

Jażdżewska-Gutta, Magdalena

**Conference Paper**

## Supply Chain Security Measures - The Business Perspective

**Provided in Cooperation with:**

Hamburg University of Technology (TUHH), Institute of Business Logistics and General Management

*Suggested Citation:* Jażdżewska-Gutta, Magdalena (2014) : Supply Chain Security Measures - The Business Perspective, In: Blecker, Thorsten Kersten, Wolfgang Ringle, Christian M. 978-3-7375-0341-9 (Ed.): Innovative Methods in Logistics and Supply Chain Management: Current Issues and Emerging Practices. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 18, epubli GmbH, Berlin, pp. 225-248

This Version is available at:

<https://hdl.handle.net/10419/209233>

**Standard-Nutzungsbedingungen:**

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

**Terms of use:**

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*



<https://creativecommons.org/licenses/by-sa/4.0/>

# Supply Chain Security Measures - The Business Perspective

Magdalena Jażdżewska-Gutta

## **Abstract**

Since 2001, supply chain security has become a vital issue for governments, international organizations, many business entities and scientific research. The governments and international organizations have introduced many regulations in order to make the trade flows more visible and protect them from unauthorized access. However, from the point of view of business sector, these regulations have sometimes a negative impact on supply chain activities. What is more, they are aimed mainly at protection from terrorism and smuggling of weapons of mass destruction, while the companies need protection in different areas, such as thefts in transit.

The aim of the study is to investigate the perceptions of managers on supply chain security threats and regulations, and to analyze the activities of the companies in the area of supply chain security management. The research is based on a survey conducted among 1200 exporters and importers from Germany and Poland. The survey reveals rather low awareness of security issues and that not many companies apply supply chain security measures. If they do, this is usually determined by customers and industry factors. They employ mainly reactive measures, such as buying insurance. Not many companies are interested in security certification. There are however some differences in the perceptions of German and Polish managers. The paper analyses these differences and proposes some measures that could be applied in order to protect the supply chains.

**Keywords:** transport chain security, supply chain security, supply chain security management, supply chain regulations

## 1. Introduction

Supply chain security in its present form emerged as a business, research and administrative issue after the terrorist attacks on September 11, 2001. The disruptions caused by such reactions as the post-attack closure of seaports and airports, affected a number of companies and their supply chains. The deliveries of many goods were delayed or cancelled, causing losses to business and the economy. Moreover, it occurred that the means of transport and entire transport network can be used by unauthorized persons for terrorist activity and smuggling of weapons of mass destruction. These events led policymakers from nation-states and international organizations to implement security policies for supply chains. They resulted in a number of regulations and security initiatives that are applicable to many supply chains around the world. These regulations are focused mainly on reducing the possibility of a terrorist attack through preventing unauthorized access to transport vehicles, containers and terminals, and through improving the supply chain visibility (Gould et al., 2010).

It was obvious that also business sector should be concerned about security issues. Many authors underline that recent global developments revealed the importance of supply chain security for all the supply chains and companies involved (Williams et al., 2009; Hintsa et al., 2009). European Commission recommended that security measures should be included by private industries in their daily operations (Commission of the European Communities, 2006). Hintsa and Hameri also point out that companies must also comply with the security regulations, which results in the changes of their organizational settings (Hintsa and Hameri, 2009). In order to secure their supply chains and to comply to the requirements of security regulations, the companies need to adopt specific security measures. However, the managers aware of the costs these measures

involve, very often abstain from dedicating special resources to supply chain security (Williams et al. 2008).

The aim of the study is to investigate the perceptions of managers on supply chain security threats and regulations, and to analyze the activities of the companies in the area of supply chain security management. While there are a lot of studies on customs and maritime transport, and relatively little attention is paid to the companies trading with the goods, the main focus of this study is on the exporters and importers. The first section of the paper explains the motivation of the research. The second section contains literature review on supply chain security measures applied by companies. The next section presents the methodology of the research and empirical findings. The analysis is based on a survey conducted among representatives of 1200 exporters and importers from Poland and Germany. The surveyed companies are present in international and global supply chains. They represent countries which play a vital role in the transport and logistics map of Europe. For those reasons, the survey provides a good overview of supply chain security issues in the European background and allows to analyze how the exporters and importers perceive the identified imperfections. The last section comprises discussion, recommendations for the companies and conclusions.

