Security culture and transport network terminal activities

Daniel Ekwall *

Bertil Rolandsson**

*) School of Engineering, University of Borås, 501 90 Borås, Sweden
E-mail: daniel.ekwall@hb.se, +46 33 435 59 72

**) School of Education and Behavioural Sciences, College of Borås, 501 90, Borås, Sweden
E-mail: Bertil.Rolandsson@hb.se, +46 33 435 42 06

ABSTRACT

Purpose of this paper

All freights within a transport network are to some extent scheduled. This predictability plays an important role in all potential crimes against the network. Several different supply chain security programs advocate for increased security awareness regarding potential security breaches. What are the organisational consequences in terms of security culture for terminal workers?

Design/methodology/approach

A semi-structured interview guide was designed, in order to facilitate both a theoretical focus and flexible conversations. 15 interviews were done altogether at three different goods/freight terminals, and each interview took approximately 30-45 minutes. The nature of this study is explorative and therefore it focuses on the similarities rather than the differences within the interviews.

Findings

The management wants the terminal workers to perform their planed and scheduled operational tasks according to the written procedures. The security awareness idea advocates that, if needed, shall the employee perform security tasks instead of the planed operations. This means that the employees may be forced to choose between fulfilling their normal tasks or performing security duties. This duality in management signals restrains the development of security awareness.

Research limitations/implications (if applicable)

The research are limited by the difficultness in establish clear and evident causal relationships between all the different factors that together compose the corporate security culture.

Practical implications (if applicable)

This paper shows that all management initiative affects the security culture in the transport network. In order to create the right security culture is it vital that all management initiative is understood from a user perspective and with a holistic approach.

What is original/value of paper

Using theories from social sciences in logistics in order to fill the gap between the ideas from supply chain security programs and the real situation in the transport network.

Keywords: Security culture, Criminal activity, Transport network, Supply chain security programmes, Security awareness

1. INTRODUCTION

The increasing trend toward globalisation has led to an increase in logistic activity. The process of shipping goods around the world is long and complex (Scharyand and Skjott-Larsen, 2001), and yet the international trading system is dependent on the effective transport of these goods. Also, these transports have become more and more vulnerable. Christopher and Lee (2004) suggest that the increased vulnerability in supply chains is a result of the drive towards more efficiency, which in turn increases vulnerability from disruptions or disturbances. According to Svensson (2000), "Vulnerability is defined as the existence of random disturbance that lead to deviations in the supply chain of components and material from normal." The outcome of such a disturbance should also have a negative effect on the companies involved (Svensson, 2000). This definition contains two difficulties; namely, the ideas of "random disturbance" and "deviation from normal." Random disturbance indicates that the focal company does not control the change, while a deviation from normal suggests that there is such a thing as a normal or scheduled situation. The occurrence of a normal state is more probable in the transport network than in the flow of material. Thus the interactive sub-system of products and processes, using Juttner's (et al., 2003) definition, is more flexible and thereby also possesses a larger tolerance towards deviation than the resources (facilities and cargo carriers) can manage. The transport network is therefore more vulnerable than the product flow, but the transport disturbance also affects the product flow.

This vulnerability can in many cases be described as "unwanted effects" in the supply chain caused either by internal or external forces that create disturbances larger than the supply chain is designed to handle (Ekwall, 2009 - a). The disturbance can be unintentional or deliberate, legal or illegal. Today there is a significant problem with the theft of cargo worldwide. The theft of cargo value for the EU-area is estimated to be €8.2 billion each year. When allocated on all transports, this gives an average value of €6.72 per trip (EP, 2007). There are suggestions that the real figures for cargo theft in official reports are either grossly underestimated or overestimated (Gips, 2006). Gathering accurate numbers for cargo theft losses is difficult and in many cases impossible, due to limited reporting by the transportation

industry and the lack of a national law enforcement system requiring reporting and tracking uniformity (ECMT, 2001 - a).

In the CEN report (2006) *Draft final report,* different security measures are categorised into three different approaches: systematic, technological, and psychological. The systematic approach strives to establish action against threats and resilience as a response to incidents. The systematic approach also addresses different organisational aspects in supply chain security. The technological approach relates to the need for technological innovations to achieve a state-of-the-art technological advantage. The psychological approach aims to establish awareness among all personnel working within the transport network. The psychological approach can also be described as awareness or alertness within the transport chain. High awareness or alertness depends on the interaction and involvement of personnel in policy and business processes. Good awareness about problems with cargo theft must therefore be a part of the unwritten regulation of behaviour or a part of the company's culture with regards to cargo theft problems. Several supply chain security programs such as C-TPAT (Customs-Trade Partnership Against Terrorism), CSI (Container Security Initiative), and AEO (Authorised Economic Operator) also emphasize the need for employee awareness in order to increase the overall security level. Awareness together with the actual way things are done can be called the security culture (c.f. Fredericks, 1995).

1.1. Research question

The purpose of this paper is to analyse the security culture among terminal workers in a transport network. This is done against a background of increasing numbers of international supply chain security programmes that all more or less advocate security awareness among the employees as a cornerstone in security.

2. FRAME OF REFERENCE

2.1. The supply chain concept and transport networks

Christopher (2005) defines the supply chain as: *The network of organisations that are involved through upstream and downstream relationships in the different processes and activities that produce value in the form of products and services in the hands of the ultimate customer".* The goal for all involved organisations is to provide the ultimate customer with the right product and the right time and place. The physical flow of products through the supply chain is conducted by a transport network. Transport networks are designed to use economy of scale when moving products from consignor to consignee through nodes and links in a supply chain. Transport nodes are terminals, warehouses, harbours and airports, while transport links are means of connecting the nodes. Goods enter and exit the network through inbound and outbound gateways (Lumsden, 2006). The transport network affects cost and throughput time, and if used smartly it can even increase the value of the product (Lambert and Stock, 1993).

