Gregor Veselko, Ph. D.
Intereuropa d.d.,
Vojkovo nabrežje 32
6000 Koper
Tina Bratkovič
University of Primorska
Cankarjeva 5
6104 Koper
Slovenia

Preliminary communication
UDC: 65.012.34
65.012.4
Received: 27th October 2008
Accepted: 25th February 2009

MANAGING RISKS AND THREATS IN GLOBAL LOGISTICS CHAINS

In comparison with local logistics chains, global logistics chains are exposed to a greater number of risks and threats. The reasons for a growing exposure of global logistics chains to risks and threats can be found primarily in their scope and structure. Global logistics chains expand throughout numerous countries and continents, thus including various links. This results in the need to coordinate an increasing number of links, cover greater geographic distances and use numerous transport means. It is true, however, that a logistics chain not capable of enabling a secure and smooth flow of goods cannot operate efficiently and attain required objectives. Therefore, the first step toward successful global logistics chains is the awareness of all logistics chain links with potential risks and threats arising in global business operations, while acquiring a set of knowledge and skills, with which companies are able to manage the risks and threats within the chain efficiently and successfully, represents the next step. As risk and threat management in logistics chains is becoming increasingly demanding, it is considered appropriate to study the issue of logistics chain security management in more detail and examine the importance of ensuring security for the efficient operation of logistics chains in global operations. It is essential to present the methods which the logistics chain links may use in order to reduce the risk and ensure greater security of business operations, for a secure logistics chain facilitates the establishment of mutual trust between business partners and thus promotes increased operational efficiency and success. Finally, the management of this field also proves as an excellent source for gaining competitive advantage, both for individual logistics chain links and for their businesses.

***Key words**: global logistics chains, logistics chain management in global business operations, risks, threats, risk and threat management.*

1. INTRODUCTION

Given the increasing exposure of logistics chains to risks and threats in global business operations, our objective is to examine, by analysing professional and scientific literature, the importance of logistics chain security management and present the methods by means of which the logistics chain participants may reduce operational risk and ensure greater security. The purpose of this article is to illuminate the significance of the appropriate management of risks and threats in logistics chains for establishing trust between logistics chain links and thus promoting efficient and successful performance of both individual logistics chain links and logistics chains as a whole, which has a positive impact on the economic growth of countries.

1.1. The issue of managing logistics chains in global business operations

Logistics chain management is affected by two dynamic factors: the globalisation process and the information technology development. The dynamics of the first factor provide guidelines to new forms of competition and new production locations, as well as influence the level of relative costs and the market size. The impact of information technology is even more pervading than globalisation itself, as it ensures global communication, enables process automation, changes the hitherto nature of business and creates new industrial branches. The merging of computers with telecommunications has changed the way people work and connected the entire world. Furthermore, the speed and unpredictability of environment changes causes managers to design only temporary and extremely adaptable solutions, characterised by fast responsiveness to market needs (Scharpy & Skjott-Larsen, 2001, p. 258).

It is much easier to operate in the local environment than beyond national borders, where companies must confront numerous changes, which may represent a risk in certain cases. The main differences between managing local logistics chains and managing global logistics chains lie primarily in geographic distances, different national regulations, difficulties in planning business events and different inspection mechanisms. The difficulties in global logistics chain management can also arise from different exchange rates, macroeconomic risks, infrastructure discrepancies, environmental protection requirements, diverse standards as well as from confronting different cultures. Longer transport routes most certainly dictate a greater exposure of goods to the risks in external environment. Moreover, companies encounter differently developed economies and infrastructures, which causes disruptions in the logistics chain and precludes the expected course of business. Since global logistics chains comprise of a combination of companies conducting different activities in different sectors, various forms of transport and capabilities of individual

operators intersect with each other. Therefore, the coordination of individual links in the logistics chain is crucial in order to achieve successful operation of the entire chain (Veselko, 2005, p. 358).

The complexity of logistics chain management increases with environment uncertainty and the rising number of companies in the logistics chain. Furthermore, transferring the implementation of specific activities to outsourcers increases the company's exposure to the risk that the activity would not be implemented as required or expected by the contracting entity. Companies build up greater safety stock than needed for the planned production due to mistrust, as they question the reliability of timely supply of the ordered material. Greater safety stock, which results in unnecessarily higher company costs, enables companies to buffer themselves against untimely deliveries of the raw material, other material and feedstock required for continued production. In order to prevent the accumulation of safety stock, it is necessary to establish mutual trust between the links in the logistics chain. However, the relationship of trust can only be established if appropriate operational security is ensured beforehand, which minimises the risk in cooperating with a business partner.