## **2. Literature review**

This section contains review of literature on supply chain security, risk and security measures. By integrating these areas it sets background for further empirical analysis.

### **2.1 Supply chain security and risk**

Supply chain security can be defined as a “general system property characterizing uninterrupted performance of a supply chain functioning to achieve its goals under protection against external purposeful threats” (Ivanov and Sokolov, 2010). To achieve that state of uninterrupted performance, the

companies and other entities must implement sets of security measures that are described as supply chain security management (SCSM). Closs and McGarrel provided also the definition of supply SCSM:

"Supply chain security management is the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain." (Closs and McGarrel, 2004).

It is important to mention, that the above definitions cover man-made threats and exclude natural disasters and other typical supply chain risks, which were listed by Mason-Jones and Towill: demand and supply side risks, manufacturing process risks and control system risks (Mason-Jones and Towill, 1998). These risks are a part of supply chain risk management (SCRM) and SCSM is considered to be a part of this concept (Markmann et al., 2013; Williams et al., 2008). Supply chain risk management is defined as:

"a collaborative and structured approach to risk management, embedded in the planning and control processes of the supply chain, to handle risks that might adversely affect the achievement of supply chain goals." (Pfohl et al., 2010).

Thus, the analysis of security threats to the supply chain involves risk analysis. Risk should be considered in terms of probability and severity or business consequences of the event (Brindley, 2004). The basic tool for such an analysis is the risk matrix, which can be also used for classifying security measures (Knemeyer et al., 2009). The risk matrix has two dimensions – disruption probability and consequences (business impact) which divide the risk into at least four sections. This analysis concentrates on the two sections that contain the most common security threats to the supply chains.

The section of high-probability/low-impact risk represents events that are a part of every-day functioning of the company or supply chain (Sheffi, 2007). These are mainly operational risks, such as pilferage, thefts in transit, even attacks on drivers, takeover of the cargo by false carriers, fraud. Such events, as those mentioned above, are usually taken into consideration by the managers when

developing security plans or risk management strategies. These risks are usually subject to insurance since they are quite common in business practice and easy to quantify.

The second group of risks covers catastrophic events that are characterized by low probability and high possible impact, such as terrorist attacks, organized crime, contraband of weapons of mass destruction and some others outside the scope of supply chain security – such as natural disasters. Such events can cause serious damage and negatively affect the functioning of supply chains.

The probability of such events is very low, for some firms the occurrence of such events is almost impossible. This is one of the reasons why companies usually ignore such risks, resign from developing and financing security plans and concentrate on the protection from low impact risks (Knemeyer et al., 2009).

Due to their properties, such events are also regarded as black swans (Aggarwal and Bohinc, 2012). Black swan events are unexpected, difficult to forecast and exert a significant impact on the supply chain and its surroundings (Taleb, 2007). The consequences of such event can be disastrous. The terrorist attacks on 9/11 are considered to be a black swan event.

## **2.2 Corporate vs. supply chain security**

It is important to add that estimating the risks to the supply chain is different from making the same estimates on corporate level. While corporate security is focused on risk strategies to protect an organization from security threats (Arway, 2013), supply chain security focuses more on the flows and the outside of the company. This should involve security risk assessment of the suppliers, providers and contractors along entire supply chain. The risks are therefore not limited to the company itself and should be aggregated, taking into account all links. Given the above, the results of possible events may be greater than one can realize. The company that wants to minimize risks to the supply chain should get a closer look on every link.

## **2.3 Motives for introducing supply chain security measures**

Speier et al. named several factors that influence the redesign of supply chains in terms of supply chain security. These factors include the mindfulness of the executives, supply chain complexity and risk associated with the product (Speier et al., 2011).

