Improving Supply Chain Management by enhanced Risk Management to minimize the Impact of Disruptions on Supply Chains

Dr. Nils Meyer-Larsen, Drs. Linda Drupsteen, Gerald Gräf, Laura Maier, Rainer Müller

Please leave this page blank

Abstract

Risk management, which is the identification and analysis of risks and their mitigation, is increasingly becoming a crucial factor in the management of international intermodal supply chains. On the one hand, security risks are addressed, especially since the terrorist attacks of 11 September 2001. Several laws, regulations, security procedures and technical measures to improve security were developed by the US, by international organisations and also by the industry. On the other hand, enhanced risk management also addresses operational risks which affect the logistics processes.

An important pre-requisite for risk management is the improvement of supply chain visibility, i.e. provision of the partners in the supply chain with high-quality data by accessing relevant data sources throughout the supply chain and integrating the different software systems. The latter of course is a challenge in a global scale and heterogeneous setting. Based on the availability of reliable data, both security and operational risks can be better identified and analysed. The next step is to develop mitigation strategies against the identified risks in order to make supply chains more robust.

This paper presents the research in this area. It describes different types of risks and assesses the possibility to mitigate these risks by improved supply chain visibility in order to improve the management of supply chains. Furthermore, methods to limit the impact of disruptions are discussed, which occur in case risks that affect vulnerable parts or aspects of the supply chain are not successfully mitigated.

Keywords: Supply Chain Management, Risk Management, Container Security, Supply Chain Visibility, Disruptions

1. Introduction

Risk management is increasingly playing a crucial role in the management of international intermodal supply chains. On the one hand, security risks are addressed, reflecting several laws, regulations, security procedures and technical

measures to improve security which were introduced after the terrorist attacks of 11 September 2001. On the other hand, enhanced risk management also addresses operational risks which affect the logistics processes. Of course, companies who integrate risk assessment into their supply chain management approach can still be confronted with disruptions in their operational flows. Successful companies are very resilient in dealing with these disruptions. They are able to mitigate the impact of disruptions, and can switch back to 'normal' operation in a relatively short time after an incident. By presenting key issues from research on supply chain risks and disruptions, this paper aims to contribute to more comprehensive knowledge on how disruptions can be used to reflect on companies risk management in supply chain. This study uses theoretical results from the CASSANDRA project (CASSANDRA, 2013; Drupsteen et al, 2013) and an analysis of security issues and related initiatives performed by the Institute of Shipping Economics and Logistics (Müller et al, 2013).

According to Liu et al (2012), the "current approach adopted by many supply chain managers is to leave the risk management to ex post compensation i.e. to ensure that potential losses will be reimbursed according to legislative frameworks and contractual agreements stipulated between business partners. The main problems of this approach are, first, the focus of risk management is drawn on to the financial losses but not on the root causes of the risks; second, the intermediary effect of the legislative frameworks decouples the chain of accountability, obscuring the risk-related visibility for supply chain management; and third, the lack of accountability and trust among the partners in managing one's own risk make the operations optimization on supply chain level very difficult. With the large and increasing volume of international trade, the scale of such cost and inefficiency is becoming phenomenal". Liu and his colleagues propose that disruption management at the company level should follow an integrated approach with respect to pre- and post disruption management, and that more cooperation within the supply chain is needed for successful disruption management (Liu et al., 2012).

2. Current security initiatives

As already mentioned above, several laws, regulations, and procedures to improve security were introduced after the terrorist attacks of 11 September 2001. The most important security initiatives are as follows (Müller et al, 2013):

- The C-TPAT (Customs-Trade Partnership Against Terrorism) certification (CTPAT, 2013) was established by the U.S. in 2001 in order to improve security in transports and to simplify the U.S. customs clearing process. On the EU side the AEO certification (Authorized Economic Operator) was introduced in 2008 in order to simplify the trade and the customs clearing in Europe. Mutual recognition between C-TPAT and AEO was agreed upon on July 1st 2012.
- In 2002 the Container Security Initiative (CSI) (CSI, 2013) was founded, which supports U.S. Customs and Border Protection (CBP) in order to estimate the security status of a container, based on container data provided by the Automated Manifest System (AMS) which is in use since 2003. AMS is a system to declare goods with the destination U.S. 24 hours before loading.
- The Importer Security Filling (ISF) contains the “10+2” and the “24 hour rule”. In detail, 10 data fields from the importer and two additional data fields from the shipping line have to be provided to CBP. On the basis of this data set a risk assessment is carried out by CBP in order to determine if the container may be loaded and imported to the U.S. or not.
- The Megaports initiative (Megaports, 2013), was founded in 2003 by NNSA (National Nuclear Security Administration), a subordinated agency of the U.S. Department of Energy (DOE). The main aim of this initiative is to control container transports on radioactive material on a global scale.
- The International Ship and Port Facility Security-Code (ISPS-Code) (ISPS, 2013), established in 2002 by the International Maritime Organization (IMO), describes the essential security measures to mitigate security risks at the port and on vessels. The main aims are on one side the provision of loading data from almost every ship arriving at a port and on the other side

