

Visibility Platforms for Enhancing Supply Chain Security: a Case Study in the Port of Rotterdam

Marcel P.A. van Oosterhout¹⁾, A.W. Veenstra²⁾, M.A.G. Meijer³⁾, N. Popal⁴⁾, J. van den Berg⁵⁾

¹⁾ RSM Erasmus University, Erasmus University Rotterdam, the Netherlands, moosterhout@rsm.nl

²⁾ RSM Erasmus University, Erasmus University Rotterdam, the Netherlands, aveenstra@rsm.nl

³⁾ TNO Built Environment and Geosciences, the Netherlands, markmeijer@planet.nl

⁴⁾ RSM Erasmus University, Erasmus University Rotterdam, the Netherlands, nawid.popal@gmail.com

^{5a)} Delft University of Technology, Faculty of TPM, the Netherlands, J.vandenBerg@tudelft.nl

^{5b)} Rotterdam University, Institute for Information Technology Programs, the Netherlands, bervd@hro.nl

Abstract

In this paper we describe how supply chain visibility platforms can be used to enhance supply chain security for maritime container transport. We use a three-step approach to define information needs for supply chain security. We map these information needs onto the current IT architecture and IT systems in the port of Rotterdam. This results into a gap analyses. We conclude the paper with a number of possible scenarios for the further development of supply chain visibility platforms. The paper is based on a field study conducted among 14 organizations in the port of Rotterdam in 2006 as part of the PROTECT research project.

Keywords

Supply chain security; IT architecture; visibility platforms; port community systems

1. Introduction

1.1 Background

In many supply chains world-wide, the parties are becoming aware that their increasingly complex supply chains also become vulnerable for attacks by terrorists and criminals. Some companies have a long record of measures against these threats, and others have just started to secure their supply chain in the wake of the recent terrorist attacks and the regulation that was issued as a result of these attacks. The focus of many of these regulations and measures are on air transport and on containerised transport.

In port supply chains the initiatives to increase security focus on maritime transport and especially on securing container transport and port facilities locations or port areas in which transshipment of cargo takes place. The

initiatives Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), Smart and Secure Trade lanes (SST) and various others have learned that secure supply chains can only be achieved by a combination of technology, clear rules and procedures and cooperation between companies and government. Obviously, the human factor always determines the ultimate success or failure of each security system (Verduijn and Becker, 2005).

Requirements for supply chain security and the role of IT and Inter-Organization Systems (IOS) are studied within the project PROTECT. PROTECT is a Dutch research project (2005-2008) funded by the Dutch transport research fund TRANSUMO (<http://protect.transumo.nl>). Within PROTECT participate the Port of Rotterdam, Dutch Customs, the shippers branch organization EVO, Transport and Logistics Netherlands, Holland Distribution Council, Det Norske Veritas, RSM Erasmus University, TNO, Technical University Delft and Buck Consultants.

1.2 Objective and structure of paper

The objective of this paper is to analyze the information needs for supply chain security, the role of supply chain visibility platforms and to develop migration scenarios towards a wider supply chain visibility for the port of Rotterdam.

We start this paper with a definition of supply chain security. In our definition we include terrorism, smuggle and theft as possible threats to security. Next, we analyse the key areas of risk in the supply chain with regards to security. We distinguish between physical security risks and information security risks. Next, we describe possible measures to respond to these risks. We distinguish between preventive measures, detective measures and corrective measures. Next, we specify the requirements and information needs which result from these measures. These information needs were validated in a field research study in the port of Rotterdam by

interviewing port managers from 14 companies. We map the information needs on the current IT architecture and IOS in the port of Rotterdam. This results into a gap analysis. The paper ends with a number of recommendations and possible scenarios to extend the current IT architecture and combine data from different IT systems to create a wider supply chain visibility platform, which enhances the overall level of supply chain security.

2. Supply Chain security

A secure supply chain is a supply chain where various measures have been taken to guarantee a certain level of security. Security measures can be taken with regards to (a combination of) physical flows, information flows and/or money flows (Veenstra, 2005a). Besides protection against terrorist attacks we include counterfeiting smuggling and preventing theft as the main reasons for supply chain security.