All freights within a transport network are to some extent scheduled based on various reasons. One of the most common is the consignee terminal's need for product delivery within a certain window of time. This makes the network predictable for all actors involved, including the potential perpetrator. This predictability plays an important role in all potential crimes within the network. The rigid scheduling in the transport network provides an excellent breeding ground for recurring crime opportunities (Ekwall, 2010). Even when recurring, the transport network will view a crime opportunity that is taken as an extraordinary event,

something that is not a part of the usual pace in daily work. The terminal employees therefore need to be aware of such extraordinary events in order to minimize its consequences.

2.2. System of supply chains

Descriptions of supply chains are in general achieved with a system approach in logistics research. The description of the context and the boundaries of the supply chain are essential to understand the description of each supply chain. This is achieved as each supply chain is separated into several different sub-systems that together provide a wider understanding of the context and present different necessary boundaries. According to Arnäs (2007), is it useful to separate logistics and transports from each other and instead emphasize the dialectic relationship between the terms or systems.

The logistics system is constituted of three structured elements/components: Products, Locations and Facilities. The transport system is constituted of three different structured elements/components: Vehicles/Vessels, Freight and Ways & Terminals. The dialectic relationship between logistics and transport is illustrated in figure 2.2.

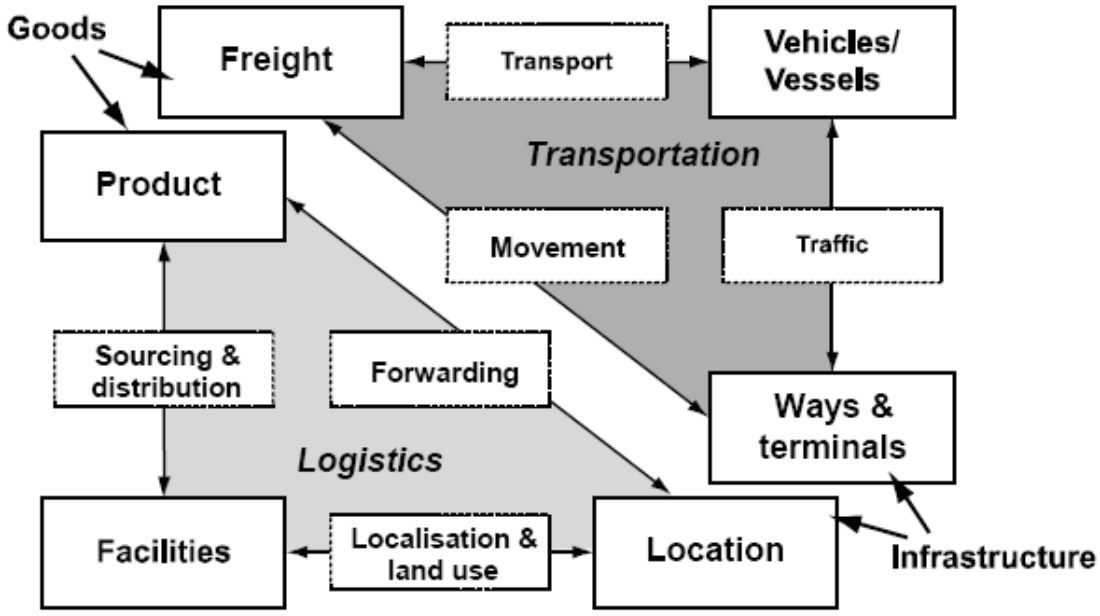

Figure 2.2: The dialectic relationship between logistics and transportation (Arnäs, 2007).

The joint positions (dialectic relationship) in figure 2.2 are the six different diagonal elements. Goods are represented by the terms Product and Freight, but from different perspectives. The infrastructure is also represented from two different perspectives as Location and Ways & Terminals. The relocation of goods using an infrastructure is represented by the processes of Forwarding and Movement (Arnäs, 2007). The dialectic relationship between logistics and transport provides an excellent description of the supply chain content products and infrastructure, but lacks the organizational element and also the wider environment that everything is acting within. By adding two additional systems to the logistics and transport is it possible to better elucidate the context and boundaries for a supply chain system.

According to Juttner (et al., 2003), a supply chain is an interactive system with four different levels. The first two levels correspond to the dialectic relationship between logistics and transport, while the other two levels represent the organizational structure and the wider environment. Each level includes various elements and content descriptions. These elements

and descriptions are of a general nature and therefore not decisive; rather, they are more illustrative and explanatory. The main advantage of using four levels (or subsystems) to describe the supply chain system is that they automatically provide a contextual understanding and boundaries to the problem of antagonistic threats towards the logistics business. Further, to each level is attached a description of the major risk sources and the different risk management strategies normally used to handle (and hopefully minimize) the risk consequences attached to each level. A business generally considers the risk sources in the various levels differently. For example, a risk in level 2 is normally considered negative, while the same risk source may, in the perspective presented in level 3, represent a new business opportunity, which is normally considered good. Table 2.2 presents the system of supply chain risks.

Table 2.2: System of supply chain with risk description and risk management strategies (based on Juttner et al., 2003 and Peck, 2008).

