and draw up a satisfactory contract.
Even when vertical integration and trust was advocated for organizations (Williamson, 1986), the expansion of supply chains has forced companies to focus more on inter connectivity and building of coalitions to dominate the market rather than only concentrating on internal operation (Lysons & Farrington, 2006). Yet, the importance of internal organization cannot be under estimated if the business is to survive in the supply chain (Hadjimanolis, 2000). Hadjimanolis (2000) pointed out that human behavior was paramount in management and decision making within organizations. If managers were not innovative with sufficient bargaining skills among stakeholders, projects for example implementation of suitable ICT would not be supported and hence could lead to supply chain vulnerability.

c. Policing and enforcement:-
The costs of ensuring that the other party complies with the terms of the contract and of taking reasonable action, if not. It should also be noted that western high-wage corporations outsourced production to low-wage nations such as Vietnam and China (Carmel & Tjia, 2005).

Internet technology made it easier for companies to monitor the quality of the products coming off the production line, see if what was being produced matched what was ordered, and monitor the products around the globe. Freer trade ("WTO | Understanding the WTO - The GATT Years," n.d.) and lower transportation costs have contributed to driving this phenomenon. R&D was also divided into higher-value product production, which was often left in the home country and lower-value activities that were often outsourced to India.

Product Lifecycle Management applications offered a growing development forum for companies and a way for them to track the progress made by engineers in India. Outsourcing became a more viable option in trying to reduce transaction costs and expand businesses (Buck-Lew, 1992). Modern ICT has facilitated outsourcing, reduced all three sets of transaction costs, the most significant was lower cost of policing and compliance.

Unlike earlier predictions by researchers such as Pitelis & Pseiridis (1999) that transaction costs need much attention, with this new technology it can be argued that their approach may not be very successful on its own without incorporating the current trends that advocate for alliances through partnerships such as outsourcing, integrated electronic requirement plan (ERP) systems which have changed the goal of the game giving rise to other forms of risks that need a different way of management in order for businesses to succeed.

Given the current trend of the supply chain integration backed by modern ICT or modern technology many companies have got new approaches to business dealings that have shifted the focus from transaction costs to other forms of business models such as outsourcing (Quinn & Hilmer, 1994). Non-core transactions depending on the nature of business can be outsourced to other companies that specialize in those fields of businesses. The type of transactions that are normally outsourced are those that may require higher cost to manage internally or deemed non critical to the business. These may include manufacturing, human resource, transport, marketing among others depending on the business approach. Outsourcing when well managed greatly reduces transaction costs. Lower transaction costs have made it easier for businesses to be less vertically integrated (Buck-Lew, 1992).

Therefore, with the current global changes of trade it can be argued that only relying on transaction theory assumptions to manage risks may lead to supply chain vulnerability since it does not optimize the capability to expand and optimize the advantages of integrated supply chain. Even the trend of supply chain integration may weaken such businesses that cannot evolve with the new business norms that are greatly supported by modern technology (Lysons & Farrington, 2006).

2.1.1.2 Network perspective theory.

As defined by many scholars, the network theory deals with the interaction of companies with different entities, such as suppliers, consumers or buyers through their supply chains. Starting with the context and roots of the theory, it can be seen that the word 'relationship' was not used

in the 1970s, although the term 'supply chain management' was already present at the time, to describe operations such as those with suppliers (Harland, 1996).

Still, a first change was evident in terms of supplier evaluation and the contribution of stronger ties to quality , delivery and price (Harland, 1996). The early research during this decade, however, began by focusing on closer relations between two firms, by analyzing topics such as trust , cooperation or strategic partnerships, and not on the perspective of the network as per say (Mills, Schmitz, & Frizelle, 2004). After that time and in the early 1980s, companies in the market world started documenting moves towards greater competition.

They joined a call for movement away from central management and multi-level hierarchies towards a variety of decentralized structures, suggesting that conventional hierarchical pyramids are closer to a network model (Miles & Snow, 1992). During this time, highly competitive companies began to downsize their core competencies, redesigned the management hierarchies and began outsourcing those operating operations while others focused on vertical integration (Miles & Snow, 1992) . Some new group of business companies resisted expansion and instead pursued strategic partnerships with independent suppliers (Miles & Snow, 1992). Despite adopting the network approach, early 1980s research often concentrated on examining basic relationship, cooperation between two organizations, or defining strategic partnerships and alliances (Yee & Platts, 2006).

After that, researchers took a wider view of so-called 'supply networks' and they began to incorporate, next to the actual movement of materials, the product creation process and collective learning (Mills et al., 2004). Researchers' attention changed from focusing solely on one business unit or organization to analyzing dyadic relationship management with corporate partners (Yee & Platts, 2006). A network perspective was brought to the agenda of studies about strategic alliances and the creation of inter-organizational networks contributing to the formation of strategic alliances as first introduced (Gulati & Gargiulo, 1999). From that time on, strategic alliances were considered to be essentially dyadic exchanges, main precursors, processes and outcomes embedded within most firms that could be identified and formed by the network (Gulati & Gargiulo, 1999).

Supply chains have been characterized since the late 1980s as the network that leads to the inbound and outbound of products and services within the value chain and has thus gained more alertness from organizational theorists (Miles & Snow, 2007). It was believed that the use of the word 'network' was intended to expand the concept of supply chain management to gain more knowledge of resource potential and improve relationship efficiency (Johnsen, Wynstra, Zheng, Harland, & Lamming, 2000). This was because the literature and some empirical research showed that companies were typically entangled with multiple customers and various vendors in more than one supply chain (Mills et al., 2004). From that time on, (Lamming, Johnsen, Zheng, & Harland, 2000) identified the idea of 'supply networks' as being researched in two separate ways that affected the creation of the whole concept.

In their report, they note that the researchers of the Industrial Marketing and Purchasing Community (IMP) conducted a descriptive analysis on industrial networks, which created models to facilitate a better consensus of business markets in relation to the relations between buyers and suppliers and the embedding of organizations into networks. Next to that, according to Lamming et al., (2000), another study, which is part of the more prescriptive research on supply chains management, was investigated in the area of strategic management, operations management and logistics (Johnsen et al., 2000).

Although when the network theory was first introduced, it was still an important topic discussed in the research era of 1970s and 1980s. Researchers were primarily concerned with understanding what makes an organization successful, and what processes are needed to do so. However, the concept of achieving productivity has been recognized over the past decades through the communication and contact with other supply chain parties (H\aakansson & Snehota, 1989). Nevertheless, as (Miles & Snow, 2007) claim in their article, the emergence of multi-company network organization has opened up a whole new arena for strategic choice, and many firms have become far stronger competitors by linking with specialist suppliers in an integrated supply chain (Miles & Snow, 2007).