Williams et al. named four primary areas that create pressure for introducing SCS strategies – government, customers, competitors and society. Their research revealed that among these factors the government pressure affects the implementation of security measures the most (Williams et al., 2009). Pressure of governments is reflected in number of regulations, which can be mandatory or voluntary. The mandatory regulations require compliance from companies that want to participate in international supply chains. They are often seen as an obstacle to achieving higher efficiency and smooth functioning of supply chains. This is due to the fact that in many cases they raise cost and extend time of moving goods internationally. The voluntary programs often bring some benefits to the companies that decide to join them, and therefore can be regarded as facilitating tools rather than another obstacle.

The need for the cooperation between governments and companies was underlined by several authors (Sheffi, 2001; Rice and Caniato, 2003, Dulbecco and Laporte, 2005, Manuj and Mentzer, 2008). Ireland underlined also the important role of trust between customs authorities and trading companies for the sustainability of AEO Program (Ireland, 2011).

## **2.4 Proactive and reactive measures**

In the area of SCSM there are two basic types of measures: proactive and reactive, which both have a significant meaning for the supply chain resiliency. Proactive measures include identification of threats, risk assessment, development of standard procedures and their implementation, as well as their evaluation and continuous improvement. They lead to minimizing disruption risk. Briano et al. underlined that the success of recovery after a catastrophic event

happens, depends mostly on the actions that had been undertaken before the disaster occurred (Briano et al., 2009).

Reactive measures are the response to a disruption. Their effectiveness depends on the quality of introduced procedures, personnel actions that had been trained in drills and exercises, speed of eliminating the source of danger and its consequences. Insurance is an example of such reactive measures. Even if the insurance is bought before a disruption happens, its main goal is to minimize the loss and not to prevent the disruption.

The research by pwc (PWC, 2011) indicated that some managers discussed the importance and greater effectiveness of preventive over reactive security measures, while others suggested a balanced approach by combining both methods. This combination is the key to optimizing the costs and effects of security measures.

## **2.5 Costs and benefits of security measures**

Introducing security measures by companies requires some expenditures to be incurred. These expenditures include expenses for physical security, technical equipment and its maintenance, additional personnel salaries, training, information processing and data analysis and communication (Allen, 2007).

However, security measures result not only in costs but also bring some benefits to the companies. Allen distinguished the following benefits of introducing security measures: lower exposure to losses resulting from WMD smuggling, terrorist activity, crime and fraud, higher reliability of entire supply chain and improved tracking of cargo (Allen, 2007).

## **3. Methodology**

The data were collected from a questionnaire survey that took place between June and August 2013. The survey was conducted in the form of computer assisted telephone interview which allowed to achieve high response rates. On request the respondents were additionally given the link to the online survey in



order to have a better insight into the survey. Interviewers responsible for the survey had been trained in the area of supply chain security in order to be able to explain more difficult questions to the respondents.

The questionnaire consisted of closed-ended questions with a given list of threats and measures. The answers to the questions were derived on the basis of previously conducted researches and literature. Such questions allowed better generalization of data, especially for such a big sample, and gave the respondents more ideas to choose from, in comparison to open-ended questions. In many questions, however, the respondents were also given the opportunity to add their own answers if they recognized the given examples insufficient. In most questions the respondents were to choose more than one answer. The questionnaire was prepared in two languages - Polish (for Polish respondents) and German (for German respondents), in order to avoid any misunderstandings resulting from language competences. The actual survey was proceeded by a pilot study that allowed to verify the survey questionnaire and eliminate the inefficiencies. Each interview took from 30-40 minutes depending on the interviewer.

The sample consisted of 600 companies from Poland and 600 companies from Germany. The companies chosen for the research were exporters and importers (within and outside the EU) of goods which places them as the links in international supply chains. The sample covered exporting companies (39,4% of the sample), importers (13,8%) and companies that both exported and imported goods (46,8%). All these companies were exporting or importing goods in such industries as food, wood, chemical, machinery, metal etc. Companies active in such fields as mining, building or services (apart from trade) were excluded as most of the questions in the survey related to physical movement of goods. The size of the companies was differentiated, from micro and small companies, that constituted 56,7% of the sample to big companies that represented 12,5% of all surveyed companies.