Level	**Elements**	**Content Description**	**Risks**	**Risk Management Strategies**
1	Products and processes	Inventory and Information flows	*Considered Bad:* variance, inefficiency, lack of responsiveness, demand uncertainty	Substitution of information for inventory; better visibility, velocity and control
2	Assets and infrastructure dependencies	Fixed and mobile assets	*Considered Bad:* loss of link or nodes factors	Insurance and contingency/business continuity planning
3	Organisations and inter-organisational networks	Contractual and trading relationships, financial wellbeing	*Considered Good and Bad*: financial decisions/organisational failure	Contractually governed: partnering; dual sourcing; outsourcing
4	The wider environment	Economy, society and the forces of nature	*Considered Good and Bad:* geological, metrological and pathological forces of nature	

Most current logistics security programs have addressed different parts of level 2 while focusing on infrastructure risks, thereby achieving better security in the supply chain system. Programs such as AEO have glided a little closer to level 3 than other programs because it does criminal background checks (for customs crimes) on senior management of the certified company. This shall be compared with the corporate culture found in level 3 as it is a palpable part of all organisations.

Table 2.2 follows the logistics research tradition of not including people in the model or system. This may be a good approach in most logistics research but when the research question and purpose focus on the security culture; the research should be centred on human involvement. However, the supply chain system does not include cultural values such as security and team spirit. The reality in which the terminal worker acts is more complex and full of nuances in a way that logistics theories normally avoid. Terminal activities, security culture and team spirit can be described as functions that operate through group interaction and iteration, which is one of the criteria for wicked problems (Rittel et al., 1973). Therefore, the inclusion of people and cultural values into logistics research aims to strengthen the knowledge base in logistics (Stock, 1997). An interdisciplinary exchange of views, ideas and theories is needed to develop logistics into an applied science (Klaus et al., 1993).

2.3. Security, risk management and crime prevention

Security, risk management and crime prevention are often considered similar and always work together (Manunta, 1999). This suggests that security and risk management are good, at least from an ethical point of view, because they reduce crime; thus more or better security or risk management should reduce problems caused by crime. The problem is that a crime is defined by law, according to the principle "no crime without a law", while security or risk management has no philosophical attachment to the law. This means that people on both sides of the law can have better or worse security or risk management and that security and risk management are not necessarily for the prevention of crime. Unrestricted security for an individual or a group of individuals can jeopardise security for others by threatening them or transferring threats to them. This type of discussion can be heard from philosophers like Hobbes and Mills. Unbounded or unrestricted individual security could even threaten the authority of a state. Thus, a security problem may or may not be a legal problem. Security, as an idea, can be explained as having two parts: a protector or guardian and the threat it tries to protect the asset or object from. This threat can be from either side of the law. To obtain the right security it is vital to answer who is protecting what, from whom, in which situation, to what extent and to what consequence (Manunta, 1999).

Successful risk management needs to operate in a fairly predictable world or at least to be dependent on a large amount of trustworthy statistics. Because previous events or incidents are the basis of risk management, it cannot effectively deal with a self-inflicted alteration of the threat pattern. This means that, in crime prevention, risk management is effective if the potential perpetrators are limited to the use of unsophisticated and indifferent methods that are based on opportunistic behaviour (Manunta, 2002). However, as potential perpetrators become more and more sophisticated and develop larger capability, the statistical predictability of risk will reduce dramatically. The antagonistic perpetrators study the victim to discover routines and regularities and with this knowledge they improve their skills (planning, technologies and tactics) to maximize their likelihood for success (Clutterbuck, 1987). The prevention of antagonistic threats by following current business trends makes the system even more predictable. Military special forces and similar organizations have proven this time after time (Manunta, 2002). Therefore is the human involvement in security function of most importance. If each employee in all organisations would have the awareness both about security problems and how these shall be solved, it would reduce the general risk attached to security issues.

2.4. Transport and freight security

According to Borodzicz (2005) security can be considered as interpreted as either *freedom from danger* or a *show of force (or strength)*. Both interpretations are valid for this paper but

in normal life is the last meaning of the word security more common. The need or demand for security during transportation is to prevent unwanted negative disruption in the flow of goods. The general term for this prevention is transport security (EC, 2003), defined as the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems and workers against intentional unlawful acts (EU, 2003). Technological development in the range and sophistication of anti-theft devices and after-theft systems is increasing rapidly. Special attention has been given to systems that track the goods themselves throughout transport (ECMT 2001 - b); but applying different technological systems is only a part of transport security strategy (Tyska and Fennelly, 1983). The key issue is the successful coordination and cooperation of the actors involved in the transportation. At present this cooperation is not widely developed (ECMT 2001 - b). Present supply chain security research outlines several changes for how security in a supply chain should be approached. First, supply chain security should incorporate not only theft prevention but also anti-terrorism measures. Second, the focus is now on global issues and not just local or national issues (Sweet, 2006). Third, when conducting contingency planning, the concept of crisis management is to be included to obtain better resilience. Last, security is no longer an internal corporate question but rather an issue for all actors within the supply chain (Closs and McGarrell, 2004).

2.5. Company security culture

According to Frederick (1995), the corporation is a complex and diverse conceptual construction. The legal entity (the corporation) has rights, privileges and liabilities distinct from those of its members. The corporation is first an economical construction designed to deliver profit for its shareholders. In order to achieve this, the corporation needs employees, equipment and capital, and the corporation should act within the local legislation. This complex construction contains both economical and sociological constraints which depend, to different degrees, on all stakeholders. Frederick (1995) argues that the anthropological conception of culture "as that complex whole" provides a potential synthesis. Frederick (1995) states: *Culture can indeed clarify the practices and policies of modern corporations, as well as the sometimes bizarre and distressing behaviour of those who work in corporations…capturing culture's meaning may unlock many doors within the corporate citadel*. According to Brinkman (1999), an understanding of the conception of corporate culture requires "*a clarification of how the anthropologist's conception of culture relates to the economic process overall*". This requires three elements that relate to the conception of corporate culture:

(1) The economic processes;

(2) The evolution of the economic and cultural form and structure; and

(3) The process of structural transformation.