Hence, the network theory's first underlying assumption is that companies embedded in a network cannot freely decide how to behave towards their own interests, nor can they function in isolation from one another (H\aakansson & Ford, 2002). However, it is believed that the actions and activities of organizations with other companies within a network are better understood as a fragment of significant counterparts as well as strategic relationships (H\aakansson & Ford, 2002). According to Harland (1996), there are numerous factors that can be defined as critical when coding a network, namely selecting collaborating partners, maintaining a competitive position, tracking competitors, and managing relationships correctly (Harland, 1996). Furthermore, (H\aakansson & Snehota, 1989) argue that if a company has been able to attract other companies to do business with each other, and they share a common interest and a certain business environment with each other, the company is embedded in relationships with other organizations and is therefore part of a network (H\aakansson & Snehota, 1989). Shook, Adams, Ketchen, & Craighead (2009), argue that the network theory does not specifically clarify to companies when to make, purchase or join, but it does seem to provide an explanation to companies from which other firms they can choose to purchase or employ as strategic alliance partners (Shook et al., 2009).

Thus, a central point in network theory is proper management as well as the strategic search for companies with which to start a relationship. It is argued that some of the network's partnership with other organizations is in itself one of the most – if not the most – important asset it possesses (H\aakansson & Snehota, 1989). They further argue that through these partnerships, resources and activities are more available and, in exchange, better organized and used by the company to improve its own efficiency (H\aakansson & Snehota, 1989).

The next premise in supply management arising from the network principle is that a firm centrality embedded in a network is an significant factor and may justify a competitive position or advantage. No company in a network can work in isolation as has already been argued, and they are dependent on their established relationship with other parties. Through this, one might get the impression that the network does not have a center and that each company operates with a common goal in mind. However, it may be worthwhile to be able to maintain a more central role within a network and to build better relationships with companies or suppliers that are important to the network. To develop such a strong role, organizations have to be able to collaborate strongly with other companies and should begin by focusing on the ability to collaborate effectively internally (Miles & Snow, 2007). Thus, companies located at the center of a network could be regarded as having a strong internal collaborative power within their own business unit (Miles & Snow, 2007).

Access to resources is a key factor for success when needed. Occupying a central role within a network increases knowledge of resources and capacities within the supply chain and thus has a positive effect on the collaboration between the buying company and the suppliers (Bernardes & Zsidisin, 2008).

Networks are assumed to contribute to the sharing of information among entities in the supply chain. Typically knowledge, such as the cost of something or where to get the best resources, is not exchanged among organizations in the same supply chains, as they may be afraid that their rivals may profit from it (Ballou, Gilbert, & Mukherjee, 2000). Other organizations might be afraid that sharing information about their unique products, as well as the resources needed for production, could result in other supply chain companies being imitated and thus losing their competitive advantage (Lamming et al., 2000).
Networks are still expected to be open to the exchange of knowledge between companies and therefore give great leaf of reference.

Strategic networks provide a company with access to information, resources, markets, and technologies; benefits from economies of learning, scale, and scope; and enables firms to achieve strategic goals such as risk sharing and outsourcing of value chain stages and organizational functions (Zaheer, Gulati, & Nohria, 2000).

With that explanation of the network perspective it can be seen that some of its characteristics are quite hard to distinguish from that of the supply chain. Perhaps it would be reasonable to say that to a greater extent network theory portrays much of what we are seeing in the supply chain to date.

2.1.1.3 System theory

Systems theory throws light on the importance of coordination of activities, resources and human capital throughout the supply chain. Von Bertalanffy (1950) made a seminal contribution during the primary study of the advancement of systems theory. The contributions Bertalanffy (1950) made to scientific research were mainly from the perspective of physics and biology.
For example, in his paper published in 1950 – while he was a professor at the University of Ottawa – Bertalanffy (1950) analyzed the view of the open system of living organisms in contract to them being in closed systems. He suggested that the living organisms were highly organized with minimum interruptions and that this principle should further be investigated scientifically to the benefit of other systems. His research, after the 1950s, was mainly about the advancement of science's methods, which contributed to the creation of general system theory. Bertalanffy (1950) questioned classical modelling, based on a quantitative view of the processes, arguing that the time factor affects these open systems. Open systems can be related to supply chains that are vulnerable and therefore need risk management to make them sustainable.
It is no wonder that closed systems characterise some of the strong supply chains that are well managed by the stakeholders. To understand these open systems, therefore, a dynamic view of the systems is required (K. M. Lavassani & Movahedi, 2010b).

Gripsrud et al., (2006) discuss the early system theory implementation in supply chain management and especially in the logistics context. They claim that during the time from the 1950s-1970s the neoclassical economic theories were dominant. The emphasis during this time was one "absolute cost" and one "trade-off". However, since the 1970s the system theory has been dominant in understanding the context and operation of the supply chain of organizations. it is with no doubt that under rating such system theory approaches to management of supply chain can easily render it vulnerable hence increasing risks especially in this era of technology.

2.2 Summary of literature review

Basing on the above literature reviewed much as earlier studies were using different approaches to define the behavior of individual businesses in managing risks, a similar approach can be traced in the current supply chains we are experiencing today. In developing countries however, most of the theories discussed in this literature still apply in risk management since the level of technology is not as high as that in the developed countries (Gupta et al., 2008). Therefore, the approach to risk management and supply chain vulnerability may take a different form compared to that in the developed countries even when they are all operating in integrated supply chains.

CHAPTER 3:

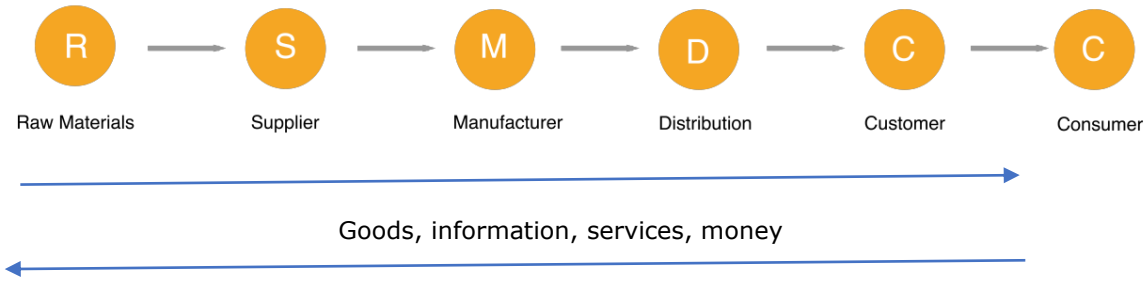
3.1 Discussion.