1.2. Reasons for a growing need to ensure security in logistics chains

The twenty-first century has brought numerous changes to the world economy, which put forth a growing need for greater security within logistics chains. One of the main factors is doubtlessly the phenomenon of an increasingly intensive globalisation and liberalisation of the economies which are based on the free movement of goods, people, capital and information. Due to the globalisation of supply markets and the transfer of production to places with cheaper labour force, logistics chains nowadays begin in one country and end in another country on a different continent. This is one of the reasons why logistics chains in global operations are exposed to a greater number of risks and threats than logistics chains operating only within the local environment. The next factor promoting the need for enhanced logistics chain security is the growing dependency of economies on efficient logistics chain operation. Ensuring greater security of global operations is thus also in the interest of government institutions. The final key factor lies in terrorist attacks, which represent a growing threat to logistics chains in global operations.

The need to ensure enhanced security is further dictated by the fact that maritime traffic is increasing as a consequence of liberalisation and globalisation, as it is precisely the container ships in global operations that are most exposed to terrorist threats. More than 90 percent of world trade involves container ships, amounting to approximately 20 million container transports annually (Lee, 2004, p. 2).

In Europe and the Mediterranean, there was a 40 percent increase in container traffic from 2000 to 2005. In comparison with 2004, the Koper port

achieved a 17.2 percent increase in container traffic in 2005, whereas the Reka port achieved a 25.3 percent growth, which is considered to be extremely substantial even when compared to the largest port in the world (Singapore), which had a 8.7 percent growth that year (Beškovnik, 2006, p. 9).

The facts enumerated above have presented companies, countries and the world economy with numerous challenges. One of the key challenges is undoubtedly to achieve balance between implementing measures for increasing security and keeping the flow of goods and information as smooth as possible.

The reasons for a rising exposure of logistics chains to business risk and the consequent growing needs for establishing a unified security system, which spreads throughout the entire logistics chain, are an increasing supply and demand uncertainty, the globalisation of buying and selling resources, shortened production and delivery times, and the use of production, distribution and logistics partners, which are made responsible for implementing certain activities (Veselko, 2003).

2. TYPES OF RISKS AND THREATS IN GLOBAL LOGISTICS CHAINS

Appropriate business policies, procedures and preventive measures can prevent a major part of risks and threats the companies face in global operations or at least mitigate possible negative consequences and their adverse effect. It is of great significance that companies are well informed about all potential risks and threats they may encounter.

Companies face the following business risks within logistics chains (Veselko, 2003):

- financial risk,
- chaos risk,
- market risk.

Financial risk can occur as a consequence of obsolete products, vanishing markets for them or shortage of product quantity. **Chaos risk** is a consequence of excessive reactions, unnecessary interventions and distorted information within the logistics chain. The latter may cause incorrect decisions and unconcerted action among logistics chain links. **Market risk** manifests itself as the incapability of exploiting business opportunities. When no appropriate system for obtaining market signals is established in the logistics chain, companies are unable to react to market changes and consumer needs in a timely manner. The consequence of these three types of risk is reflected in the operational inefficiency of logistics chains and incapability of satisfying end consumers.

According to Alan Braithwaite (2003, p. 7), global logistics chains are confronted with the following risks:

- risk of collaboration costs,
- risk of ineffective activity execution and poor quality products,
- demand risk,
- supply risk,
- environmental risk.

Braithwaite defined the first risk as the **risk of costs associated with collaboration** in the logistics chain (costs regarding transportation and handling goods, duty, infrastructure, inventory, etc.), which may be higher than anticipated by the company. Since the global logistics chain cannot be as responsive as the local logistics chain, there exists the risk of market loss due to the inability to respond to growing demand in a timely manner. **The risk of ineffective activity execution and poor quality products** arises as a consequence of the fact that numerous companies collaborate in the process of creating and delivering products. Companies transfer certain activities to their partners and thus lose some control over their implementation. The risk may also emerge if **know-how** is given away to companies, which allows them to enter the market. Furthermore, the author believes that operational and market transparency is less clear in global logistics chains, which leads to incorrect recognition of supply and demand trends. The risks encountered by companies in the external environment can be grouped into the following three classes: **demand risk, supply risk and environmental risk.** Both the supply risk as well as the demand risk are related to potential disturbances in the flow of products, services, financial resources and information between the point of origin and the end consumer. Environmental risk is the risk associated with natural disaster occurrence and cannot be controlled by the company. Natural disasters can affect companies and other market participants indirectly as well as directly, that is, through operations with other links of the global logistics chain, which suffered damage and consequently experienced disruptions in normal operations (Braithwaite, 2003, p. 7).

In addition to the described risks, international operations can also be marked by (Makovec Brenčič, 2005):

- risk in choosing business partners,
- payment risk,
- credit risk,
- foreign-exchange or currency risk,
- price fluctuation risk.