The real world description of products forwarded to every corner of the world through global networks clearly demonstrates that both social and cultural issues need to be within analytic boundaries instead of outside them (Reason, 1997). Consequently is it a good idea to describe the transport business as a comprehensive infrastructure requiring flexible and self-governing employees (Castells, 1996; 1998). Organisational complexity seems to be the rule. In several discussions about global and complex organisations such as transports, self-conducted staffs appear to be increasingly important for the coordination of security (Mythen and Walklate, 2006; Kemshall, 2006). In accordance with discussions about the organisation of work and security, self-governing individuals could offer a way of coping with a broad spectrum of potential risks such as theft (Rose, 1999; Stokes, 2007). Managers, then, are tackling organisational insecurity caused by difficulties in controlling the organisational complexity by

delegating responsibility from the top to the individual employee and assessing the outcome (Rose, 2000; Roberts, 2006). One possible outcome of this is that the management focus on reducing the variability in human behaviour at the sharp end of system operation rather than the inadequate conditions present in the system itself (Reason, 2000). This may depend on the infrequency in security incidents and that the direct consequence of an incident normally is a temporary change in the local human behaviour than evolution in the company security culture (cf. Burke, 2005).

3. METHOD

The research was conducted as an interview study. Data was collected through 15 qualitative interviews at three different terminals (five interviews at each terminal). The use of qualitative interviews was motivated by the fact that the issue of the study is sensitive. Employees can be inclined to answer ordinary survey questions about thefts at their work in a politically correct way, which makes such data less reliable (Seidman, 1998). The problem of correctness does not vanish by using interviews, but it gives the opportunity to explain questions and to ask respondents to explain their answers. In addition, interviews always began with general and less sensitive questions about the employee's background and about the job. This helped the conversation to become more relaxed and allowed a sense of trust to be established between the interviewer and the respondent. This made it easier to go behind more formal descriptions of highlighted security problems (Kvale, 1997).

A semi-structured interview guide was designed to facilitate both a theoretical focus and flexible conversations. The guide was based on three main themes: the employee's group identification at work, the organisational structure and aspects of the surrounding world such as temporary employees and unidentified visitors. The interviews began with less sensitive background questions, including employee age, years at work, and tasks typically performed. This helped to defuse the real issue. Fifteen interviews lasting approximately 30-45 minutes each were conducted at three different goods/freight terminals. It appeared that the theme of our study did not allow the conversation to be pushed longer. Furthermore, we interviewed employees at work; in many cases they had jobs waiting for them.

After the interviews had been transcribed, the transcriptions and what the employees had said during our conversations were analysed. Initially, theoretically anchored themes connecting different statements were used. These themes included "the surrounding world", "group identity", and "hierarchy", and allowed us to also analyse different external and internal relations that the employees talked about. Codes indicating both whom and how employees connected thefts or other security issues with these themes were then used. The codes indicated both relations and contents (e.g. "insiders" or "prioritized/not prioritized question"). This made it easier to understand the meanings attributed to this issue and the similarities and differences that existed in the interpretative patterns at each terminal (Kelle, 1995). The latter also demanded a final and thorough confrontation with our theoretical point of departure: the underlying systematic and coherent conclusions about the security frames that were expressed at each terminal (Miles and Huberman, 1994). The research procedure used in this paper can therefore be categorized as abductive (Kovacs, and Spens, 2005). The lack of previous research in this area makes the nature of this study explorative and therefore it focuses on the similarities rather than the differences within the interviews. High reliability in the research presented in this paper is achieved by using obvious and clear questions. During an interview is it important to give the interviewee all the time he/she needs and to conduct the interview in an environment where the interviewee feels safe.

4. EMPIRICAL FINDINGS

4.1. Terminal description

The three different terminals involved in this research were all chosen by the researchers. The selection was made in accordance with the following criteria: The terminal should be owned by a major LSP company, situated close to the theft-endangered areas in Sweden according to official criminal statistics (Nilsson and Rosberg, 2009) and willing to participate in this research. The chosen terminals belong to two different companies (A and BC). The terminals are located in three different cities; terminals B and C belonging to company BC were in mid-size cities while terminal A was located in a bigger city. The choice of interviewees was made at each terminal by the local site security officer (SSO). The guideline provided to each SSO was to choose blue-collar workers with a representative mixture of age, gender and length of employment at the company. During the interview, all normative discussion was held to a minimum. This was done to get the interviewees to state their true opinion and experience. For the same reason, all interviewees were guaranteed anonymity so they did not fear reprimands from their employers.