In the previous chapters of this study, risk, information communication and technology (ICT), supply chain vulnerability have been discussed in general. In this chapter supply chain vulnerability will be analyzed both within the organization, through the supply chain and the environment mainly focusing on ICTs.

3.1.1 Why does ICT make the supply chain vulnerable?

supply chain is the flow of materials and information upstream from the source then downstream towards the ultimate user or customer (Lysons & Farrington, 2006). Upstream includes sources of raw materials, supplier, manufacturer, downstream involves whole sellers, distribution, retail/customers and customer/end user.

Figure 6: Simple supply chain flow



In figure 6, the supply chain flow is mainly woven together by the flow of information, goods, services and money. But, because in most cases the players within the supply chain are located in different geographical locations, communications rely more on the internet of things which includes ICT tools such as smart phones, emails, electronic resource planning software (ERP), online banking, teleworking all of which sustain business operations. Search and information systems that were earlier identified by (Pitelis & Pseiridis, 1999) have now evolved into modern information technology where hardware, software, and telecommunication equipment are paramount. International communication systems have greatly reduced the traditional operational costs as previously reviewed in chapter 2.

ICT/modern technology has enabled the interconnectivity of communication systems across the supply chains. Different information in form of data is stored by the different players in the supply chain system in electronic form. With such actions the supply chain has become vulnerable due to internal organizational and external factors below:-

3.1.1.1 Internal factors

a. **Type of management** – The organizational structure determines the way decisions are made in organizations. Depending on the type of business activities being carried out, flat structures facilitate quicker actions while hierarchy structures make decision processes longer. Striking a balance between which structure is suitable may not be easy since trade is very dynamic and sometimes full of uncertainty. The lack of streamlines management systems, policy manuals, trained information technology teams has led to poor communication network systems that have exposed companies some of which have run bankrupt while others have completely collapsed (Hadjimanolis, 2000). The way organizations are managed most of the time affect the rest of the entities in the supply chain. A mere management problem may escalate and disrupt the rest of the activities across supply chain creating vulnerability (Bartiromo, 2018).

b. **Capital allocation**- Modern technology/ ICTs require substantial investment depending on the size and position of an entity within the supply chain. The speed at which technology is evolving requires constant re-investment in order to keep up to date with the rest of the competitors and partners on the global market. When one or more players in the supply chain for example farmers do not have enough money to buy modern equipment, this may slow or disrupt acquisition of raw materials used in manufacturing hence affecting lead time for customers. As a result the lack of capital to invest in modern technology may render the supply chain vulnerable. Initiatives to try and cut costs and increase profits have been reflected in the literature review (Pitelis & Pseiridis, 1999).

c. **IT infrastructure-** The type or style of IT infrastructure that is adopted by an entity in the supply chain may also become a source of supply chain vulnerability (Laudon & Laudon, 2006). An oversight in the implementation of a software to run certain tasks in a given organization may create adverse consequences that can spread across the supply chain. An example is when a small to medium enterprise (SME) operating at a local level to run a children day care center makes a decision to deploy a Micro software such as SAP Hana that is mostly recommended for much bigger organizations. This automatically puts the SME at stake as well as its suppliers since such software may be too expensive to maintain and in the long run inappropriate given the nature and size of the business. Such mistakes are still being made across the globe since IT perception is not the same across the different stakeholders. Such misappropriate software adaptation in organizations may create supply chain vulnerability.

d. **Training-** The quick evolution of ICT requires constant training, coaching and support from experts who may be inhouse or externally outsourced in form of consultants in order to reduce risks that arise when network systems collapse (Stanton & Webster, 2014).

Although most organizations try to keep up their employees with constant trainings on new software, it has become rather expensive to sustain trainings especially due to the fact that workers keep moving from one organization to another in form of search for 'greener pastures'. Training may also be very expensive depending on the nature of the organization. Given the fact that the different organizations have varying profitability, not all of them within the supply chain can be on the same level as far as training is concerned. This situation eventually leads to supply chain vulnerability.

e. **Maintenance-** Modern technology/ICTs most of the time require high maintenance. Technical experts have to check the quality and conformance of all software networks, data storage systems, communication equipment and data content. Since this maintenance is done by people there is a possibility that there can be errors or omissions in setting up systems. Problems caused during maintenance for example outages and loss of data or power breakdown may cause serious problems that once not controlled can lead to supply chain vulnerability https://www.vrt.be/vrtnws/en/2019/07/13/baggage-handling-problems-at-brussels-airport-are-over/

f. **Security**-This is a much broader topic that may not be exhausted here but cuts across both internal and external factors that cause supply chain vulnerability. This will be briefly discussed in four categories that include:- Internet vulnerability, wireless security challenges, malicious software, hackers and cyber vandalism (Laudon & Laudon, 2006).

- **Internet vulnerability-** People in the different parts of the world are connected via the internet and it is evident that most organization if not all rely on the internet to carry out businesses.
- The fact that the internet is an openly accessed platform there are very many opportunities that can help sustain organizations. Yet, it cannot be ruled out that there are also very many threats that render supply chains vulnerable. Both inside employees and outsiders can illegally hack and access private information for malicious damage to companies. Tapping of phone conversations, credit cards, bank accounts, copy right and patent information is also at stake if not well protected by businesses or individuals in charge. If organizations have not put in place strong IT security systems in place such illegal actions affect businesses which may spread throughout the supply chain (Laudon & Laudon, 2006).

- **Wireless security challenges-** How safe wireless fidelity (wi-fi) is can also be contested. Different people always on the move find it convenient to log on any available wi-fi in areas such as air ports, restaurants, and other waiting areas. The fact that these networks most of the time are unsecured and accessed by different people who come in and out of those areas, illegal people have used them to gather information over different companies via individual gadgets. Some of this information may be highly sensitive and once exposed to the public may lead to serious consequences such as exposure to the media, litigation among many other negative

consequences. If wi-fi challenges are not controlled they may spread throughout the supply chain resulting in its vulnerability (Laudon & Laudon, 2006).