In order for a company to avoid the **risk in choosing business partners**, it is necessary to analyse all possible and available information about potential

business partners. Further on, **payment risk** is reflected in the possibility that a customer who already received the product does not settle the bill. To this end, there exist payment instruments, which help vendors to buffer themselves against potential non-payments. This also holds true in regard to **credit risk**, as vendors may encounter the risk of non-payment or payment delay. In international operations, **foreign-exchange risk** is of equal importance, as changes in currency value influence the agreed price (Makovec Brenčič, 2005).

According to Finch (2004, p. 185), threats within global logistics chains can be divided into three levels: the application, organisational and inter-organisational level.

Types of threats on the application level are as follows (Finch, 2004, p. 185):

- **natural disasters** (e.g. floods, thunderstorms, breakdowns of electricity, epidemics, etc.)
- **illegal acts** (e.g. sabotage, theft, terrorism, vandalism, smuggling, etc.)
- **low confidential data security** (e.g. hacker intrusions into systems, viruses, etc.)
- **unsuccessful management** (e.g. wrong decision making)
- **other accidents** (e.g. fire, badly designed, constructed and maintained buildings, human errors, etc.)

Secondly, on the organisational level companies encounter a great number of other threats, in addition to the mentioned first level threats, which arise in relation to (Finch, 2004, p. 188):

- **legislation** (e.g. breaching of intellectual property rights),
- **strategic decision making,**
- **lack of investment in maintaining competitive advantage and**
- **changing bargaining power.**

According to the author, the last level or the inter-organisational level includes all threats of the first two levels, as well as the threat of **weak and inefficient company control over the operations of its suppliers, customers and the entire logistics chain.** This threat occurs due to an increasingly intensive networking of companies. Companies no longer operate individually, nor are they isolated from other market operators, but are creating networks, concluding strategic alliances or agreements and establishing long-term partner relationships. By becoming dependent on operations of other firms in the network, companies are exposing themselves to a greater number of threats. The latter can be illustrated with the following example: a production unit of a company in the chain is destroyed in a fire, which brings their activities to a standstill and also leads to the interruption of operations in the entire logistics chain. Given the intertwined and dependent relations between companies, the

control over the operations of individual companies and the entire network is becoming much more complex and less transparent than otherwise (Finch, 2004, p. 190).

In addition to the threats identified by Finch (2004, pp. 185-190), threats to logistics chains in global operations include the threat of **economic crises, political disturbances** and the resulting **legislation changes, employee strikes** and **non-compliance with international maritime clauses.**

One of the essential consequences of economic and political disturbances within countries, which must be pointed out, is the phenomenon of terrorism. In recent years, terrorist actions have become increasingly organised, more frequent and more aggressive, and as such pose a great threat to logistics chains in global business operations. It is often the case that containers, a fundamental tool in today's global operations, are abused as a means for smuggling weapons.

The global logistics chains that are characterised by a high degree of such risks and exposed to numerous threats in their operations preclude the establishment of trust between companies within the chain, which results in operational inefficiency of the logistics chain.

3. ESTABLISHING LOGISTICS CHAIN SECURITY IN GLOBAL BUSINESS OPERATIONS

The answer to the question why it is significant to create an integrated security system, which is implemented throughout the entire logistics chain, can be found in the interconnection and interdependence between operations conducted by individual logistics chain links and other links. It therefore follows that the success of individual chain links is highly dependent on the success of the entire logistics chain. If a link in the logistics chain is affected by an accident, this does not only lead to a disrupted operation of that link, but also to standstills in the entire logistics chain. Such logistics chains can no longer operate efficiently, nor can they successfully meet end-customer demands, which results in revenue shortfall within the entire chain and market share loss. This is why establishing secure global operations must be in the interest of all logistics chain participants.

It is necessary to integrate the security measures of all operators involved in global logistics chain operations and those which influence the chain. Companies must be aware that, in addition to the security of processes within their own companies and the security in operations with direct business partners within the logistics chain, the security of all processes taking place in the entire logistics chain is of key importance. The operation of a plant at the beginning of the chain equally depends on efficient and uninterrupted operation of a

distribution company at the end of the chain, although they are not in direct contact. It is thus essential that companies are extremely careful in selecting their suppliers and business partners in foreign countries.

Collaboration between the private and public sector is also vital in ensuring logistics chain security, with the government having the role of coordinator and the industry that of consultant and supervisor. The common goal is to protect cargo throughout its journey from the point of origin to the final destination. While manufacturers naturally find continued and reliable supply most important and carriers focus on not losing or damaging their assets and customer goods, the most significant aspect for the government is the issue of national security. The international level requires the coordination and establishment of uniform security requirements and measures by different countries. Within stipulated security measures, multinational companies can also establish their own measures so as to ensure additional security and reliability of operations in global logistics chains. At first sight, additional security measures prolong delivery times and increase costs, but the benefits are in fact much greater than the costs. The implementation of certain security measures has resulted in more efficient and more productive logistics chains. Moreover, reducing the number of various disruptions in operations and related incidents has contributed to higher profits of all logistics chain links (Cargo and Supply Chain Security Trends 2005, 2005, p. 3).