an extensive access control for the authorities. In 2004 the European parliament applied the ISPS-Code into an EU regulation.

- The SAFE Port Act (Security and Accountability of every Port Act) (SAFE, 2013) was adopted in 2004 by the American Congress, building the frame for the active defense at the ports in the U.S.
- The H.R.1 (House of Representatives 1) bill, also called 100% scanning rule, has been adopted in 2007 by the U.S. Congress. According to this bill, any container with direction of the U.S. has to be scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel (Bennett, 2008). The H.R.1 became law on 01.07.2012. As at the moment no port is capable to fulfil the requirements concerning 100% scanning, the implementation of the law was postponed for two years until 2014.

This non-exhaustive list of existing security initiatives clearly demonstrates that huge efforts are taken by authorities and businesses in order to improve the security status of international transports and to assess and minimize security risks which occur in relation to those transports. As a matter of fact, all of these initiatives of course put additional demands on the supply chain, and the non-observance of the related requirements will result in detaining consequences, thus implying additional risks for the supply chain especially from the business perspective. This fact has to be taken into account in order to establish efficient mechanisms to deal with all possible kinds of risks and disruptions.

3. Disruptive events

The definition of a supply chain disruption according to Behdani (2012) is “an event that might happen in any part of a supply chain and causes undesired impacts on the (achievement of) objective and the performance of supply chain. As a corollary, if an event has no adverse effect on the achievement of objectives, it is not regarded as a disruption”. Craighead et al. have a similar definition, more focused on the flow of goods, in which supply chain disruptions are “unplanned and unanticipated events that disrupt the normal flow of goods and materials within a supply chain” (Craighead, 2007; p. 132).

If the identified risks are managed well, they will not lead to disruptions. However, not all disruptions can be predicted and “even for disruptions that companies expect, they cannot afford to invest in preventing all of them” (Behdani, 2012). Consequently, it is not possible or economically sensible to attempt dealing with every possible disruption in the supply chain. For those disruptions that cannot be prevented, more attention might be paid to the response side of the disruption management process. For instance, for rare events like an earthquake, companies would prefer a contingency tactic, as contingent costs are incurred only in the event of a disruption (Tomlin, 2006 in Behdani, 2012).

Not all risks can be managed, nor can all disruptions be predicted. Many studies have been performed to identify what kind of disruptions do occur and what their impact on the supply chain is. However, different terminologies are used in the studies that seem to be intertwined. Some studies discuss risks that could result in disruptions, others focus on threats and a third category identifies sources for disruptions. A fourth category focuses on vulnerabilities, meaning the susceptibility of the supply chain to the likelihood and consequences of disruptions (Blos et al., 2009). These studies have in common that they focus on situations or events that might lead to a disruption in the continuity of the supply chain and on the conditions that allow for the disruption to have effects on the supply chain operation. In the CASSANDRA project (CASSANDRA, 2013) main risks for the supply chain, and therefore possible disruptions are identified. The risks are categorized into three groups: business or operational risks, such as delays and quality loss crime related risks and other risks, including environmental risks.

The crime related risks were identified in the European FP7 project LOGSEC (LOGSEC, 2013) which identified security threats that might lead to disruptions. The most commonly mentioned form of crime in the LOGSEC project was theft in transit, followed by cybercrime. Cybercrime was also listed as one of three main causes for disruptions in a survey report of the Business Continuity Institute (Business Continuity Institute, 2012). Results from the survey study in supply chains in 62 countries indicated adverse weather as the main cause of disruption to supply chain continuity. The second most likely disruption was unplanned IT and telecommunication outages and the third most likely disruption category was cybercrime.

Kleindorfer and Saad (2005) studied disruptions in supply chains in the Chemical industry in the U.S. The conceptual model that they used for the study distinguished between three disruption risk sources: operational risks, risks arising from natural hazards and risk arising from terrorism or political instability.