- **Malicious software-** "Malicious software programs are referred to as malware and include a variety of threats, such as computer viruses, worms, trojan horses" (Laudon & Laudon, 2006). Most of these come in form of emails, messages on smart phones, or transferred from computer to computer through flask disks, USB and other gadgets. Given the nature of the supply chain it is evident that speed is required to carry out transactions in order to sustain businesses. But, in case employees do not take care to follow IT security guidelines in place while exchanging information organizations may loss important data. This may lead to disruption of the supply chain for example when a supplier loses customer contacts and as a consequence they are unable to deliver goods on time.

- **Hackers and cyber vandalism-** This is also not a new threat in the internet world. The better the IT security systems the smarter the hackers. It is more of a competition between hackers and IT security systems. A hacker is one who accesses a computer system without authorization (Laudon & Laudon, 2006). Many people have realized that having information over certain companies can make them earn profits. Data has become an expensive item to trade that some companies go all the way in hacking activities to compete for businesses or even completely vandalize the networks of their opponents in the market. Hackers may spoof and sniff, launch Denial of Access attacks (Dos) among other ways so that they destroy the network or disrupt business operations. This once not well controlled may also lead to the vulnerability of the supply chain (Laudon & Laudon, 2006).

3.1.1.2 External factors.

The external factors making supply chain vulnerable may be discussed by looking at the political, economic, social, technological, environmental and legal aspects in relation to ICTs.

Politically depending on the location of an organization, actions of government that include political unrest may increase insecurity and lead to wars causing vulnerability of the supply chain. Planning and implementation of business activities becomes difficult in such an environment due to fears of losing lives or looting. This also discourages investors from operating in such uncertainty. Wars affect IT infrastructure and deter development of modern technology. In turn, all organizations within the supply chain but located in unaffected areas in this case Limburg may face shortage of supplies or services (Şen & Babalı, 2007). It is not only through political instability that supply chains may be vulnerable but also government policies. Imposing high taxes and corruption tendencies by government officials does not also favor investors including those for modern ICTs. Perhaps some traits of internal organization may be looked at where behavior of individuals in political positions may contribute to poor planning, decision making and not be able to address problems in a timely manner (Hadjimanolis, 2000).

The economic situation of a country and profitability of individual organizations may contribute to the vulnerability of the supply chain. Companies located in countries where the economy is not as strong face challenges of inadequate financing to run their business activities efficiently. Big agricultural projects may fail to take off in some third world countries where factors of production are still a struggle, such as presence of modern buildings and poor roads, scarcity of skilled manpower, lack of modern IT, hence failing to sustaining global operations (Gibbon, Ponte, & Lazaro, 2010). The existence of such challenges makes the supply chain of products such as cash crops like coffee to Limburg from let's say Kenya vulnerable. Modern ICT being an expensive venture may not also get much attention given the fact that it is not among the essential projects of such countries.

The social aspect may not be underrated since people are the ones that run businesses. Culture of a community plays a big role to the extent of the vulnerability of a supply chain. Countries for example China which is communist creates an environment of communal work. With that spirit they were able to build a hospital of 1000 beds in 6 days during the beginning of the global pandemic COVID-19 (Vaswani, 2020). This eased the burden on the patients being admitted in hospitals and saved thousands of lives. It can be noted that with such an approach the country has managed to successfully open unlike in other countries such as United States of America where the culture is different and some protests are being witnessed. Universal social actions through the use of social media among other channels greatly determines the extent of the strength or supply chain vulnerability.

Much as the political, economic and social aspects are paramount in the strength or vulnerability of the supply chain, the risks associated with these may be managed by key supply chain players. Yet, with the environment, especially natural disasters are harder to predict and in fact cause massive losses some of which may never be recovered. Some of these natural disasters include floods, hurricanes, earthquakes, tornados, landslides, volcanic eruptions but to name a few. Even where the organizations in the supply chain are strongly integrated this vulnerability may disrupt all operations in the affected areas leading to their collapse ("Europe Grapples with Storm Ciara's High Winds," 2020).

Legal aspects have become more and more sensitive in the discussion of ICT across the globe (Adomi, 2010). The ethical code of conduct is one of the documents every employee signs before they start a new job. Although companies are very conscious there are many loop holes that both internal and external employees among other stakeholders have utilized to share private information into the public resulting into expensive litigation processes. For example Dunkin's brands which was sued for not informing its customers that their accounts had been targeted in forms of cyber-attacks. On top of legal charges, it lost many customers and its shares also went as low as 2% (Wu, 2019). Such a scenario may have also been as a result of decision making illustrated by (Pitelis & Pseiridis, 1999). Copy right and patents cannot also not be ignored as important legal factors making the supply chain vulnerable. Breach of contractual obligations may be an obstacle for some businesses within the supply chain.

Legal cases may arise from simple business transactions for example failure to transport a passenger to the airport on time, and as a result he/she misses a flight to an important conference where 100 people are waiting for his/her presentation.
Then one of the conference attendants decides to sue the presenter and his/her affiliates. Such legal issues some of which are controllable while others may not be controllable depending on the situation render the supply chain vulnerable.

With the above external factors it is indeed true that the vulnerability of the supply chain may arise from any area.

3.1.2 Which ICT areas make the supply chain vulnerable?

Teleconferencing

The term tele means remoteness. The word 'conference' means debate, consultation. The process of holding conferences through telephone or network link. Teleconferencing is the live exchange and mass circulation of information between many individuals and machines remote from each other but connected by the telecommunication network. This trend has gradually picked momentum in today's world since most businesses hold offices in different geographical locations. Teleconferencing is a much viable option since it cuts down on travel costs, time, and increases flexibility in carrying out quick decisions. Yet, it should be noted that teleconferencing makes it harder to observe body language behaviour of participants, hence difficult to predict the impact of the meetings convened. Sometimes members are completely doing other things like sending emails during the call, which may imply that the level of participants paying attention is rather harder to predict. Criminal gangs have also interrupted some of these meetings and reports made to government authorities such as FBI ("Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic," 2020). The fact that safety and 100% positive realisation from teleconferencing is not guaranteed this makes the communication throughout the supply chain vulnerable.