3.1. Methods of reducing risk

Increased safety stock can help protect companies against supply and demand uncertainty. Safety stock enables quick responses to demand changes. Moreover, **increased capacities** facilitate greater flexibility and easier coordination of demand from various clients. By **supplying material from various suppliers**, companies create alternative sources and thus buffer themselves against potential supplier terminations or delays in delivery times (Braithwaite, 2003, p. 8).

Despite the benefits which the above-mentioned measures may bring at first sight, it is also necessary to devote attention to the negative consequences of implementing these measures. Namely, they cause additional costs in the form of tied financial resources in inventories, financial risk of inventory obsolescence and smaller quantity discounts on material supply. Furthermore, the described measures are appropriate for reducing the supply risk and not for reducing risk in other stages of operation.

It is precisely due to the mentioned weaknesses that **the importance of transparency and control** is coming to the forefront as an effective measure for reducing the entire operational risk, not only the supply risk. The transparency of all activities within the logistics chain is vital for operational transparency, which ensures that the right link in the chain is provided with the right

information in due time. In addition to transparency, the control over the implementation of all activities in the logistics chain is also highly significant. On the basis of received information, the control system enables a timely response both to individual logistics chain links and the logistics chain as a whole. However, it should be borne in mind that control within the chain is becoming increasingly demanding due to the extension of logistics chains. Consequently, managers of logistics chains have a limited view over activities within the chains. This decreases the capacity of responsiveness to unexpected events and renders the process of correct decision making more difficult. For instance, if storage facilities are not well informed about the characteristics and size of the arriving cargo, this results in a lack of cargo storage space or inappropriate storage facility premises (Veselko, 2003, p. 19).

3.2. Methods of increasing security

The essence of ensuring enhanced security lies in the shift from one philosophy of operation into another, namely the shift from focusing on the security of processes within the boundaries of own organisation to establishing mutual collaboration of all links in the global logistics chain so as to achieve integrated security of the entire logistics chain.

Such a shift in thinking was also necessary in gaining understanding of the modern concept of quality or integrated quality management. Thus, parallels can be found between the principle of achieving greater efficiency while ensuring greater security and the principle claiming that proper management can help achieve higher quality at lower cost. Just as quality management cannot be based merely on determining the quality of products at the end of the product line, so too logistics chain security cannot rely merely on randomised inspections. Security must be ensured at every stage of the logistics chain, in all processes and on all levels. The company operating at the beginning of the global logistics chain must therefore endeavour to establish a secure implementation of its own processes as well as increased security at the end of the logistics chain (Closs et al., 2004, p. 16).

3.2.1. Methods of increasing security in theory

One of the suggestions for increasing security is accelerated information exchange between business partners, ports, shipping companies and governments. This increases the transparency of and information available to the links in the entire chain. Enhanced control over the product flow in the logistics chain consequently helps achieve greater logistics chain security. On the other hand, this can result in increased costs, longer manufacturing and delivery times and more frequent disruptions in the material flow from the source to the consumer (Lee, 2004, p. 2).

Finch (2004, p. 190) highlights the following measures for ensuring heightened security:

- design of contingency plans,
- insurance policy renewal,
- design of preventive measures or procedures,
- data security,
- design of an appropriate strategy.

In collaboration with other participants in global operations, the government must establish specific rules and guidelines, which shall ensure the safety of people, country and commerce. The government measures are as follows (Knight, 2003, p. 6):

- ensuring the provision of security level information to ship owners and ports,
- establishing procedures to verify the validity of security certificates (International Ship Security Certificate),
- conducting security agreements with other countries, government institutions, ports and key trading partners,
- ensuring standards for enabling aviation security,
- organising training courses on adopted security standards,
- using a common methodology to verify whether companies and other subjects in global operations comply with requirements,
- requiring companies to draw up action plans.

Physical security, which includes the monitoring of the object's interior and exterior, can be attained with the following measures (Knight, 2003, p. 10):

- video surveillance,
- regular inspections of security measures implementation,
- appropriate locking and closing of external and internal doors, windows, fences, and installing of alarm devices,
- appropriate marking of dangerous cargo,
- ensuring separate and secured car parks for employees and visitors,
- prohibited parking of passenger vehicles in the vicinity of storage facilities,
- restricted access to document and cargo storage areas,
- highly restricted access to areas of key importance,
- use of metal detectors.

Port authorities are responsible for ensuring the security of ports, infrastructure, ships, people, cargo and its transport. The measures used to achieve the desired level of security are as follows (Knight, 2003, p. 8):

- drawing up security procedures and processes for areas under the control of port authorities,
- participating in assessing the security of ports,
- appropriate responding to security level information provided by the government,
- implementing inspections of required areas,
- using the Global Positioning System (GPS) to locate containers,
- establishing and maintaining communication with vessels,
- conducting training courses on processes for ensuring security,
- participating in the development of contingency plans.