4.2. Crime risk around the terminals: official statistics

No complete and fully trustworthy statement about the problem of theft of goods in relationship with the European transport network exists. Still, it is reported that in some European countries up to one percent of cargo vehicles are stolen each year (ECMT, 2002). This is an indicator of the seriousness of criminal activities within the logistics business. Cargo theft, vehicle theft, theft of goods from vehicles and theft of entire vehicles loaded with goods have increased. In Sweden does the attacks occurred mainly along the major roads and during night time. The most palpable findings in the official Swedish criminal statistics for freight related crimes is the 81 percent of all reported crimes attacked unprotected lorries or trailers (Nilsson and Rosberg, 2009). There was a little reduction in number of stolen Lorries during 198 (2008) from 216 (2007) but the number of non-recovered Lorries was double to 26 (2008). The development for the theft of trailers is increasing from 105 (2007) to 135 (2008) where the number of non-recovered trailers increased by 25 percent to 25 (2008) (Nilsson and Rosberg, 2009). The change in what types of goods are desirable depends more on the general change in customer demand. This means that the causality, from a crime displacement perspective, with regards to the stolen goods is very difficult to establish (Ekwall, 2009 – b).

4.3. Crime risk around the terminals: company risk ranking

Neither of the two companies were willing to share their own statistics regarding thefts in the three terminals with the researchers because of business reasons, but they were willing to rank the terminals according to their perceived theft threat level (both companies have terminals in the same three cities) and cooperate without sharing statistics but by exchanging intelligence and information regarding threat levels). Both companies' CSOs independently ranked the theft threat level for the terminals; the results were identical.

Official criminal statistics with both companies as injured parties give a different image of the risks to the terminals. Company BC is, according to the official statistics, more exposed for criminal attacks than company A. According to both CSOs, this difference can be explained because company BC has a policy to always report all suspected crimes while company A does not. Also, the official statistics with the companies as injured parties contain all types of crime against the company, not just theft; therefore these statistics give only a hint about the companies' problems with criminality. The risk was considered highest for terminal A, followed by B and finally C. Table 4.3 shows the crime risk ranking for the terminals.

Table 4.3: Risk ranking for involved terminals (1 is highest and 3 is lowest)

	Terminal A	***Terminal B***	***Terminal C***
CSO company A risk ranking	1	2	3
CSO company BC risk ranking	1	2	3
Researcher risk ranking according to interview comments	1	2	3
Reported crimes with the company as injured party 2006-2007	4 (company A) 130 (company BC)	26 (company A) 78 (company BC)	12 (company A) 57 (company BC)
Overall risk ranking	**1**	**2**	**3**

4.4. Security organisation in each company

The security organisation in both companies is set up in similar ways. In both companies they are considered secondary to the operational structure and instructions. In all three terminals there is an appointed Site Security Officer (SSO) with operational responsibility regarding security in the terminal area. The SSOs report to both the terminal manager and the security organisation. There is a difference in security organisation between the countries' Chief Security Officer (CSO) and the SSOs; there company A has an appointed regional security officer (responsible for a smaller number of terminals) with a preliminary coordinating function. Mutual in both cases is that the cost for security is part of the terminal manager's budget and that the CSO holds centralized staffs function under the Managing Director. Company A has had a security organisation a few years more than company BC. This has led to a practical difference where company A has more and better implemented security guidelines and is more experienced when it comes to security issues. With this said, the security organisations in both companies are seen more as a necessary evil than as something that contributes to the bottom line (profit). In reality the security issues at each terminal are closely related to the SSO at each terminal while the central organisation only appears to do a security inspection or help the SSO to investigate difficult thefts.

4.5. Interviews

The interview guide used in all interviews was structured according to each individual's experience of the work environment with regards to the security situation. This led to the use of three main themes in the interview guide: identification at work, the organisational structure and aspects of the surrounding world. The presentation of the interviews will follow this structure. All interviews were conducted in the native language of both the researchers and the interviewees, namely Swedish, and all quotes have been translated by the researchers.

4.6. Identification at work

In all interviews the work assignment was described as monotonous and repetitious tasks that were planned as parts of the general terminal process. For each individual this leads to insignificant possibilities to affect his or her own work assignment. Still, the general terminal function and need for personnel also entails positive effects for the employees. As one of the interviewees stated, "The assignments are mostly monotonous but with good working hours". One drawback with monotonous and repetitious tasks was that staff turnover was described as either acceptable or high. In one terminal they described an extended use of seasonal workers

in the form of students who worked for a shorter period. It was desirable for the number of personnel working at the same time at any of the terminals to be as low as possible, which led to an extended use of personnel from staffing companies. All interviewees mentioned that the staff turnover entailed that they worked with relatively new people all the time. In some interviews this was considered as positive while in others this was seen as a negative effect. All interviewees identified themselves as blue–collar workers who were separate from the white collar staff.

4.7. Organisational structure

Both companies have adopted very similar hierarchical organisations that in both cases emphasise that there is a certain way to perform a certain task and this method should be followed at all times. All responsibility within the companies and terminals comes from the top manager and is from there distributed throughout the hierarchy. The trust in top management to handle the companies or terminals is high. As one interviewee stated: "*If there is a problem, I inform my boss and he solves the problem for me*". The interviews clearly proved that the entire general attitude towards uncertainty (regardless of type) is that it shall be reduced as far as possible. The basis of this idea is that equilibrium and stability exist in all logistics (Lambert 1998). In other words, everything can be controlled. The idea that everything can be controlled was the red thread throughout all interviews. Therefore it is possible to state that operational control is a vital part of the corporate culture.

Almost all interviewees provided one or more different narrative descriptions of self- or co-worker-experienced security incidents, mostly cargo thefts. As one interview described it, "*I have captured a few guys red-handed with a computer theft. Other times investigations have led to thieves being captured who were colleagues, drivers or staffing personnel*". The uncertainty related to security incidents seems to threaten the cultural belief in operational control and organisational stability that was considered normal. The existence of thieves and other threats to operational control and organisational stability is a continuous generator of uncertainty and disbelief in management control functions, which generates waves of security cultural consequences over an extended period. Such a period can stretch to several years as some of the interviewees recalled security incidents years ago and repeated the experience to new colleagues. The different organisational structures of the two companies could be identified in the interviews, where company A had tried to handle security-related uncertainty by creating a security organisation that was a little more locally based and the SSOs had a better understanding for what was expected of them and what they were allowed to do.