Video conferencing

With videoconferencing people will communicate with both pictures and sound transfer in real time as if they were communicating face to face. In the fields of finance, distance learning, home offices, legal setting and telemedicine, video conferencing has been used to date. Not every organisation in the supply chain can afford such IT infrastructure. Sustaining a video conference requires that all participants have good internet connection which sometimes is not the case especially in rural areas. Yet, the rural areas are places where big factories are located, local farmers all of whom feed the supply chain in one way or another. Even when Belgium registered 99% household high speed internet connection in 2018 the problem is still the same with rural areas ("99% of Belgian Households Connected to High-Speed Internet," 2018). This is worse in other countries especially in Africa such as Kenya which serves as one of the main suppliers of flowers to Belgium.

With this inequality in accessing good internet for quality video conferencing the benefits of face to face meetings which enhance trust among supply chain players may not be easily realised hence leading to supply chain vulnerability.

Mobile Phones

Mobile phones, also known as cell phones or cellular phones, are portable telephones with antennas built in. Cell phones, unlike home phones, can be brought with minimal hassle from place to place. The pitfall with mobile phones is they are easily stolen, misplaced, or spoilt. With the advancement of smart phones some people store a lot of information and data which if not regularly backed up may be lost. Loss of important company information may cause problems of illegal access to private information by criminals, fraud due to access of the online banks, and misrepresentation all of which may put both individuals and companies at steak. ("4 in 10 Belgians Don't Protect Access to Their Smartphone," 2019). Much as mobile phones have made it much easier to make business transactions caution should be adhered to otherwise they render the supply chain vulnerable.

Computers

A computer is a programmable machine for inputting, processing, and outputting data. A computer system refers to the computer, as well as all its devices. Computers around the world make communication much swifter within an organisation, the supply chain, and other stake holders around the world. But, because different people may access one computer such as users, technicians, visitors, children for those who work from home it becomes rather hard to have 100% guaranteed secured access. Passwords may be hacked if not strong enough, electricity blackouts may destroy data bases, viruses may accidentally be downloaded intentional or unintentional all of which make computers not very secure (Wu, 2019). Therefore, users have to abide by up to date IT security guidelines to ensure that computers do not pause a threat to their companies. A technician can easily transfer important information from one company to another within the supply chain or even to the public. Hence, making computers one of the factors in the supply chain vulnerability (Laudon & Laudon, 2006).

Social media platforms

The researcher may have discussed these under computers or mobile phones but because they cut across and have become more dominant in the business world they are to be elaborated independently. Social media platforms can be accessed via different websites and apps that can be downloaded on computers, laptops, smart phones, smart watches, smart sports T-shirts, vehicles, just to name a few. The most prominent apps across the globe to date are Face book, WhatsApp, tweeter, Snap chat, and others that may be customised for particular business communications. All these platforms allow people to share content quickly. The ability to share documents, photos, advertisements, and all other personal and business information has greatly enhanced business performance in the different parts of the world.

A person in Limburg can share information with another in China or Hong Kong in just seconds. No wonder the power of social media can not be under estimated in developing supply chains and enhancing business growth and expansion around the world. However, it should be noted that a slight mistake in communication on social media may lead to loses and caos as already explained in the H&M sweatshirt advert that was misperceived by consumers as a racist act (Bartiromo, 2018).
That is why The General Data Protection Regulation in Belgium was adopted in September 2018 to streamline data processing activities.("Data Protection Authority," n.d.)

Automated Teller Machines (ATMs).

An Automated Teller Machine is also known as an automated banking machine (ABM), or cash machine, a computerized telecommunication system that provides financial services to customers with access to public space financial transactions without the need for a cashier, human clerk or bank teller. They are self-banking machines located in different bank branches. In some instances, high way criminals with guns tend to raid deserted petrol stations, supermarkets, and other businesses not to forget main banks where these ATMs are located. An example was when 10 Dutch national were sentenced to 13 years in prison by the court of Antwerp when they broke 5 ATM machines and were attempting to break the 6th. A total of 80800 euros was stolen (News, 12:28+02:00). Once money is stolen from these machines profits and capital may totally be lost. Smaller affected banks try to push on through claiming damages from the insurance a process that takes long or resort to financing with high interest rates from central banks. Others may completely collapse. Such problems may lead to disruption of the supply chain since cash flow is essential in business transactions.

Television

Television or TV is a telecommunication medium used for transmitting sound in black and white or color or three diameters with moving images. Over years, televisions among other communication aids has been key all over the world. Through advertisements companies have earned a lot of profits and been able to expand nationally and internationally. Among the 10 biggest advertisement spenders of 2019 included General Motors that spent $ 3.14 million in total spending (Luce, n.d.). No wonder it is one of the biggest motor companies in the United States to date. Meanwhile, other companies have faced back clashes due to inappropriate communication or advertisements that they released to the public. A case is that of H&M when it advertised a "coolest monkey sweatshirt in the jungle" featuring a black child (Bartiromo, 2018). Even when they eventually retracted the advert, some customers decided to stop buying from them. That incident led to protests especially in South Africa where their new branch had just opened. The shop was vandalized and property looted/ spoilt. H&M quickly reacted to make new human resource policies some of which stated that by 2025 all staff members will feel equally privileged regardless of their racial backgrounds and origin (Bjerre, n.d.). Therefore communication via different social media platforms including television once not well thought through may lead to supply chain vulnerability.

Radio Set

A radio receiver (also widely referred to as a radio) is an electronic device that receives radio wave and transforms the information it carries into a usable form. Used with an antenna. The antenna intercepts radio waves (electro-magnetic) and converts them to the small alternating current applied to the receiver.
The science of radios was first discovered by Heinrich Hertz in 1886 (Bryant, 1998). Unlike earlier when radios were either at home or in offices today in addition to already existing places these can be accessed from a variety of gargets such as the internet, smart phones, smart watches, motor vehicles, tables to list but a few.

Normally people at home or office or those on the move especially in planes, trains, motor vehicles, can listen to their favorite programs. News, advertisements and other important information can be hard via radios. It should be noted that depending on the nature and global location of an organization in the supply chain there are people in remote areas who still depend on radios as a source of information. Yet, streaming services have become a great threat to its existence. Adults in the U.S. also spent an average of 102 minutes a day tuning in to the radio in the first quarter of 2019, even though this marked a decrease of 3.77 percent from the previous year, according to data collected from Nielsen. Approximately 45 percent of this listening takes place in the car, while another 21 percent takes place at work. In-home 31 per cent Adults in the U.S. also spent an average of 102 minutes a day tuning in to the radio in the first quarter of 2019, even though this marked a decrease of 3.77 percent from the previous year, according to data collected from Nielsen. Approximately 45 percent of this listening takes place in the car, while another 21 percent takes place at work. In-home 31 per cent happens (Andrews, 2019). Therefore much as radios are still used in most parts of the world, the pressure to communicate via other social media networks is rather high. This may lead to information not reaching certain players in the supply chain especially in remote areas and yet that is where sometimes chains begin from. Hence creating supply chain vulnerability.