The respondents were either the owners of the companies (24,5% of respondents) or managers responsible for export, transport or logistics (27,9%),

or employees responsible for export, transport or logistics (47,3%), depending on the structure of the company.

The countries were chosen for the research on the basis of their role in European transport sector. As most of the regulations come from the United States, the European perspective might throw a new light on this problem. Other criteria for choosing this country include relatively high importance of inland transport in both countries and relatively high importance of transport and logistics industry. Both Germany and Poland are transit countries which is an important feature concerning supply chain security. In terms of supply chain security, both countries hold relatively many AEO certificates, however there is a significant difference between them, as German companies hold more Certificates in the area of security, while Polish companies are mainly focused on gaining customs preferences, which might indicate that German companies are more aware of the security issues.

## **4. Results**

### **4.1 Threats**

In order to assess the perception of the managers on supply chain security threats, respondents were asked if the specific threat relates to their supply chain (table 1). Respondents could choose any threat they considered dangerous for their supply chains. Most companies indicated the following threats: thefts of cargo and vehicles in transit, thefts of goods in terminals and warehouses, overtaking the cargo by false carriers, breach of information security and counterfeit.

Threat	Germany				Poland			
	Mean	SD	Nr. of co.	Rank	Mean	SD	Nr. of co.	Rank
Pirate attack	2,50	1,732	4	1	3,11	1,423	27	3
Smuggling of WMD in the container where cargo was placed	2,43	1,813	7	2	2,90	1,611	29	8
Overtaking of cargo or vehicle for ransom	2,20	1,687	10	3	3,08	1,275	50	4
Thefts of goods in terminals and warehouses	2,20	,963	95	4	2,84	1,172	119	9
Terrorist attack	2,13	1,808	8	5	3,28	1,579	29	1
Breach of information security	2,06	1,111	47	6	3,23	1,389	57	2
Thefts of cargo or vehicles in transit	1,97	,900	86	7	2,91	1,037	168	7

Threat	Germany				Poland			
	Mean	SD	Nr. of co.	Rank	Mean	SD	Nr. of co.	Rank
Using the vehicle, where the co.'s cargo is placed, for smug. goods	1,90	1,221	21	8	2,83	1,372	47	10
Counterfeit	1,75	1,180	36	9	2,94	1,300	50	6
Overtaking of cargo by false carriers	1,52	,727	52	10	3,02	1,361	62	5

Tab.1: Respondents' perception of threats to the supply chains. Source of the figure: Own elaborations based on empirical research

Then the interviewees were asked to evaluate the chosen threats, using a scale from 1, which indicated very low danger to the supply chain, to 5, which indicated very high danger. Most of the threats were evaluated quite low in term of their severity to the supply chains. The highest ranking belongs to pirate attack (among German respondents) and terrorist attack (Polish respondents). However not many companies believe that these events might threat their supply chains. This might mean, that these threats are not taken into consideration by companies while preparing security plans. Following this assumption – not many companies might be willing to pay extra security fees to protect themselves from such disruptions.

## 4.2 Regulations

The research revealed that most companies do not consider these regulations as a burden. Only 10,2 % of Polish companies and 7% of German companies

noted that the regulations are burdensome. Most of these companies mentioned bureaucracy as the main burden. Some companies mentioned also higher costs (more in Poland than in Germany), the necessity to provide too detailed information on the product, and extended time of delivery. One of the reasons for such low response in this matter is that exporters and importers usually use the services of freight forwarders and logistics operators for shipping cargo and often do not get a complete information on all the procedures and a detailed cost breakdown. Thus exporters and importers are not always aware of all security fees and documents that are required for transport process and may perceive security regulations as less burdensome than they actually are.

On the other hand, much more companies were affected by the security regulations (22,2 % of German and 26,8 of Polish companies), and, in most cases, the impact was negative. The most frequent responses included additional costs, longer delivery times, delays due to inspection of cargo and the need to employ additional persons to handle the security documentation.