4.8. Aspects of the surrounding world

The threats or security risks that emerge from the world closely surrounding the terminal, which includes all insider-related issues, contributes to the feelings of security-related uncertainty presented in all interviews. As one interview described it, "*The biggest threats come from the outside but that depends on the tip-offs from the inside the terminal/organisation*." Another said, "*The thieves knew when and where the truckload of computers was here and how to steal it. They must have had information from inside to pull that one off.*" It was clear during the interviews that the mythical insider is, in actuality, far from a myth. Several of the interviewees knew of colleagues who been investigated and later sentenced for theft and thereby also discharged and blacklisted from the company. The presence of both eye-witness experience and mythical descriptions of insiders as one of the main security threats was in line with expectations based on previous studies and theoretical descriptions (Barth and White, 1998; Tryon and Kleiner, 1997; Muir, 1996; Beck, 2002;

Speed, 2003). In all three terminals the discussion and description of insiders was similar; possibly the workers in terminal A had more eye-witness experience than the workers in the other two, but that might be because the interviewees in terminal A in general had been on the job longer. The effects on security culture from the insider problem can contribute to increasing distrust between personnel within the transport network. This is a negative impact, especially since general operational instructions are based on the idea that personnel trusts or at least checks that the previous operations were executed correctly.

The general descriptions of thieves contained everything from "pilfering" to "professional thieves", with an emphasis on the latter. As one interview described it, "*These guys that come here, they are professional, they are tremendously skilled and they are accordingly professional thieves. Thus they know when and how before they conduct the action*." All interviews ended with how the interviewee ranked the security aspect of the company in relationship to other issues in their working environment. In almost all interviews other issues such as safety and general working conditions (temperature, ergonomics issues and working hours, etc.) ranked as more important than security. Those interviewees that had experienced security incidents were the most reluctant to write off the need for security.

Suggested security solutions from the interviewees were in most cases physical obstacles such as gates and fences together with surveillance cameras (CCTV). A few suggested better use of security procedures. The interviewees all believed that the hierarchical organisation will handle future security-related incidents and prevention so that they (the interviewees) can continue performing their work assignments as usual.

5. DISCUSSION

In this study, all workers expressed a common belief in the higher hierarchy's or organisation's ability to design and implement procedures for all problems that may or may not occur at work. They described a legitimate hierarchy and a wish to keep the organisation and working groups honest and stable (Douglas and Wildavsky, 1983; Engdahl, 2003). Rather than referring to themselves as autonomous individuals conducting complex jobs in an ever-changing transport network, they framed themselves as decent blue-collar workers at the bottom of the organisation. They complained about repetitive tasks, bad working conditions and poor communication with the top management, which delimited their own initiatives. However, it was also important that management followed established routines and procedures in the organisation (Mars, 1997). The interviewees all expressed the belief that terminal processes are designed, maintained and performed in accordance with the idea that equilibrium and stability exists in all logistics. There is no surprise that the presence of criminal actions in the logistics threatens the idea of stability and thereby also the strong belief that the hierarchal organisation will solve the problem. If the problem with security incidents increases (both occurrence and impact), the stress on the hierarchical organisation's problem solving ability becomes greater. If the organisation does not prove its ability to handle security incidents, the terminal workers' trust that the organisation can handle other issues may also be threatened and consequently the corporate culture will be altered. The duality of security efforts can also lead to that individual employees express a distrust in the management when they introduce security equipment (Howie, 2007). In this research we found small support to this belief.

Despite this contribution to the corporate culture, no respondent wanted a security organisation in which flexible individuals replaced hierarchical top-down control (Rose, 1999; Stern, 2006). Even though the big city terminal appeared to be exposed to less controllable

circumstances, the workers claimed that it was mainly the management that had responsibility for cutting the risk of thefts at work. Most of them wanted to see more initiatives from the managers rather than from themselves, which underlines the importance they ascribe to a stable hierarchy. However, terminal A respondents described a need to intervene themselves. Based on our empirical material it cannot be determined whether they have been included in any decision-making dialogue. It can be said, however, that organised crime and the terminal's location in the city centre meant that the workers felt that they had to take individual initiatives on the shop floor (Mars, 1984). Given that they knew about the security policy and wanted more education about it, it may be said that they combined a wish for more initiatives from the management with features of self-governed workers who conduct themselves in accordance with knowledge, policies and rules of the company. However, the main reason why this shop floor initiative was needed appear to have been unpredictable external conditions rather than management steering the workers from a distance (Rose, 2000; Mythen and Walklate, 2006). In line with Frederick's (1995) argument that culture is a complex whole, this clearly demonstrates that if the corporate culture strongly emphasizes the hierarchic top-down control that conception will affect all processes and operations regardless of the demanded approach for special issues. This may lead to problems when security awareness depends on the interaction and involvement of personnel in policy and business processes but in normal logistics activities the involvement of personnel is held to a minimum. This shall be compared with that codes and policies (security or not) are not adequate guides, especially at the operational level, where the right behaviour is needed (Berglas, 1997; Boyer and Webb, 1992, von der Embse et al., 2004).