3.1.3 What should be done to mitigate supply chain vulnerability with focus on ICTs?

There are different ways through which the risk management can reduce supply chain vulnerability. It may be done on an organization level, supply chain level, national or global level.

Organizational level:-

Management support- Without involvement of top management most good projects initiated by employees do not normally succeed. Key stake holders in an organization have to pay

attention to risks that may render the supply chain vulnerable. This has to be done together with employees so that the level of commitment is assured from both parties.

Employee trainings- Since vulnerability of the supply chain may originate from different areas both internal sources and externally training of employees is very crucial to ensure that everyone involved in the organizational operations understands the nature of risks that may occur and have sufficient knowledge of what should be done. In ware houses for example safety measures are pinned around areas of common use like cafeteria so that everyone can read them. Incase of ICT regular change of passwords is always encouraged and such information is normally pined next to desk tops so that people do not forget.

Capital savings and investment- Risk management requires capital savings and investment. This is because threats may lead to the need to overhaul of all electronic devises, software systems in order to save a business. Some threats may also require legal representation such as mediation, litigation among others. Occurrence of natural calamities may require some form of backup plans before counting on insurance companies.

Risk management policy and backup- Having policies and systems in place in all organizations is one thing but creating awareness of these across organizations is another. Some companies do not take time to remind employees about risk management in detail.
They only mention safety measures while at work yet, risk is much wider than that as already discussed in the previous chapters. Therefore, it is important that a risk management policy and backup plan is regularly communicated to employees especially in the areas where they directly have an impact.

Active risk management committee- This means that organizations have to have a team of members who regularly remind relevant stakeholders the importance of risk management. This can be done in form of periodic workshops where it is mandatory for all relevant employees to attend. Certificates of recognition in form of motivation may be awarded to best persons that have carried out risk mitigation actions in the organization.

Risk management audits- This may be internally aided by expert employees or engaging external consultants or audit firms to carry out the audit. Much as finance, logistics, sales and marketing may be key in these audits depending on the organization, IT has also become a point to key interest and tools of for example data mining maybe used to generate important information for informed decision making.

Legal advisors- Legal advisors are necessary in every organizations' survivor. These maybe internally employed or brought in as experts to advise the organization in certain business ventures or act as legal representatives in dispute resolutions. That way the vulnerability of a business may be reduced.

Ethical code of conduct- Perhaps this falls under the legal advisors above. The researcher has addressed it differently since it has become a great source of litigation lately. Sharing of company information without authorization may lead to the breach of the ethical code of conduct.

No wonder all companies make their codes of conduct among the contract documents of employment admission. Much as these codes of conduct are signed by employees, it is important that the information in them is shared across the organization in more simplified ways such as company slogans, illustrated in form of paintings, hanged on notice boards among others. This will endure that every employees is aware of what is acceptable and what is not acceptable at their work place.

Supply chain level:-

Timely sharing of necessary information- Across the supply chain it is important that information is readily available to all stakeholders in order to act appropriately. Lack of information lets say by restaurant owner that food markets will be closed on festival days may lead to loses since they will not have got the chance to stock enough food to do business that day.

As a result customers may also get disappointed and hence create a bad reputation for the restaurant. Therefore timely information sharing if very important in reducing supply chain vulnerability.

Partnership meetings- These may be beneficial for organizations especially those that are located in the same area and depend on each other's services. An example is a poultry firm supplying its waste to a company making fertilizers for farmers. With this ideas can be shared on how best both companies may co-exist with each other and support each other for growth. Hence mitigating the supply chain vulnerability.

Strategic alliances

National level:-

Securing government support- This can be done through networking and participation in social cooperate responsibility national activities. That way the popularity earned in serving the nation may turn out to be beneficial in case there is a serious crisis that may crash the organization. Through such networking it becomes easier to get in touch with key decision makers who may offer their support to save the business.

Taxes and fines- Non-payment of taxes and other government dues makes the supply chain vulnerable since government may force non-compliant business to pay heavy fines or close. To avoid such occurrences it is important that all organizations big or small within the supply chain make timely payment of government taxes and other dues as soon as there is need.

Political interference- Most of the times when employees decide to engage in politics they resign their present jobs so that they can take on their new role. This is the norm in most developed countries. However in a few developing countries directors and entrepreneurs engage In politics while maintaining their positions in their organizations. This may be problematic since it is not easy to fulfill both obligations.

Those who insist sometimes end up losing their businesses especial those that are still small in size. Therefore it is good practice that an employee or director resigns the moment they decide to go political.

Globally:-

Secure ICTs- Since this is the common umbrella of communication across the globe, with the increasing hackers, cyber terrorism, software malware and others as earlier discussed, IT especially cyber security has to be in place in order to not only reduce supply chain vulnerability but also protect other parts of like such as personal privacy.

3.1.4 Conclusion

Therefore, this study examined the different aspects of risk management and supply chain vulnerability with focus on ICTs. The literature review goes in details to explain the different theories relevant for this study. Although the transaction theory, Network theory and system theories were the focus of this study, there are many more theories related to this field of study that were not relevant in this research. It should be noted that even when modern technology is currently prevailing , the theories in this study can still be traced in the business transactions especially within organizations that are not yet fully automated. Despite the fact that there is already existing literature and research carried out in risk management and supply chain vulnerability with focus on ICTs, in this study the researcher observed that some companies did not show enthusiasm in risk management implementation. Among these companies was an international company in Limburg where there were a few power outages, failure to work the whole day due to downloading and backup issues from the USA, errors in data cleaning all of which led to higher labor costs due to overtime to try and meet deadlines. From the details of this study supply chain vulnerability can be mitigated through well-established risk management structures, trained teams, capital investment, periodic ICT efficiency reviews, strong ICT security systems, legal compliance within organizations, throughout the supply chain and globally where applicable.

3.2 Bibliography

4 in 10 Belgians don't protect access to their smartphone. (2019, October 19). Retrieved June 2, 2020, from The Brussels Times website: https://www.brusselstimes.com/all-news/belgium-all-news/74379/four-in-ten-belgians-dont-protect-access-to-their-smartphone/

99% of Belgian households connected to high-speed internet. (2018, June 13). Retrieved June 2, 2020, from Invest In Flanders website: https://www.flandersinvestmentandtrade.com/invest/en/news/99-belgian-households-connected-high-speed-internet

Adomi, E. E. (2010). *Frameworks for ICT Policy: Government, Social and Legal Issues*. Information Science Reference.