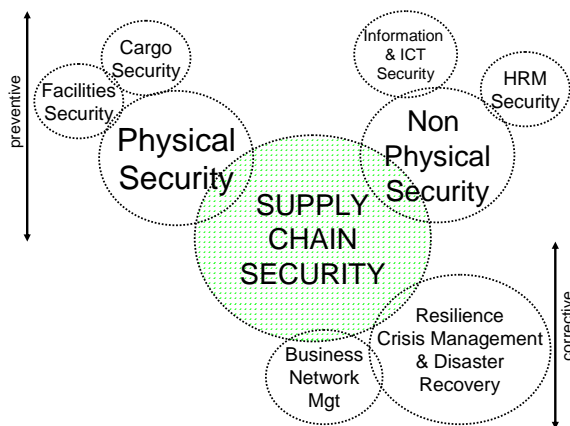


Fig. 1: Components of Supply Chain Security

Supply chain security is a wide concept, which entails both physical- and non physical security and preventive-versus more corrective measures. Examples of physical security and preventive measures are facilities security and security of cargo. Examples of non physical security and preventive measures are information security and security of personnel. One can also take another approach towards supply chain security, which implies organizing your supply chain in such a way, that in case a (security) emergency occurs, the supply chain quickly can recover into a state of normal operations. This area of research is resilience management and business

network management (Sheffi, 2005).

In this paper we focus on improvement of cargo security and information security. However, we will keep the general term supply chain security in the remainder of the paper.

3. Security Risks in global supply chains

3.1 Introduction

Figure 2 provides an overview of a typical port supply chain with an export flow, ocean transport and an import flow. A number of possible areas of security risks are indicated.

Security risks for specific supply chain nodes can be defined as a function of vulnerability for disruption of the supply chain and security controls or measures in place (Unisis, 2005). The largest security risks (or gaps) are found in those nodes or activities, where vulnerability for disruption is relatively high and security controls or measures in place are relatively low.

For instance in barge transport, containers are loaded in such a way that it is not possible to open them during the transport itself. The barge operates on inland waterways, which means that containers are not easily accessible by unauthorized people. Vulnerability for disruption of the supply chain for transport of containers via barge therefore can be considered relatively low.

In this paper we use the framework of Willis et al. (2004) to analyse supply chains that recognises three different layers (i.e. sets of activities): the first layer relates to physical activities, such as transport and transshipment. The second layer is a layer of contracting or transaction activities that encompass all commercial relationships between parties in the chain. Finally, we include a governance layer, in which all governing bodies with their inspection and verification activities are included.

3.2 Security risks in the physical layer

In general container and goods in motion reduces security related risks. Based on previous research (Goedhart & Hulsebosch, 2001; DNV Consulting, 2005) and interviews with various supply chain parties (Popal, 2007) a number of key areas of potential security risk in the physical supply chain have been identified. The transport supply chain (cargo or mobile unit) can be

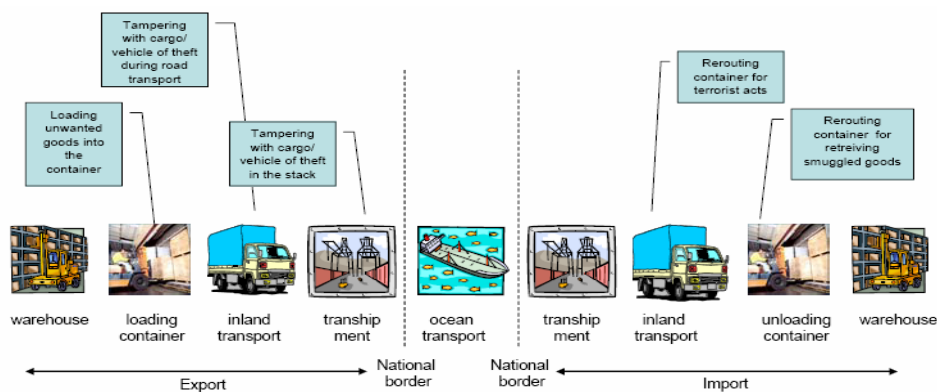


Fig. 2: Supply Chain Processes and security risks (Verduijn and Becker, 2005: 5)

used as a means to conceal and transport various explosives, incendiary devices or nuclear devices to a location where they are unloaded or detonated. Furthermore, the transport supply chain itself can be misused as a weapon (DNV Consulting, 2005).