Due to the interdependence of all logistics chain links in global operations, an increasingly intensive and efficient information exchange is necessary for their coordinated operation. It is of utmost importance that the information is not lost or destroyed and that it does not fall into the wrong hands. For this purpose, the following measures are introduced (Knight, 2003, p. 17):

- limited access to logistics chain information,
- safeguarding computer access,
- monitoring information system access,
- physical security of areas where the access to data is possible,
- creating and saving backup copies of data.

There exist numerous known measures for ensuring secure operations in global logistics chains. Although most of the above-mentioned measures are already in use in many countries and companies in global business operations, the measures differ according to the intensity of use.

3.2.2. Methods of increasing security in USA

The September 11, 2001 attack gave rise to an intensification of previous security measures and implementation of numerous new ones. Adopted security initiatives are aimed primarily at preventive actions and not only at final inspection.

In February 2003, the U.S. Customs Service issued an **Advanced Manifest Rule (AMR)**, which stipulates that cargo on U.S.-bound ships must be declared to the U.S. Customs Service at least 24 hours prior to departing from the departure port. This provides the customs service with sufficient time for an accurate check of all cargo manifests. The **Container Security Initiative (CSI)**

and the **Customs-Trade Partnership Against Terrorism (C-TPAT)** can be pointed out as another example. C-TPAT is a guide to increasing the efficiency of maritime logistics chains and mitigating the exposure of links to various natural disasters, theft, terrorism and other threats, while CSI focuses on the security of ship containers. Security screening of containers bound for the United States is thus implemented already at departure ports. CSI also stipulates that U.S. Customs officers are placed in all major world ports (Singapore, Rotterdam, Hamburg, Antwerpen, Hong Kong, Tokyo). The initiative comprises of four key components: information, x-ray, technology and smart containers (Lee, 2004, p. 4).

Moreover, the **International Ship and Port Facility Security Code (ISPS)** was also introduced. It includes regulations determining security standards for maritime ports and ships in maritime trade. The objective of the ISPS Code is to detect terrorist acts in a timely manner and successfully suppress them. The ISPS Code states that the security of ships and ports is a matter of crisis management, and involves a standardised manner of risk evaluation (Khalid, 2005, p. 3).

In addition to the initiatives described above, the following agreements contribute to enhanced security of logistics chains in global business operations: Business Anti-Smuggling Coalition (BASC), Business Executives for National Security (BENS), Council of Security and Strategic Technology Organizations (COSTO), International Port Security Program (IPSP), National Industrial Transportation League (NITL), National Petrochemicals and Refiners Association (NPRA), Smart and Secure Tradelane Initiative (SSTI), Smart and Secure Tradelanes (SST), Strategic Council on Security Technology (SCST) and Technology Asset Protection Association (TAPA) (Rice, 2003, p. 6).

The European Union (EU) is also actively involved in the field of ensuring greater global security. In order to ensure increased maritime security and prevent pollution, it has adopted important resolutions (Beškovnik, 2006a, p. 13):

- prohibited entrance of single-hull tankers into EU ports,
- more stringent control in EU ports,
- limited transportation of heavy oil in double-hull tankers,
- issue of criminal and financial sanctions for causing ecological damage through negligence.

On the basis of the above described agreements and adopted measures, it can be confirmed that the USA and its partner states have become very active in the field of ensuring increased security in mutual trade. Their goal was to ensure safe business environment for their companies and thus promote mutual trade and its positive impact on the state of economy. Furthermore, companies themselves have also exerted efforts to prevent damage occurrence in business operations.

The measures undertaken by firms such as Ford and Chrysler can be listed as an example. Ford has brought suppliers geographically closer, thus shortening the time of cargo being exposed to external impacts during transportation, whereas the Chrysler company focused on alternative transport routes and, in addition to using air freight to transport cargo from Virginia to Mexico, took advantage of road transport. Moreover, one of the possible methods is decentralised distribution, as a potential accident at one location does not destroy all distribution products (Rice, 2003, p. 14).

3.2.3. Most commonly used methods of ensuring security in practice

In July 2005, Eyefortransport conducted a survey entitled Cargo and Supply Chain Security and interviewed more than 140 subjects involved in logistics chains (manufacturers, logistics service providers, carriers, warehousemen, distributors, consultants, etc.). One of the questions was concerned with the measures their company uses in order to increase or ensure security. The answers were as follows: data protection system and cyber security is used by 58 percent of the respondents, smart containers by 19 percent of the respondents, personnel screening by 53 percent of the respondents, physical security is used by a considerable 72 percent of the respondents, area surveillance by 53 percent of the respondents, x-ray or other intruder detectors by 22 percent of the respondents, while 29 percent of the respondents said that they already avail themselves of radio-frequency identification (RFID) and other tracking devices. When asked about the security solutions planned for the future, the majority of the respondents (58 percent) replied that they are considering the use of RFID (Cargo and Supply Chain Security Trends 2005, 2005, p. 8).