Although security regulations are considered to have a rather negative impact on supply chains, there are also some benefits. However, most of the companies in the research did not mention any positive impact of security regulations on their supply chains. A few companies mentioned that with these security regulations the transport of cargo is more secure. This is done by reducing the risk of unexpected events that could cause serious damage or disrupt the functioning of supply chains. Thus, exporters and importers can benefit from the lower risk of major delay, damage to assets or loss of cargo.

### 4.3 Security measures

The respondents were asked if there were any specific internal security measures or security management system introduced in their companies. The answers are presented in table 2.

Less than 10 per cent of managers declared having a complex supply chain security management system. Almost 20 per cent of German companies and almost 30 per cent of Polish companies introduced single procedures. What is important, most of the managers claimed that their companies did not introduce any procedures at all. However, this might be caused by low level of knowledge on supply chain security as in the next question more companies declared having introduced some procedures in order to enhance the security of supply chains.

Has the company introduced any specific internal security measures or security management system?	Percentage of German respondents	Percentage of Polish respondents
Yes, we have introduced complex supply chain security management system	8,2	8,8
Yes, we have introduced single procedures or sets of security measures	19,5	29,2
No, we haven't introduced any procedures	72,3	62,0

Tab. 2: Internal security procedures. Source of the figure: Own elaborations based on empirical research.

The respondents were also asked for the motives for introducing security measures (table 3). They could choose from a list of motives (more than one) or add their own answer.

The most important factors for both German and Polish companies were the requirements of public authorities and customers, and product and industry factors. Companies that represent strategically important industries, such as defense industry, or vulnerable industries such as pharmaceutical, are more

dependent on industry factors than others. They are obliged to introduce specific security measures. Surprisingly, many managers, especially from Germany, mentioned that security measures are an element of company's general strategy or supply chain risk management strategy. On the other hand, the AEO certification, which might be expected to take a high position in the ranking, was evaluated as the least important motive. The survey reveals that European Union AEO certification program, is not of interest to the companies. Only 4,5 per cent of Polish respondents and 2,2 per cent of German respondents declared having AEO certificate. What is more, in most cases this was the Customs certificate (AEO-C), which does not directly cover the area of security.

Motives	Germany		Poland	
	% of respondents	Rank	% of respondents	Rank
As an element of our general strategy or supply chain risk management strategy	14,5	1	4,0	6
Product and industry factors	14,0	2	8,7	3
Requirements of public authorities	13,2	3	10,3	2
Due to customer requirements	13,0	4	15,5	1
Due to requirements of transport and logistics providers	11,3	5	2,3	7

Motives	Germany		Poland	
	% of respondents	Rank	% of respondents	Rank
Following competition or increasing competitive advantage	10,5	6	1,2	11
As an element of CSR strategy, for social benefits	8,3	8	4,2	4/5
Because not all areas of supply chain security are regulated	8,2	9/10	1,2	10
For benefits at customs clearance	6,0	11	2,0	9
For AEO certification	3,8	12	0,7	13
For reducing possible losses due to criminal activity	3,0	13	4,2	4/5

Tab. 3: Motives for introducing security measures. Source of the figure: Own elaborations based on empirical research.

#### 4.4 Security measures

Knemeyer et al. described two fundamental features of security countermeasures: their impact on overall probability of catastrophic event and their impact on estimated loss that would be incurred from disruption (Knemeyer et al., 2009). The positive fact is that companies put more effort into implementing proactive measures that aim to minimize the probability of disruption, such as video monitoring, tracking of cargo, control of the carriers or subcontractors. However it is important to mention that many companies are not interested in any security measures. As a result they are more exposed to risk.