One of the most critical points in the supply chain is the point of stuffing and (relatively less important) the point of stripping of a container. This is the point where illegal goods can be placed into the container for smuggling or terrorist objectives. This can also be the point of sealing, but in many supply chains this point is at a later moment in the supply chain (e.g. on arrival at the sea terminal). The points of stuffing and consolidation and transshipment points are other points in the supply chain with a potential security related risk. Stops during inland transport, for instance of trucks at parking places, are also potential areas of risk. Finally the point of arrival at the end-user might pose a risk, e.g. in case of return loads in the same container. Special attention deserves the handling of empty containers, which receives relatively little attention with regards to supply chain security. There are hardly any security controls or measures in place at the empty container depots and in the transport of empty containers from depots to points of stuffing.

3.3 Security risks in the transaction and governance layer

Besides physical security risks in the logistics process, the transaction and governance layers contain a number of potential information security risks. These are more or less related to security of the information accompanying the logistical process. Information security risks are related to the CIA criteria confidentiality, integrity and availability described in the British standard 7799 (BS 7799-1:1999). *Confidentiality of data* ensures that information is accessible only to those authorized to have access (authorization and authentication of the person who enters or modifies the data in the IOS). *Integrity of data* safeguards the accuracy and completeness of information and processing methods. Data (values) can be different at different moments in time (e.g. the goods description sometimes differs, depending of the status of the process). When is it treated by supply chain parties as being correct? An important criterion in this respect is to make use of original data sources as much as possible. *Availability and timeliness of data* ensures that authorized users have access to information and associated assets when required at the right moment in the supply chain. Access usually requires some sort of authentication, which can be something known (e.g. password), something possessed (e.g. cargo card) or something unique (e.g. signature or biometric details) (Turban et al, 2006). Port supply chains are characterized by dependencies on (timeliness and integrity of) data from previous parties in the supply chain.

A final requirement related to information security is non repudiation. *Non-repudiation* is the ability to limit parties from refuting that a legitimate transaction took

place, usually by means of a signature (Turban, 2006). This means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of *origin* proves that data has been sent, and non-repudiation of *delivery* proves it has been received (Wikipedia, 2007).

If a road operator has more detailed information regarding the contents of a container – which is not always the case – it can plan the safest route to its final destination and it can take preventive measures in case something happens to the container. However, the downside of increased transparency is that security relevant information can leak to unauthorized people, who can misuse this information for reasons of theft or conducting a terrorist attack. This stresses the importance of the CIA requirements to safeguard information security in the supply chain.

4. Security Measures & Requirements

4.1 Security measures and requirements

Based on risk assessments organizations should decide whether to focus on security measures to *reduce the probability* of a certain risk and/or focus on supply chain resilience to *reduce the consequences* in case of a (security) emergency (Rice, 2006). Security measures can be taken within the different layers as defined by Willis et al (2004). Some examples are given in table 1.