Andrews, J. (2019, August 9). Would you care if music disappeared from FM radio? You may only have a decade to save it. Retrieved June 3, 2020, from CNBC website: https://www.cnbc.com/2019/08/09/would-you-care-if-music-disappeared-from-fm-radio.html

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: A transaction cost and agency theory-based perspective. *Journal of Information Technology*, *18*(3), 211–221.

Ballou, R. H., Gilbert, S. M., & Mukherjee, A. (2000). New managerial challenges from supply chain opportunities. *Industrial Marketing Management*, *29*(1), 7–18.

Bartiromo, M. (2018, January 8). H&M apologizes for "Coolest Monkey" sweatshirt ad featuring black child [Text.Article]. Retrieved June 3, 2020, from Fox News website: https://www.foxnews.com/lifestyle/hm-apologizes-for-coolest-monkey-sweatshirt-ad-featuring-black-child

Bernardes, E. S., & Zsidisin, G. A. (2008). An examination of strategic supply management benefits and performance implications. *Journal of Purchasing and Supply Management*, *14*(4), 209–219.

Bernstein, P. L. (1996). The new religion of risk management. *Harvard Business Review*, *74*(2), 47.

Bjerre, M. C. (n.d.). *H&M &" Coolest Monkey in the Jungle"*.

Bryant, J. H. (1998). Heinrich Hertz's experiments and experimental apparatus: His discovery of radio waves and his delineation of their properties. In *Heinrich Hertz: Classical physicist, modern philosopher* (pp. 39–58). Springer.

Buck-Lew, M. (1992). To outsource or not? *International Journal of Information Management*, *12*(1), 3–20.

Carmel, E., & Tjia, P. (2005). *Offshoring information technology: Sourcing and outsourcing to a global workforce*. Cambridge university press.

Chen, I. J., & Paulraj, A. (2004). Towards a theory of supply chain management: The constructs and measurements. *Journal of Operations Management*, *22*(2), 119–150.

Child, J., & Mansfield, R. (1972). Technology, size, and organization structure. *Sociology*, *6*(3), 369–393.

Coviello, N. E., & Munro, H. J. (1995). Growing the entrepreneurial firm. *European Journal of Marketing*.

Data Protection Authority. (n.d.). Retrieved June 3, 2020, from https://www.dataprotectionauthority.be/

Devlin, K. (2010). *The unfinished game: Pascal, Fermat, and the seventeenth-century letter that made the world modern*. Basic Books.

Dow, G. K. (1987). The function of authority in transaction cost economics. *Journal of Economic Behavior & Organization*, *8*(1), 13–38.

Europe grapples with Storm Ciara's high winds. (2020, February 9). *BBC News*. Retrieved from https://www.bbc.com/news/world-europe-51436040

Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic. (2020, April 3). Retrieved June 2, 2020, from https://www.justice.gov/usao-edmi/pr/federal-state-and-local-law-enforcement-warn-against-teleconferencing-hacking-during

Feldman, M. H., & Sauvage, C. (2010). Objects of Prestige? Chariots in the Late Bronze Age Eastern Mediterranean and Near East. *Ägypten Und Levante/Egypt and the Levant*, *20*, 67–181.

Ghauri, P., & Hassan, I. (2014). *Evaluating companies for mergers and acquisitions*. Emerald Group Publishing.

Gibbon, P., Ponte, S., & Lazaro, E. (2010). *Global agro-food trade and standards: Challenges for Africa*. Springer.

Gripsrud, G., Jahre, M., & Persson, G. (2006). Supply chain management–back to the future? *International Journal of Physical Distribution & Logistics Management*.

Gulati, R., & Gargiulo, M. (1999). Where do interorganizational networks come from? *American Journal of Sociology*, *104*(5), 1439–1493.

Gulati, R., Nohria, N., & Zaheer, A. (2000). Strategic networks. *Strategic Management Journal*, *21*(3), 203–215.

Gupta, B., Dasgupta, S., & Gupta, A. (2008). Adoption of ICT in a government organization in a developing country: An empirical study. *The Journal of Strategic Information Systems*, *17*(2), 140–154.

H\aakansson, H., & Ford, D. (2002). How should companies interact in business networks? *Journal of Business Research*, *55*(2), 133–139.

H\aakansson, H., & Snehota, I. (1989). *No Business Is An Island: The Network Concept Of Business Strategy', reprinted in Ford, David (ed.)(1990) Understanding Business Markets*. San Diego, California: Academic Press.

Hadjimanolis, A. (2000). A resource-based view of innovativeness in small firms. *Technology Analysis & Strategic Management*, *12*(2), 263–281.

Harland, C. M. (1996). Supply chain management: Relationships, chains and networks. *British Journal of Management*, *7*, S63–S80.

Hayes, M., & Whitebread, D. (2006). *ICT in the Early Years*. McGraw-Hill Education (UK).

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk–Definition, measure and modeling. *Omega*, *52*, 119–132.

Hindmoor, A. (1998). The importance of being trusted: Transaction costs and policy network theory. *Public Administration*, *76*(1), 25–43.

Jiang, W. (2019). Sustainable Development of Supply Chain in Footwear Industry–Take Nike as the Case. *Asian Business Research*, *4*(3), 86.

Johnsen, T., Wynstra, F., Zheng, J., Harland, C., & Lamming, R. (2000). Networking activities in supply networks. *Journal of Strategic Marketing*, *8*(2), 161–181.

Jüttner, U. (2005). Supply chain risk management. *The International Journal of Logistics Management*.

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, *6*(4), 197–210.

Kato, H., Tan, K. T., & Chai, D. (2010). *Barcodes for mobile devices*. Cambridge University Press.

Katz, H. (2020). Settlement Processes in the Meron Ridges During the Iron Age I. *Bulletin of the American Schools of Oriental Research*, *383*(1), 000–000.

Khan, O., & Burnes, B. (2007). Risk and supply chain management: Creating a research agenda. *The International Journal of Logistics Management*.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management*, *14*(1), 53–68.

Knapp, A. B. (2013). *The Archaeology of Cyprus: From Earliest Prehistory Through the Bronze Age*. Cambridge University Press.