A study that focuses on the process that is disrupted as a consequence instead of on the risk of a disruption is that of Rice and Caniato (2003, in Behdani et al, 2012). Rice and Caniato (2003) focus on failure modes in the supply chain, meaning the consequences of an event. They claim that while there are many types of risk, there is only a limited set of possible outcomes or impacts from those risks. They identified five failure modes, which are: disruptions in supply, in transportation, in facilities, in communications or in human resources. This approach is especially interesting since the assumption of this project is that disruptions do occur, so the sources for the disruption or the risks couldn't be managed or weren't managed sufficiently.

4. Disruption management

There are multiple models that describe disruption management cycles or processes. Blackhurst et al. (2005) for instance described the steps after a disruption happens in three main steps: disruption discovery, disruption recovery and supply-chain redesign to become more resilient in the future. Behdani et al (2012) mention four steps: detection, reaction, recovery and learning. Those steps are similar to those of Blackhurst et al (2005), but distinguish between an immediate response to manage the impact and the recovery to normal situations. Pyke and Tang (2010) emphasize the cyclical nature of disruption management in their three stages of supply chain management: readiness, responsiveness and recovery. The other models included a step on learning or supply chain redesign, which are the inputs for what is called readiness in the model of Pyke and Tang (2010).

Common denominators in these models are the cyclical nature of the disruption management process and the distinctions between detection of the event, response and learning. In the following we will describe some possibilities for preparation that are already known, followed by a description of detection and response in relation to a disruption.

4.1 Readiness: creating a resilient supply chain

Knowing that at some point disruptions will occur, it is recommended to prepare for that moment. Prior knowledge about potential environmental, social, and political conditions, about risk factors and about effects on the organization if a disruption occurs can help companies prepare. According to Ponomarov and Holcomb, preparation is an important aspect of resilience, which is "the adaptive capability of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them by maintaining continuity of operations at the desired level of connectedness and control over structure and function" (Ponomarov and Holcomb, 2009, p.131). This section describes two important aspects in preparation: the first is to prepare emergency response plans so that adequate measures are taken if an unwanted event occurs. Based on the risk assessment and vulnerability index, some disruptions can be 'expected'. To recover from those events once they occur, emergency plans are needed, including actions and agreements on who should do what in case the disruptions occur. Those emergency plans can be specific for typical disruptions, such as for theft or IT failure, but they could also be generic. Generic response plans are also needed for the yet unknown disruptions that cannot be predicted.

The second aspect is to reduce the possible effects of disruptions. In general, the possible response to a disruption can fall within four categories: Risk acceptance, Risk avoidance, Risk transfer or Risk reduction. Avoidance and transfer are related to risks that are already identified. However, this report focuses on the process that occurs after an unwanted event, meaning that the risk could not be avoided or transferred. Here we therefore describe possibilities to reduce the impact or the likelihood of disruptions. By reducing the risks, the likelihood that emergency response plans are needed are decreased. One option which allows for a better response to an abnormal situation and to rapidly adapt to significant changes in the supply chain is flexibility (Lee, 2004). The necessary condition for flexibility in the supply chain is having multiple interchangeable resources (Ji, 2009). Possible methods for risk mitigation through flexibility in the supply chain are: flexibility in product configuration, in transport, in the manufacturing process and in the supply base.

Another way to manage the risk of potential disruptions is creating redundancies across the supply chain. Flexibility mainly focuses on spreading options, but redundancy means you use extra back-ups. In general, redundancies are considered as expensive options for handling disruptions because they are put to use only when certain unanticipated events occur (Sheffi, 2005). For example, contracting with a local backup supplier to supply the needed material (or a part of it), when the main global supplier is disrupted, can be a costly decision. However, as a disruption occurs (e.g., an emergency in the main supplier facilities), the secondary supplier can be used to ensure a steady flow of materials across the chain.

In contrast with the unilateral control actions, co-operative responses to supply chain disruptions involve joint agreement/action by several actors in the chain (Jüttner et al., 2005). Two possible cooperative strategies are relevant: collective response planning and sharing resources and information. Collective response planning is especially important as modern supply chains are complex systems and no one actor has all the necessary information for identifying and mitigating the possible risks in the system (Butner, 2010). Additionally, in a joint risk management process, the options that might be too expensive to be implemented by a single partner can be discussed and agreed. Collaboration would help companies to pool resources and share the expenses of disruption response.