Table 1: Examples of security measures per layer (Veenstra, 2005a)

Layer	Type of Measure	Examples
Governance	Legal/policy measures	Laws, Incentives
Transaction	Organizational measures	Protocols & procedures, structuring, HRM-policy
	IT measures	authentication, VPN, encryption, chip card, biometrics
Physical	Physical measures	physical gates, camera's, smart cards

Security measures can also be categorized by their timing. We distinguish between three types of possible measures: preventive measures, detective measures and corrective measures (ISO, 2005). An example of preventive measure is safeguarding the area where the containers (with high value products) are stored by putting gates, high fences and surveillance camera's. This will make it more difficult for goods to be stolen from the containers. An example of a detective measure is the (nuclear) scanning of containers. By scanning the containers, a possible dangerous or illegal good that is inside the container is detected. This will prevent an incident to happen. Finally, if an incident has resulted in damage, security measures must be put in place to

correct the damage and recover the damaged supply chain. These are the so-called *corrective measures*. An example of a corrective measure is the presence of a Crisis Management Plan (CMP). CMP can be different dependent on the type of damage. For example if an empty container is stolen, it will disrupt the SC process of the companies concerned. To recover this disruption, a new empty container must be brought in the SC and the search for the stolen container must be started.

Lee and Wolfe (2003) describe three generic requirements or measures from a security perspective for creating a secure freight system:

1. *Assuring integrity of conveyance loading, documentation and sealing*
2. *Reduce risk of tampering in transit (with comprehensive monitoring of tampering and intrusion)*
3. *Provide accurate, complete and protected information about shipments to those who need it in a timely manner*

On the other hand, supply chain managers have four critical requirements from security processes (Lee and Wolfe, 2003):

1. *Commit to processing and inspecting qualifying shipments in ways that permit highly reliable and predictable processing times*
2. *Protect all commercial information given to authorities*
3. *Harmonize and standardize security processes internationally*
4. *Security and anti-tampering practices should be by-products of excellent supply chain management practices.*

The World Customs Organization (WCO), the International Organization for Standardization (ISO) and the European Commission are still in the middle of the process of defining the exact security needs and requirements. WCO and ISO define high level requirements which allow much flexibility in the way they are implemented. WCO and ISO do not clearly state what kind of security checks should be used and which information should be shared between supply chain partners. Some early results from EU-projects indicate that new EU-regulation may contain some rather specific measures that supply chains need to take up. Requirements from the US are most concrete and specified. CSI and WCO require all manifest information be electronically provided 24 hours before containers are loaded in to a vessel at foreign ports destined for US ports (Giermanski, 2007). Furthermore, more and more supply chain wide security is required from origin until destination (i.e. C-TPAT, Safe Port Act). Gradually, more guidance is provided in the development of functional requirements of supply chain security information systems.

4.2 Importance of supply chain visibility

Better visibility and control is the focal theme found in

most of the measures and requirements to mitigate the security risks. Supply chain security risks can be reduced or eliminated by increasing the visibility of the supply chain, i.e. providing transparency with regards to (the status of) physical flows, information flows and money flows (Lee and Wolfe, 2003). The transparency of a supply chain increases when more, timely and especially quality information becomes available throughout the entire chain. Three types of information are relevant in this respect: Cargo information, Process information (Tracking & Tracing) and information about the integrity of the goods and cargo carrier.

Supply chain visibility is a prerequisite for increasing supply chain security, but will also be the basis for various collateral benefits like increased logistics efficiency (Rice & Spayd, 2005). These benefits will be the trigger for supply chain parties to connect to chain wide visibility platforms. Visibility is important for the security of supply chains, because it may generate information that helps mitigating vulnerabilities. This requires a high level of information security, i.e., information that is correct and available if needed.

Visibility across the chain can help to make early identification of sources of risk against which countermeasures have to be taken (prevention – e.g. on the basis of data-mining). It can also help early identification of disruptions (detection, sensing) and reveal impacts of measures and structural weaknesses, and thus vulnerabilities (see Sheffi, 2005). Detective measures are needed to track any abnormal changes or deviations from planning. In case something does happen, corrective measures (responding) are needed to make the supply chain resilient and bring it back in normal operations as quickly as possible. These ideas are also put forward by Christopher and Lee (2004), who discuss supply chain risk and improved supply chain confidence and Dove (2001), who presents the sense-and respond organization and supply chain to respond to unforeseen events in an agile manner. Preventive and detective measures are part of the sensing phase, while detective and corrective measures are part of the responding phase (see Figure 3). Furthermore, learning should be incorporated to make security measures effective in the longer term.