Knippenberg, H., & Markusse, J. (2012). *Nationalising and denationalising European border regions, 1800–2000: Views from geography and history* (Vol. 53). Springer Science & Business Media.

Lamming, R., Johnsen, T., Zheng, J., & Harland, C. (2000). An initial classification of supply networks. *International Journal of Operations & Production Management*, *20*(6), 675–691.

Laudon, K., & Laudon, J. (2006). *Management information systems: Managing the digital firm*. New York: MacMillan.

Lavassani, K. M., & Movahedi, B. (2010a). Critical analysis of the supply chain management theories: Toward the stakeholder theory. *POMS 21st Annual Conference, Vancouver*.

Lavassani, K. M., & Movahedi, B. (2010b). Critical analysis of the supply chain management theories: Toward the stakeholder theory. *POMS 21st Annual Conference, Vancouver*.

Lavassani, K., Movahedi, B., & Kumar, V. (2008). Evolution of supply chain theories: A comprehensive literature review. *19th Annual Conference of the Production and Operations Management Society (POMS)*.

Luce, I. D. (n.d.). 10 companies that spent more than $1 billion in ads so you'd buy their products. Retrieved June 3, 2020, from Business Insider website: https://www.businessinsider.com/10-biggest-advertising-spenders-in-the-us-2015-7

Lysons, K., & Farrington, B. (2006). *Purchasing and supply chain management*. Pearson Education.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science*, *33*(11), 1404–1418.

McNichols, T., Brennan, L., & Middel, R. (2006). *Facilitating collaboration in e-supply chain systems: An action learning-based approach*.

Merrick, H. V., & Brown, F. H. (1984). Obsidian sources and patterns of source utilization in Kenya and northern Tanzania: Some initial findings. *African Archaeological Review*, *2*(1), 129–152.

Messenger, J. C., & Gschwind, L. (2016). Three generations of Telework: New ICT s and the (R) evolution from Home Office to Virtual Office. *New Technology, Work and Employment*, *31*(3), 195–208.

Miles, R. E., & Snow, C. C. (1992). Causes of failure in network organizations. *California Management Review*, *34*(4), 53–72.

Miles, R. E., & Snow, C. C. (2007). Organization theory and supply chain management: An evolving research perspective. *Journal of Operations Management*, *25*(2), 459–463.

Mills, J., Schmitz, J., & Frizelle, G. (2004). A strategic review of "supply networks." *International Journal of Operations & Production Management*.

News, F. (12:28+02:00). Sentences of up to 13 years for ATM robbers. Retrieved June 2, 2020, from Vrtnws.be website: https://www.vrt.be/vrtnws/en/2019/09/18/sentences-of-up-to-13-years-for-atm-robbers/

Norrman, A., & Lindroth, R. (2004). Categorization of supply chain risk and risk management. *Supply Chain Risk*, *15*(2), 14–27.

Pitelis, C. N., & Pseiridis, A. N. (1999). Transaction costs versus resource value? *Journal of Economic Studies*.

Ponis, S. (2010). *Managing Risk in Virtual Enterprise Networks: Implementing Supply Chain Principles: Implementing Supply Chain Principles*. IGI Global.

Quinn, J. B., & Hilmer, F. G. (1994). Strategic outsourcing. *MIT Sloan Management Review*, *35*(4), 43.

Rahman, M. M., & Kumaraswamy, M. M. (2002). Joint risk management through transactionally efficient relational contracting. *Construction Management & Economics*, *20*(1), 45–54.

Şen, Ş., & Babalı, T. (2007). Security concerns in the Middle East for oil supply: Problems and solutions. *Energy Policy*, *35*(3), 1517–1524.

Shook, C. L., Adams, G. L., Ketchen, D. J., & Craighead, C. W. (2009). Towards a "theoretical toolbox" for strategic sourcing. *Supply Chain Management: An International Journal*.

Silverstein, B. (2020). Managerial Opportunism and Corporate Investment Efficiency. *Available at SSRN 3463419*.

Stanton, T., & Webster, D. W. (2014). *Managing Risk and Performance: A Guide for Government Decision Makers*. John Wiley & Sons.

Svensson, G. (2002). A conceptual framework of vulnerability in firms' inbound and outbound logistics flows. *International Journal of Physical Distribution & Logistics Management*.

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, *103*(2), 451–488.

Vaswani, S. W., Karishma. (2020, January 31). How can China build a hospital so quickly? *BBC News*. Retrieved from https://www.bbc.com/news/world-asia-china-51245156

Von Bertalanffy, L. (1950). The theory of open systems in physics and biology. *Science*, *111*(2872), 23–29.

Vu, K. (2005). Measuring the impact of ICT investments on economic growth. *Journal of Economic Growth*.

Waters, D. (2011). *Supply chain risk management: Vulnerability and resilience in logistics*. Kogan Page Publishers.

Williamson, O. E. (1986). Vertical integration and related variations on a transaction-cost economics theme. In *New developments in the analysis of market structure* (pp. 149–176). Springer.

WTO | Understanding the WTO - The GATT years: From Havana to Marrakesh. (n.d.). Retrieved May 17, 2020, from https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact4_e.htm

Wu, J. (2019, September 26). Dunkin' sued for cyberattacks resulting in tens of thousands of dollars stolen. Retrieved June 5, 2020, from CNBC website: https://www.cnbc.com/2019/09/26/dunkin-sued-for-cyberattacks-resulting-in-tens-of-thousands-of-dollars-stolen.html

Yee, C. L., & Platts, K. W. (2006). A framework and tool for supply network strategy operationalisation. *International Journal of Production Economics*, *104*(1), 230–248.

Youssef, M. H., & Haj Youssef, M. (2013). Strategic tensions within the smartphones industry: The case of BlackBerry. *VISTAS: Education, Economy and Community*, *3*, 125–141.

Zaheer, A., Gulati, R., & Nohria, N. (2000). Strategic networks. *Strategic Management Journal*, *21*(3), 203.

Zhao, X., Liang, J., & Zhao, X. (2011). Research on the characteristics of supply chain risk conduction based on the self-organization theory. *2011 International Conference on Computer and Management (CAMAN)*, 1–4. IEEE.

Zsidisin, G. A. (2003). A grounded definition of supply risk. *Journal of Purchasing and Supply Management*, *9*(5–6), 217–224.

Zsidisin, G. A., & Henke, M. (2019). *Revisiting Supply Chain Risk*. Springer.

3.3 Appendice

3.3.1 Map of Belgium showing location of Limburg