The DHL company, a member of the Deutsche Post World Net group, already uses RFID in transport operations in food industry and in transporting clothes from China to Europe. The RFID technology is also used by the Wal-Mart and Metro groups. The latter marks pallets with smart labels, which enables easier screening of delivered products (Urbanija, 2006, p. 20).

The reasons for a growing interest of companies in introducing RFID and relevant information and communication technologies into their operation can be found in the global component of operation, due to which cargo tracking is becoming increasingly important as well as increasingly demanding. Companies can track the material flow in the logistics chain efficiently only by using an appropriately established information and communication system.

4. ACTIVITIES UNDERTAKEN BY SLOVENIAN COMPANIES IN MANAGING LOGISTICS CHAINS AND ENSURING GREATER SECURITY IN GLOBAL BUSINESS OPERATIONS

In comparison with companies from Western countries, Slovenian companies are significantly less aware of the importance of establishing an integrated security system within the entire logistics chain. Possible reasons can be found in a lower number of companies participating in global operations and in a smaller amount of resources available to companies for the investment in research and development and the modernisation of operating processes.

A study conducted by Veselko (2006, pp. 100-109) in 2006 proved that Slovenian companies indeed suffer from a lack of understanding of the logistics chain concept. The survey examined the development of the logistics chains of Slovenian companies in different economic environments. 60 larger companies were included in the sample: 20 production and services companies, 20 commercial companies and 20 companies which are involved in logistics activities. The tool for carrying out the survey was a questionnaire, which was divided into six sets of questions about the following fields:

- customer servicing management,
- order and demand management,
- production management,
- supply management,
- distribution and warehousing,
- general (logistics chain organisation, success measurement, e-SCM).

On the basis of the answers to questions provided in individual sets, the development level of a specific segment in a company was defined. The final overall assessment of the research showed that Slovenian companies have a low understanding of the logistics chain concept and are only partially familiar with the concepts of global logistics chains, which results in their inefficient operation. Given that Slovenian companies are not familiar with logistics chain concepts, not much is known about the importance of establishing security in logistics chains either. The negligent attitude towards the importance of ensuring efficient logistics chain management and secure logistics chain operation causes Slovenian companies, and hence also Slovenian economy, to lose ground in its competitiveness (Veselko, 2006, p. 106).

On the other hand, some companies' results were above the average, which indicates that certain Slovenian companies are aware that the field of logistics chain management is highly important and that they follow world trends (Veselko 2006, p. 106). One of the better Slovenian examples is the Lek company, which imports ninety percent of its production to Western, Central and East-

ern Europe, as well as to the USA. Fully informatised production enables Lek to trace the raw product from its supply to the production end. Moreover, Lek uses automated pallet preparation, which provides precise information about what an individual pallet contains. In the future, the company plans to introduce radio-frequency identification to improve product traceability and thus prevent counterfeiting of medicinal products. Additionally, this is one of the requirements put forth by American drug distributors so as to ensure enhanced reliability and security in global business operations (V.P., 2006, p. 24). Furthermore, the Slovenian company Viator & Vektor is also aware of the tremendous significance of ensuring security in global operations. For this purpose, it has introduced the VIA-VEK system, which enables vehicle tracking, into its operation. The system operates on the basis of the GPS receiver data and the maps stored on the memory medium of the device. This allows for identifying the exact location of the vehicle at any moment. In addition, the system's advantages are evident in easier route planning, route navigation, easer search of users, monitoring unforeseen traffic jams and lower communication costs. The system for tracking all vehicles in the international transport is likewise used by Intereuropa, a provider of logistics services. Amongst other, it helps the company obtain timely information about potential accidents and thefts of vehicles (Hafner, 2006, p. 26). Another example of a company pursuing increased security and efficiency of its operation is ATech elektronika d.o.o, owned by a Primorska region entrepreneur Davor Jakulin. If the company was not devoted to continuously improving the efficiency of the working environment and its security, it could not keep up with its extremely fast growth as successfully. As the company engages in high-technology processes, securing data and materials is vital. To this end, it has introduced the Time&Space solution, which operates on the basis of wireless RFID technology. The device was installed in eight passageways, thus ensuring continuous access control. By determining in advance who has the access to certain units and data and when this access is allowed as well as limiting the access of employees to certain units outside working hours, a high level of operational reliability and security has been provided (ATech - Od zajema podatkov do učinkovitosti delovnega okolja, 2006). Moreover, the Luka Koper port is also aware that the threat of terrorism is present always and everywhere, and has therefore placed radioactive radiation detectors in the port in collaboration with the USA. The device is intended to screen containers, vehicles and pedestrians on entry to and departure from the port so as to enable a timely discovery of suspected cargo, which could cause an accident in case of improper handling, and prevent illegal transport of radioactive material. Additionally, the deployment of radioactive radiation detectors was one of the requirements put forth by the USA, which wish to ensure a high level of security in its operation as well as in that of trading partner countries, particularly so after Sep-

tember 11 (Detektorji radioaktivnega sevanja v koprskem pristanišču predani v uporabo, 2006).