The survey reveals that there were significant differences between Polish and German companies in the area of security measures they implemented (table 4.). The interviewees could choose from the list of security measures (more than one answer could be chosen) or add their own answer. First of all, German respondents declared generally more security measures than Polish ones. German exporters and importers are more eager to incur high expenses for new technologies, such as video monitoring systems and using seals and intelligent containers. On the other hand, more Polish respondents declared buying insurance, which is only a reactive measure. Knemeyer claims that insurance as a reactive measure is used only for minimizing losses and does not influence the probability of a disruption (Knemeyer et al., 2009).

Personnel selection and training is another area where significant differences can be found. According to the survey, Polish managers attach less importance than German respondents to instructions and training for employees in the area of continuous monitoring of security, analysis of the profiles of candidates for work in terms of security, and unannounced drills and exercises. That area should be improved in both countries as the personnel is the key to supply chain security. Even the best technology does not provide the best security if there are no skilled people to make use of that. It is worth mentioning that the attitude of the personnel is the element of supply chain security culture and is vital for enhancing security (Williams et al., 2009 [2]). According to this philosophy, the supply chain security should become a priority for the employees. The survey shows however, that companies do not attach much importance to that issue.

The opinions gathered from the survey reveal also, that security measures are mainly focused on preventing the supply chains or single companies from high-probability, low-impact threats such as thefts. Other studies show, that in case of low-probability high-impact events companies usually decide to do nothing and accept the risk (Knemeyer et al., 2009, Chopra and Sodhi, 2004). Instead of concentrating on such risks, business attaches more attention to reducing costs and enhancing efficiency (Aggarwal and Bohinc, 2012).

Financing security measures is another important issue. Security can be financed by users, public or private sources (Dulbecco and Laporte, 2005). In case of security regulations, especially in sea transport, the most costs are incurred by transport companies which pass them to exporters and importers. Finally, this is usually the customer who pays for the security as the costs are hidden in the final price of the product. However, from the point of view of an exporter or importer, the security expenses in terms of compliance to regulations are costs that negatively influence the overall effectiveness of the supply chain and do not bring major benefits such as improving processes or creating efficiencies.

The survey reveals that this is the private sector who should take care of security, either on their own or with cooperation with governments or international organizations (table 5). The interviewees could choose from the list of entities (more than one answer could be chosen).

Supply chain security measure	% of German respondents	Rank for Germany	% of Polish respondents	Rank for Poland
Video monitoring systems	59,2	1	8,8	8
Seals and intelligent containers	50,2	2	20,5	2
Cargo insurance	35,7	3	71,3	1
Cargo tracking	30,7	4	20,0	3
Instructions and training for employees in the area of continuous monitoring of security	27,3	5	11,5	5

Supply chain security measure	% of German respondents	Rank for Germany	% of Polish respondents	Rank for Poland
Analysis of the profiles of candidates for work in terms of security	26,3	6	7,0	9
Control and risk analysis of suppliers	18,2	7	12,2	4
Permanent cooperation with suppliers and customers within the supply chain	15,3	8	11,3	6
Control and risk analysis of carriers, freight forwarders and other subcontractors	12,2	9	6,0	10
Guidelines for carriers on the use of guarded parking areas	10,2	10	9,2	7
Permanent cooperation with public entities for enhancing security	10,0	11	3,7	13
Protection of information and computer systems from unauthorized access	9,2	12	4,0	11
Direct control of loading cargo in order to avoid smuggling	8,7	13	5,7	12

Supply chain security measure	% of German respondents	Rank for Germany	% of Polish respondents	Rank for Poland
Complex risk identification and assessment in supply chain (security auditing)	5,8	14	2,7	14
Unannounced drills and exercises	5,2	15	1,5	15

Tab. 4: Security measures implemented by companies. Source of the figure: Own elaborations based on empirical research.

Who should take care of supply chain security?	% of German companies	% of Polish companies
Companies on their own	40,5	52,3
Companies in the cooperation with international organizations	31,6	19,3
Companies in the cooperation with governments	26,0	36,8
Countries and governments	13,8	14,2
International organizations	9,3	9,5

Tab. 5: Opinions on the entity which should be responsible for enhancing security. Source of the figure: Own elaborations based on empirical research.