4.2 Detect

Despite enough safeguards, at a specific point, an actual disruption may happen. An effective response to a disruption requires detecting quickly the location and nature of disruption. To handle a disruption, the first step is detecting the location of disruption, its profile and the expected consequences on the system as quickly as possible (Drupsteen et al, 2013). With faster detection of disruption in the chain, corrective actions can begin quickly, the escalation of the disruption impact can be avoided, and consequently, the impact of the disruption can be reduced. Craighead (2007) states the importance of a warning capability which refers to interactions and coordination of supply chain resources to detect a pending or realized disruption and to subsequently disseminate information about the disruption to relevant entities within the supply chain.

In order to detect supply chain disruptions quickly, many enterprises are using shipment visibility systems. Such systems became widespread in the 1990s and are now familiar to consumers who use FedEx or UPS. Such tracking and tracing capabilities can help customers anticipate late shipments and sometimes detect abnormal patterns that can warn of larger problems (Sheffi and Rice, 2005). The coming deployment of radio frequency identification technologies may increase the ability to identify disruptions quickly by providing managers with an accurate and detailed picture of all inbound material and outbound goods at any given point in time. In case of a disruption, flows could be rerouted immediately and used where they are needed most (Sheffi and Rice, 2005).

For a faster detection of disruption, supply chain visibility is an advantage, meaning that there is clear visibility of all partners in the supply chain from suppliers to end costumers. This visibility is highest between actors that collaborate with each other and that easily share information, such as forecast demands, inventory levels, and processing capacities. To get the information, cohesion of the chain is relevant.

According to CASSANDRA (2013), risk, disruption and security should be dealt with in close interrelation in the supply chain security framework. Sources of risk can lead to disruption when they affect vulnerable parts or aspects of the supply chain. Vulnerabilities of the chain depend on the logistic structure and design of the chain (e.g. interdependencies) and the measures that have been taken to make the supply chain less vulnerable to certain risks. These security enhancing measures consist of analysis tools, and preventive and reactive measures. Both industry and authorities take security enhancing measures to avoid disruptions or reduce their impact. Analysis tools are a crucial part since these analyze the supply chain and give insight in the actual vulnerabilities, developments over time and the effect of taken measures. But of course analysis tools are as reliable and correct as the information that feeds them. This means that supply chain information that is used for risk (vulnerability) assessment is of crucial importance to both authorities and business, each for their own specific assessment goal (operations and security).The main outcome of this concept is a vision that should help defining how the data sharing concept developed within the CASSANDRA project could contribute to the sharing of information that will increase the resilience of companies and the whole supply chain in dealing with disruptions.

4.3 Respond (reaction and recovery)

After a disruption detected, a company must quickly react to cope with the impact and restore to the normal operation of the supply chain. The primary response will be on the basis of pre-defined response plans. If the pre-defined response plan is found inadequate to control the impact of disruption on supply chain or if no response plan has been defined for a specific disruption, the firms must quickly find alternative solutions and implement them to restore the normal supply network operations.

For a better reaction three key issues are listed in the literature: coordination of activities and actors. The disruption likely has an effect on multiple actors in the supply chain. Actions taken by one actor could in turn also have effect on other actors and therefore it is important to coordinate and if possible combine activities to respond to the disruption. Lack of coordination may also slow down the efforts to manage disruptions and worsen the effects. The second key issue is communication and information sharing, which is crucial for an early as possible detection of abnormalities. Also in reaction to the disruption continuous sharing of information is necessary, to make sure all information is combined. For instance suppliers might have other information than a shipper. With more information, a better estimate of successful mitigation strategies can be made and coordination is facilitated.

The third key aspect is resource finding and (re-)allocation. If the supply chain is disrupted, alternatives will be discussed: to have other suppliers, other manufacturers, etc. Based on the available resources, for instance found by combining resources of multiple partners, possible reactions to a disruption can be defined and implemented. It might be a challenge, since many objectives are to be considered. A simulation in which the reaction to a possible disruption is analysed can be helpful.