5. CONCLUSION

Logistics chains are becoming increasingly exposed to risks and threats in global business operations. As a consequence, logistics chain management is becoming increasingly complex, which calls for new knowledge and shifts in the thinking of all participants of global logistics chains. Together with their wide geographic scope and long duration, negative consequences of such threats can affect a great number of operators on the market, as they are interrelated and represent the continuous chain of goods, services, information and financial resources. The success of an individual logistics chain is thus highly dependent on the success of the entire logistics chain. First of all, it must be recognised that the human factor remains essential in ensuring enhanced security, since employees and their understanding of security are extremely important in the process of ensuring security in global operations. The reliability and caution of employees in implementing all activities in the company is undoubtedly the first requirement for achieving secure operation. A shift in the thinking of all logistics chain participants is needed in order for them to gain the understanding that securing the company's internal processes is no longer sufficient to achieve a desired level of operational security. It is necessary to establish an integrated security system, which will not only ensure greater security on all levels of the global logistics chain, but will also enable a smooth flow of goods, services and information. The next step in effective provision of security is the awareness of the entire logistics chain with potential risks and threats, on the basis of which appropriate security measures can be formed. The logistics chain links are introducing numerous measures for increasing security in their operations, from the design of contingency plans, use of video surveillance, security doors, anti-virus software, tracking devices, smart containers, employment of security services and employee training to participation in international organisations for security promotion. The level of implementing security measures differs according to individual links of logistics chains. The reason for that can be found in different amounts of funds available to companies or in different perceptions regarding the significance of security held by individual companies within the logistics chain. Naturally, companies with greater amounts of funds are able to invest more intensively in the technology providing enhanced security in the framework of their operations, whereas other firms cannot afford such investments. Moreover, companies which are aware of the negative consequences that high exposure to risks and threats can have on operational efficiency are more active in mitigat-

ing the level of risk and preventing accident occurrence. Greater security and efficiency of logistics chains in global business operations can also be contributed to by government institutions and organisations, which likewise represent an important link of logistics chains. Government institutions can ensure a high level of global security by forming appropriate economic policies, issuing guidelines and ensuring the application of international standards.

An integrated security system must therefore cover the security of the entire logistics chain in global operations, as the security of the first link in the chain also depends on the security of the last link in the chain. In addition to secure global operation, the established integrated security system must also ensure a smooth flow of goods, services and information to the end consumer. It is only thus that secure global operation will enable logistics chains to operate efficiently and successfully, exceed customer expectations and achieve required objectives.

BIBLIOGRAPHY

[1] *ATech - Od zajema podatkov do učinkovitosti delovnega okolja* [Internet]. Available from: <http://www.spica.si/caseStudies/caseStudies_ATech.aspx> [Accessed 15 September 2006].
[2] Beškovnik, B. (2006) Rast pretovora v pomorskem prometu tudi v prihodnjih letih. *Logistika & Transport (priloga Dela)*, 2 (7), pp. 8-11.
[3] Beškovnik, B. (2006a) Smernice pomorske prometne politike v EU. *Logistika & Transport (priloga Dela)*, 2 (7), pp. 12-14.
[4] Braithwaite, A. (2003) *The Supply Chain Risks of Global Sourcing*. Berkhamsted, LCP Consulting, pp. 1-11.
[5] Cargo and Supply Chain Security Trends 2005 (2005). *Eyefortransport's 4th North American Cargo Security Forum*. Washington, Eyefortransport, pp. 1-9.
[6] Closs D.J., McConnell H.J., McGarrell F.E. (2004) *Enhancing Security Throughout the Supply Chain.* Michigan, Michigan State Universty, IBM Center for Business of Government, pp. 1-52.
[7] *Detektorji radioaktivnega sevanja v koprskem pristanišču predani v uporabo* [Internet]. Available from: <http://www.luka-kp.si/novica.asp?IDpm=5&ID=886G> [Accessed 8 November 2006].
[8] Finch, P. (2004) Supply Chain Risk Management. *Supply Chain Management*, 9 (2), pp. 183-196.
[9] Hafner, A. (2006) Za kakovostno delo je nujen sistem sledenja. *Logistika in Transport (priloga Financ),* 46, pp. 26-27.
[10] Khalid, N. (2005) *Maritime Security Initiatives Post 9-11: Costs and Implications to the Port Sector* [Internet], June 22, Kuala Lumpur, Center for Economics Studies & Ocean Industries, Maritime Institute of Malaysia, pp. 1-11. Available from: <http://www.marecentre.nl/people_and_the_sea_3/papers/Stream%204/Panel%203/Khalid-MODIFIED-Amsterdam%20Paper%20(22%20June).pdf> [Accessed 22 June 2005].
[12] Knight, P. (2002) *Supply Chain Security Guidelines*. New York, International Busines Machines Corporation, pp. 1-22.