The regulations do not protect the supply chains from every kind of threat and the companies need to act on their own. Fight with piracy is a good example of such activity. The governments send navy ships to protect commercial vessels from pirate attacks, however this is usually not enough and carriers hire private maritime security companies. The cost of protecting vessel is usually passed to exporters and importers by applying higher freight rates or special surcharges.

In order to enhance the effectiveness of security solutions and better protect the supply chains, companies need to build their own security plans and incorporate mandatory regulations into them. Companies should also manage the security across the supply chain, by tight control, especially in case of new business partners, and building long-term relationships and trust with other links in the supply chain. Another possibility is to join voluntary security programs. Such programs are also a cost for a company but are considered to bring also benefits, such as less controls at the border, gaining competitive advantage and improving the overall security.

## **5. Conclusions and recommendations**

It became obvious that due to long-term trends of globalization, outsourcing and lean management strategies, the supply chains became more vulnerable to any disruptions. Due to the character of supply chains, the consequences of a disruption can be more serious than we expect, as the single threats to any company involved in the flow of goods sum up along the supply chain. It is thus important that companies attach enough importance to implementing supply chain security measures. However, the majority of surveyed exporters and importers underestimate the importance of supply chain security and many of them did not introduce any security measures. What is more, some respondents, especially from small companies, were not acquainted with the issue of supply chain security and did not know anything on certification programs such as AEO. This means that the customs authorities, international organizations and governments could put more effort into providing business with security information.

The surveyed companies concentrated mainly on high-probability, low-impact risks, while low-probability, high-impact risks are by them ignored or absorbed. They try to implement proactive measures but also attach much importance to insurance which is a reactive security measure. There is a significant difference between the decisions of Polish companies on buying insurance and

implementing other security measures. German respondents, in turn, attached greater importance to using technology such as video monitoring and intelligent seals and containers.

The analysis of motives behind the introduction of security measures reveals that respondents take into consideration mainly obligatory issues, such as pressure of public authorities and product and industry factors, and pressure of customers. The latter element is not strictly mandatory but every company that wants to sell its products must take into consideration the requests from its customers. It is however worth mentioning that for German respondents the main motive for introducing security measures was the fact that this is an element of their general strategy or supply chain security philosophy, however they constituted only 14,5 per cent of all surveyed companies.

Another fact worth mentioning is that respondents underestimate the importance of personnel in enhancing security. This is the area where the most effort should be put. As mentioned before, the awareness of security issues helps to create supply chain security culture. The organizational culture is a crucial success factor for introducing supply chain security culture (Williams et al., 2009 [2]). However many, especially small, companies are missing this element. Total Security Management is another philosophy that can be introduced for enhancing supply chain security (Ritter et al., 2007). It originates from Total Quality Management (TQM) and allows to achieve higher security at lower costs due to the fact that security is built in the processes (Lee and Whang, 2003).

It is also worth mentioning that security solutions are expensive. Applying the TSM approach allows to lower the overall costs but still some expenses need to be incurred. In this context, usually the biggest companies become beneficiaries of the introduced security measures. Small companies will decide to ignore the threats even if they are still exposed to the risks as the expenses for security would be too high.

## **Acknowledgements**

The research project was financed by funds of the National Science Centre (Poland) allocated on the basis of the decision no. DEC-2012/05/N/HS4/00592.