Knowing the risk ranking for all three terminals makes it easy to draw the conclusion that a riskier surrounding affects security culture among terminal workers, but how this influence affects security efforts depends on several different factors. The right response and attitude from management may hinder a fatal disbelief in the organisation's ability to prevent criminality. The response and attitude from top management all the way down to the terminal workers needs to result in the understanding of multiple alternative perspectives (top management's, customers, terminals workers, etc.) and focus on relationships between alternative solutions instead of ad-hoc and stand-alone security features.

6. CONCLUSION

The international trading system is dependent on the effective transport of goods. These transports have become more and more vulnerable. Several supply-chain security programs such as C-TPAT, CSI, and AEO emphasize the need for employee awareness in order to increase the overall security level. Good awareness about problems with cargo theft must therefore be a part of the unwritten regulation of behaviour, or in other words, the company's culture with regards to cargo theft problems. This awareness together with the actual way things are done can be called the security culture.

Risks can emerge from within both the organisation and the local environment. These risks can be described as uncertainties that need to be reduced as much as possible. This approach may be good for handling process failures but is less successful in reducing the problems with criminality within the logistics business. Management can, by interaction and involvement of personnel in policies and business process design, develop a more suitable security culture. This approach becomes more important if potential perpetrators become more and more sophisticated. Normally, the different processes in terminals are designed to be simple and repeating, according to ideas from Lean production and similar logistics theories. The presence of security threats whose occurrence is unpredictable may force employees to

choose between fulfilling their normal tasks or conducting security-related tasks, which also entails them to execute their normal tasks later and faster to reach the same level of productivity. This duality in management signals restrains the development of security awareness. The security culture depends on the organisational complexity in each terminal/company. To coordinate security in global and complex organisations, self-conducted staffs are increasingly important.

REFERENCES

Arnäs, P.O. (2007), *Heterogeneous Goods in Transportation Systems - A study on the uses of an object-oriented approach*. Division of Logistics and Transportation, Chalmers University of Technology: Göteborg.

Barth, S. and White, M. D. (1998), "Hazardous cargo". World Trade, November 1998, pp. 29.

Beck, A. (2002), "Automatic product identification & shrinkage: Scoping the potential". ECR, Brussels.

Berglas, S. (1997), "Liar, liar, pants on fire", *Citation, Inc*., Vol. 19, No. 11, p. 33.

Brinkman, R.L. (1999), "The dynamics of corporate culture: conception and theory". *International Journal of Social Economics*, Vol. 26 No. 5, pp. 674-694.

Borodzicz, E. P. (2005), *Risk, crisis & security management*. Wiley, Chichester

Boyer, E.P. and Webb, T.G. (1992), "Ethics and diversity: a correlation enhanced through corporate communications", *IEEE Transactions on Professional Communication*, Vol. 35, pp. 38-43.

Burke, R. J. (2005)," International terrorism and threats to security Implications for organizations and management". *Disaster Prevention and Management*, Vol. 14, No. 5, pp. 639-643

Castells, M. (1996) *The Rise of the Network Society – The Information Age; Economy, Society, Culture vol. 1,*

Castells, M. (1998) *End of Millennium – The Information Age; Economy, Society, Culture vol. 1,* Malden, MA:

CEN (2006), *Draft final report (2nd draft).* CEN/BT/WG161/Expert Group on Supply. CEN Brussels

Christopher, M. and Lee, H. (2004), "Mitigating supply chain risk through improved confidence". *International journal of physical distribution and logistics management*, Vol. 34 No. 5, pp. 388-96.

Christopher, M. (2005), *Logistics and supply chain management: creating value-adding networks*, Pearson Education, Harlow.

Closs, D. and McGarrell, E. (2004), "Enhancing Security Throughout the Supply Chain". IBM Centre for the business of government.

Clutterbuck, R. (1987), *Kidnap, hijack and extortion*. Basingstoke Macmillan, London

Douglas, M. and Wildavsky, A. (1983) Risk and Culture – An Essay on the Selection of Technological and Environmental Dangers. Berkeley, CA: University of California Press.

EC (2003), "Freight Transport Security". *Consultation paper*, European Commission, Brussels.

ECMT (2001 - a), *Theft of goods and goods vehicles*. CEMT/CM (2001)19, Lissabon.

ECMT (2001 - b), *Improving security for road freight vehicles*. OECD Publication Service, Paris

ECMT (2002), *Crime in road freight transport*. OECD Publication Service, Paris.

Ekwall, D. (2009 - a) *Managing the Risk for Antagonistic Threats against the Transport network*, Division of Logistics and Transportation, Chalmers University of Technology: Göteborg.

Ekwall, D. (2009 - b), "The Displacement effect in cargo theft". *International Journal of Physical Distribution and Logistics Management,* Vol. 39, No. 1, pp. 47-62

Ekwall, D. (2010), "On analyzing the official statistics for antagonistic threats against transports in EU: a supply chain risk perspective". *Journal of Transportation Security*, Vol. 3, No. 4, pp. 213-230

von der Embse, T. and Desai, M. S. and Desai, S. (2004)," How well are corporate ethics codes and policies applied in the trenches? Key factors and conditions". *Information Management & Computer Security*, Vol. 12, No. 2, pp. 146-153

Engdahl, O. (2003), *I finansvärldens bakre regioner – En studie om finansiella offshoremarknader och ekonomisk brottslighet*, Göteborg Studies in Sociology, No. 15, Sociologiska Institutionen, Göteborgs Universitet, pp 55-94 (in Swedisch)

EP - European Parliament's Committee on Transport and Tourism, (2007), *Organised theft of commercial vehicles and their loads in the European union*. European Parliament, Brussels

Frederick, W.C. (1995), *Values, Nature, and Culture in the American Corporation*. Oxford University Press, New York, NY.