5. Conclusion

In this paper, we presented security initiatives which were especially implemented as a consequence of 11 September 2001. It was discussed that the respective measures at first sight enhance the security level of the transport, but on the other hand put additional demands on the supply chain, thus implying additional risks especially from the business perspective because the non-observance of the related

requirements will result in detaining consequences. Consequently, it is of vital importance that all kind of risks or possible disruptions are included in the respective analysis. Each organization at any part of the supply chain needs to reflect on the possibilities of a disruption and their effects on its process. Is this risk acceptable or not, and if not, what precautionary measures can be taken? Most events have an effect on multiple actors in the supply chain. However, the effects can be acceptable for one actor, but maybe not for another. This makes it difficult to create general recommendations. Each actor could decide for itself, for each identified disruption whether it is acceptable, avoidable or whether it is something to for which precautionary actions need to be taken. This paper described measures about introducing flexibility, control and redundancy from an organizational perspective. However, collaboration between actors in the supply chain is strongly recommended. Continuous information sharing is necessary for an early detection of abnormalities, to coordinate activities within the supply chain and also to know how your partners could possibly have an effect on your organization. Some information can be transferred through information hubs, or a data pipeline. However, real time information allows for quicker response, which can only be facilitated by better supply chain visibility. This includes not only knowing who you are hiring and what their normal process looks like, but that also second and third tiers are visible. Their risks factors, reliability and geographical spreading can affect your business too and, if your business is affected by other factors, they are your partners in recovering from the disruption.

As a summary, we conclude that the management of supply chains clearly benefits from improved risk management and the proposed measures to deal with disruptions because all those measures lead to enhanced mitigation of risks on the one hand or, if the risk cannot be successfully mitigated, to more resilient supply chains which are capable of mitigating the impact of disruptions in a more successful way, thus being able to resume ‘normal’ operations in a relatively short time after an incident occurred.

References

Behdani, Behzad, Adhitya, Arief, Lukszo, Zofia and Srinivasan, Rajagopalan (2012) How to Handle Disruptions in Supply Chains – An Integrated Framework and a Review of Literature (July 20, 2012).

Bennett (2008) Bennett, Allison C. & Yi Zhuan Chin, 100% Container Scanning: Security Policy Implications for Glob-al Supply Chains, Massachusetts Institute of Technology, 2008

Blackhurst, J., Craighead, C.W., Elkins, D. and Handfield, R.B. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions, International Journal of Production Research 43(19): 4067-4081.

Blos, M. F., Quaddus, M., Wee, H. M. and Watanabe, K. (2009). Supply chain risk management (SCRM): a case study on the automotive and electronic industries in Brazil, Supply Chain Management: An International Journal 14(4): 247-252.

Business Continuity Institute - BCI (2012). Supply Chain Resilience 2012 4th annual survey. Retrieved from http:://theBCI.org

Butner, K. (2010). The smarter supply chain of the future. Strategy and leadership 38 (1), p. 22-31.

CASSANDRA (2013) http://www.cassandra-project.eu, accessed 16 June 2013

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J. and Handfield, R. B. (2007) The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities. Decision Sciences, 38: 131–156.

CSI (2013) http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/, accessed 17th May 2013.

CTPAT (2013) http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/, accessed 17th May 2013.

Drupsteen, L. (2013) Cassandra D2.4 - Disruption management in the container supply chain

ISPS (2013) http://www.imo.org/ourwork/security/instruments/pages/ispscode.aspx, accessed 17th May 2013.

Jüttner, U. (2005). Supply chain risk management: understanding the business requirements from a practitioner perspective, The International Journal of Logistics Management 16(1): 120-141.

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

Liu, L., Oosterhout, M. van, Zuidwijk R. (2012) Cassandra D2.2 Risk based approach

LOGSEC (2013) http://www.LOGSEC.org, accessed 16 June 2013

Megaports(2013) http://nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5, accessed 17th May 2013.

Müller et al (2013) R. Müller, G. Gräf, N. Meyer-Larsen, and L. Maier: Improving Security through Visibility in Intermodal Transports, paper submitted for the IMAM2013 Conference, to be published

Ponomarov, S.Y. and Holcomb, M.C. (2009) Understanding the concept of supply chain resilience. International Journal of Logistics Management, The, Vol. 20 Iss: 1, pp.124 – 143.

Pyke, D. and Tang, C.S., (2010). How to mitigate product safety risks proactively-Process, challenges and opportunities, International Journal of Logistics Research and Applications 13(4): 243-256.

SAFE (2013) http://www.govtrack.us/congress/bills/109/hr4954/text. accessed 17th May 2013.

Sheffi, Y. and J. Rice (2005) A Supply Chain View of the Resilient Enterprise, MIT Sloan Management Review, 47 (1): 41-48.

Sheffi, Y. (2005) Preparing for the big one, Manufacturing Engineer 84(5): 12-15