## References

- Aggarwal R., Bohinc J., 2012, "Black swans and supply chain strategic necessity", *Journal of Transportation Security* 5.
- Allen, C.H., 2007, The Role of Competent International Organizations in Developing the International Supply Chain Security Regime, *Journal of Management Science*, vol. 1, No. 2.
- Arway A. G., 2013, *Supply chain security: A comprehensive approach*, CRC Press, Boca Raton, pp. 33.
- Brindley C., 2004, *Supply Chain Risk*, Ashgate Publishing.
- Chopra S., Sodhi M.S., 2004, Managing Risk to Avoid Supply Chain Breakdown, *MITSloan Management Review*, Vol. 46, No. 1.
- Closs D.J., McGarrel E.F., 2004, *Enhancing Security Throughout the Supply Chain*, The IBM Center for the Business of Government.
- Commission of the European Communities, 2006, Proposal for a Regulation of the European Parliament and of the Council on enhancing supply chain security. Impact assessment, SEC(2006)251.
- Dulbecco P., Laporte B., 2005, "How can Security in International Trade be Financed in Developing Countries? A Global Public Good Approach", *World Development*, Vol. 33, No. 8, pp. 1201-1214
- E. Briano, C. Caballini, R. Revetria, 2009, Literature review about supply chain vulnerability and resiliency, *Proceedings of the WSEAS International Conference on SYSTEM SCIENCE and SIMULATION in ENGINEERING*.
- Gould J. E., Macharis C., Haasis H.-D., 2010, "Emergence of security in supply chain management literature", *Journal of Transportation Security* (2010) 3.
- Hintsa J., Hameri A.P., 2009, Security Programs as Part of Efficient Supply Chain Management, *Supply Chain Forum*, Vol. 10, No. 2.
- Hintsa J., Wieser P., Gutierrez X., Hameri A.-P., 2009, "Supply chain security management: An overview", *International Journal of Logistics Systems and Management*, Vol. 5., 3/4, p. 344-355.
- Ireland R., 2011, *The Customs Supply Chain Security Paradigm and 9/11: Ten Years On and Beyond*, WCO Research Paper No. 18.
- Ivanov D., Sokolov B., 2010, *Adaptive Supply Chain Management*, Springer Verlag, London, pp. 81.
- Knemeyer A.M., Zinn W., Eroglu C., 2009, "Proactive planning for catastrophic events in supply chains", *Journal of Operations Management* 27, pp. 141-153.
- Lee H.L., Whang S., 2003, *Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management*, October.



- Manuj I., Mentzer J.T., 2008, Global supply chain risk management strategies, *International Journal of Physical Distribution & Logistics Management*, Vol. 38 No. 3, pp. 192-223.
- Markmann C., Darkow I.L., von der Gracht H., 2013, A Delphi-based risk analysis – Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment, *Technological Forecasting and Social Change* vol. 80 issue 9 November, pp. 1815-1833.
- Mason-Jones R., Towill D.R., 1998, Shrinking the supply chain uncertainty circle, *Control*, September.
- Pfohl H.-C., Köhler H., Thomas D., 2010, State of art in supply chain risk management research: empirical and conceptual findings and a roadmap for the implementation in practice, *"Logistics research"*, No. 2(1).
- PWC, 2011, *Transportation and logistics 2030, Volume 4: Securing the supply chain*.
- Rice J., Caniato F., 2003, Building a secure and resilient supply network, *"Supply Chain Management Review"*, September/October.
- Ritter L., Barrett J.M., Wilson R., 2007, *Securing Global Transportation Networks*, McGraw-Hill, New York.
- Sheffi Y., 2001, Supply Chain Management under the Threat of International Terrorism, *"The International Journal of Logistics Management"*, vol. 12, No. 2.
- Sheffi Y., 2007, *The Resilient Enterprise. Overcoming Vulnerability for Competitive Advantage*, The MIT Press, Massachusetts.
- Speier C., Whipple J.M., Closs D.J., Voss M.D., 2011, Global supply chain design considerations: Mitigating product safety and security risks, *Journal of Operations Management*, 29(2011), 721-736.
- Taleb N., 2007, *The Black Swan. The impact of highly improbable*, Random House, New York.
- Williams Z., Lueg J.E., LeMay S., 2008, Supply chain security: an overview and research agenda, *"The International Journal of Logistics Management"*, vol. 19, no. 2, pp. 254-281.
- Williams Z., Lueg J.E., Taylor R.D., Cook R.L., 2009, Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS), *"International Journal of Physical Distribution & Logistics Management"*, vol. 39, No. 7, pp. 595-618.
- Williams Z., Ponder N., Autry C.W., 2009[2], Supply chain security culture: measure development and validation, *"The International Journal of Logistics Management"*.