[13] Lee, H.L. (2004) *Supply Chain Security - Are You Ready?* [Internet], September 3, Stanford, Graduate School of Business and Stanford Global Supply Chain Management Forum, Stanford University, pp. 1-16. Available from: <http://www.stanford.edu/group/scforum/Welcome/White%20Papers/SC_Security.pdf> [Accessed 3 September 2004].
[14] Makovec Brenčič, M. (2005) Mednarodno poslovanje, Predavanja 7. Ljubljana, Ekonomska fakulteta on 29 November 2005.
[15] Rice, J.B. (2003) *Supply Chain Response to the Unexpected: Resilience and Security* [Internet], April 8, ISCM Research Project Update, WebExSession, pp. 1-30. Available from: <http://web.mit.edu/supplychain/www/sp-iscm/repository/rice_scresp_040803v8.pdf> [Accessed 8 April 2003].
[16] Scharpy, P.B. & Skjott-Larsen, T. (2001) *Managing the Global Supply Chain*, 2nd ed. Copenhagen, Business School Press.
[17] Urbanija, A. (2006) Z RFID do velikih prihrankov v logistiki. *Logistika & Transport (priloga Dela)*, 8, pp. 20-21.
[18] V.P. (2006) Informacijska podpora v proizvodnji in logistiki. *Logistika & Transport (priloga Dela)*, 7, pp. 24-25.
[19] Veselko, G. (2003) Kako do zaupanja v oskrbovalnih verigah. *Logistika & transport (priloga Gospodarskega vestnika)*, 9, pp. 19-22.
[20] Veselko, G. (2006) *Model upravljanja globalnih logističnih verig*. Doktorska dizertacija. Ljubljana, Fakulteta za pomorstvo in promet, Univerza v Ljubljani.
[21] Veselko, G. (2005) Povezanost globalizacije in tržnega dogajanja z managementom oskrbovalnih verig. *Organizacija*, 38 (7), pp. 354-360.

Sažetak

UPRAVLJANJE RIZICIMA I OPASNOSTIMA U LANCIMA GLOBALNE LOGISTIKE

U usporedbi s lancima lokalne logistike, lanci globalne logistike su u većoj mjeri izloženi rizicima i opasnostima. Razlozi zbog kojih dolazi do sve većeg izlaganja lanaca globalne logistike rizicima i opasnostima mogu se prvenstveno naći u njihovoj strukturi i u području njihovog djelovanja. Lanci globalne logistike šire se kroz mnogobrojne države i kontinente, uključujući pri tome i različite karike. Ti rezultati, u želji da koordiniraju između velikog broja karika, pokrivaju veće geografske udaljenosti i koriste bezbroj prijevoznih sredstava. Istina je, međutim, da lanac logistike, koji nije u stanju osigurati siguran i neprekidan protok robe, ne može učinkovito poslovati i postići tražene ciljeve. Stoga je prvi korak koji vodi ka uspješnom lancu globalne logistike spoznaja o postojanju veza između svih lanaca logistike s potencijalnim rizicima i opasnostima, a koji se pojavljuju u globalnom poslovanju, dok stjecanje čitavog niza znanja i vještina, pomoću kojih tvrtke mogu učinkovito i uspješno upravljati rizicima i opasnostima unutar samog lanca, predstavlja sljedeći korak. Dok mogućnost upravljanja rizicima i opasnostima unutar lanca logistike postaje sve zahtjevnije, uputno je detaljnije analizirati problem sigurnosti lanca logistike, te ispitati važnost njegovog osiguranja za učinkovit rad lanaca logistike u globalnom poslovanju. Najbitnije je prikazati metode kojima se karike lanca logistike mogu poslužiti kako bi smanjile rizike i osigurale veću sigurnost poslovanja, budući da siguran lanac logistike olakšava stvaranje obostranog povjerenja među poslovnim partnerima, promovirajući na taj način povećanu učinkovitost i uspješnost u poslovanju. Na kraju, upravljanje ovim područjem pokazalo se kao izvrstan početak za stjecanjem konkurentske prednosti, kako za individualne lance logistike tako i za njihovo poslovanje.

Ključne riječi: *lanci globalne logistike, upravljanje lancima logistike u globalnom poslovanju, rizici, opasnosti, upravljanje rizicima i opasnostima.*

Gregor Veselko, Ph. D.
Intereuropa d.d.,
Vojkovo nabrežje 32
6000 Koper
Tina Bratkovič
University of Primorska
Cankarjeva 5
6104 Koper
Slovenija