Gips, M. (2006), "Cargo security getting some respect". *Security management*, July 2006, pp.28, ASIS international.

Howie, L. (2007), The terrorism threat and managing workplaces". *Disaster Prevention and Management*. Vol. 16, No. 1, pp. 70-78

Juttner, U. and Peck, H. and Christopher, M. (2003), "Supply chain risk management: outlining an agenda for future research". *International Journal of Logistics: Research and Applications*, Vol. 6 No. 4, pp. 197 – 210.

Kemshall, H. (2006), "Crime and Risk", in Taylor-Gooby, P. & Zinn, J (Eds), *Risk in Social Sciences,* Oxford: Oxford University Press, pp 76-93.

Klaus, P., Henning, H., Muller-Steinfahrt, U. and Stein, A. (1993), "The promise of interdisciplinary research in logistics". in Masters, J.M. (Ed.), *Proceedings of the twenty-second annual transportation and logistics educators conference*, pp. 161-87.

Kovacs, G. and Spens, K.M. (2005), "Abductive reasoning in logistics research". *International journal of physical distribution & logistics management*, Vol. 35, No.2, pp. 132-144

Kvale, S. (1997) *Den kvalititativa forskningsintervjun*. Lund: Studentlitteratur. (in Swedisch)

Lambert, D. and Stock, J. (1993) *Strategic logistics management*. Richard D Irwin Inc, US.

Lambert, D. and Stock, J. and Ellram, L. (1998), *Fundamentals of Logistics Management*, International ed., McGraw-Hill Higher Education, London.

Lumsden, K. (2006), *Logistikens grunder*. Studentlitteratur, Lund (in Swedish)

Manunta, G. (1999), “What is security?”. *Security journal*, Vol. 12, No. 3, pp 57-66, Perpetuity Press.

Manunta, G. (2002), “Risk and security: Are they compatible concepts?”. *Security journal*, Vol. 15, No. 2, pp 43-55, Perpetuity Press.

Mars, G. (1997), “Human Factor Failure and the Comparative Structure of Jobs”. Disaster Prevention and Management, Vol. 6, No. 5, pp 343–348.

Miles, M. B. and Huberman, M. A. (1994), *Qualitative Data Analysis – An Expanded Sourcebook,* 2nd edn, Thousand Oaks, CA: Sage Publications.
Muir, J. (1996), “Theft at work”. *Work Study*; Vol. 45.

Mythen, G. and Walklate, S. (2006), Criminology and Terrorism – Which Thesis? Risk Society or Governmentality? *British Journal of Criminology* , Vol. 46, No. 3, pp. 379-398.

Nilsson, P-A. and Rosberg, L. (2009), ”Polisens rapport on transportsäkerhet 2008”. *Polismyndigheten Västra Götaland & Skåne* (*in Swedish*)

Peck, H. (2008), “Risks in the Supply Chain – Can we Streamline the SC without Restriction?” *A presentation at Eurolog,* Göteborg 2008.

Reason, J. (1997). *Managing the risks of organisational accidents*. Burlington, VT: Ashgate Publishing Ltd

Reason, J. (2000). Human error: models and management. *BMJ*, 320, pp. 768-770.

Rittel, H.W.J. and Webber, M.M. (1973), ‘‘Dilemmas in a general theory of planning’’. *Policy Sciences*, Vol. 4, No. 2, pp. 155-69.

Roberts, D. (2006), “Human Security or Human Insecurity? – Moving the Debate Forward”. *Security Dialogue*, Vol. 37, No. 2, pp 249-261.

Rose, N. (1999), *Powers of Freedom – Reframing political thought.* Cambridge: Cambridge University Press.

Rose, N. (2000), “Government and Control”. *British Journal of Criminology*, Vol. 40, No. 2, pp 321–339.

Schary, P.B. and Skjott-Larsen, T. (2001), *Managing the Global Supply Chain, 2nd ed*., Copenhagen Business School Press, Denmark.

Seidman, I. (1998), *Interviewing as qualitative research – a guide for researchers in education and the social sciences*. New York: London, Teachers’ Collage Press, pp 79-94.

Speed, M. (2003), “Reducing employee dishonesty: In search of the right strategy”. *Security journal*, Vol. 16, No. 2, pp 31-48, Perpetuity Press.

Stern, M. (2006) ‘We’ the Subject: The Power and Failure of (In)Security, *Security Dialogue*, Vol. 37, No. 2, pp 187-205.

Stock, J. R. (1997), “Applying theories from other disciplines to logistics”. *International journal of physical distribution & logistics management*, Vol. 27, No. 9, pp. 515-539.

Stokes, R. (2007) “Coordination, Governance and Equity: A Research Framework for Security”, *Security Journal*, Vol. 20, No. 1, pp 15-18.

Svensson, G. (2000), “A conceptual framework for analysis the vulnerability in supply chain”, *International journal of physical distribution & logistics management*, Vol. 30, No. 9, pp.731-749.

Sweet, K. (2006), *Transportation and Cargo security*. Pearson Prentice Hall, New Jersey.

Tryon, G. and Kleiner, B. (1997), “How to investigate alleged employee theft properly”. *Managerial auditing journal*, Vol. 12, MCB University Press.

Tyska, L.A. and Fennelly, L.J. (1983), *Controlling cargo theft*. Woburn: Butterworth Publishers, Boston.