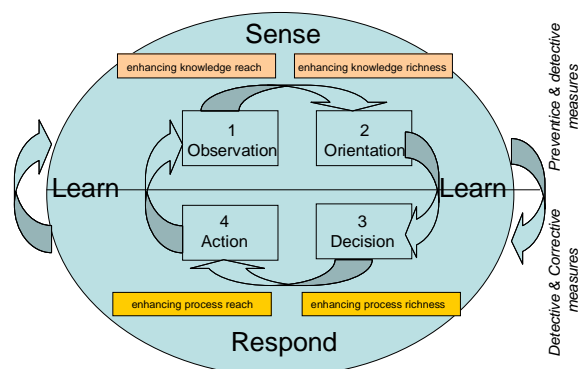


Fig. 3: Supply Chain Security Sense and Respond Model (adapted from Dove, 2001; Overby et al, 2006)

5. Information needs for implementing security measures

Three PROTECT expert meetings were organized with representatives from Port Authorities, the Port Community System Port infolink and Customs Officers to analyze the measures and information needed to effectively implement measures for supply chain security. These sessions resulted into a set of nine information blocks, which are most important in relation to supply chain security. Specific data can be needed for preventive measures, detective measures or corrective measures (Popal, 2007). A field research study was conducted via in-depth interviews among 14 managers to validate the results from the expert meetings. The most urgent security measures which resulted from the field study led to nine key information blocks. The information blocks and the most relevant data elements are summarized below.

1. **Booking Information** – this information block contains the initial (shipping line) booking ID, the B/L¹ number and the container number(s)
2. **Cargo information** – this information block contains data elements relating to the cargo inside the container (for example the description of goods, cargo value and cargo weight) as well as the status of the cargo along the supply chain (planned versus realization of delivery among different points along the supply chain).
3. **Nuclear detection** – in this information block information about the nuclear scan of the container is contained. Every container that is transferred via the port of Rotterdam via rail or road is scanned for nuclear contents via detection ports through the main access roads or terminal gates. In the future this will be extended with a nuclear detection of barge containers, for which a new in-land terminal close to the Rotterdam port area will be developed.
4. **X-Ray scan (container contents)** – this information block contains information about the scanning or inspection of the container contents. Examples of data elements within this block are the container scan type and the container scan results. These scans and inspections include both X-ray scanning and physical inspection by Customs and Heath Authorities.
5. **Container (status)** – this information block contains data elements about the container itself, like the container number, owner, TARRA, seal (status).
6. **Operator & location information** – this information block contains information about the locations where the container was handled (e.g. point of stuffing, origin sea port, port of discharge) and the

operators that handled a specific container (e.g. contact information and whether the operator is certified or not). For specific types of operators, information that is more detailed may be stored to meet specific information needs.

7. **Seal** – this information block contains data elements about the seal that is used for the container. Examples of possible data elements are the location of sealing, the seal type, seal status and the seal number. Furthermore, breaches should be recorded in (close to) real time with date, time and geographic location of the breach.
8. **Certificate information** – this information block contains data elements about the type of certificate, the issuing party, the duration of validity.
9. **Personnel** – this information block contains information about the personnel that handled the containers or opened the container during transport. This information includes personal (biometric) details, the organization for which the person is working and access rights to physical locations and/or IT systems.

The key information blocks, their interrelationships and data elements are shown in the entity relationship diagram in figure 4. The information blocks are denoted by the rectangles and the relationships are represented by the diamond shapes. For every relationship, the granularity is defined. The information blocks and the associated data elements represent the maximum of the information needs that the actors in the supply chain combined might have in the (near) future.

6. Current information architecture for Supply Chain Security

6.1 Introduction

Information Technology (IT) in general and Supply chain visibility platforms (SCVP) in specific are important elements in various security initiatives that have been presented in the maritime and especially the container industry. SCVP can be used to integrate information from the physical layer, the transaction layer and the governance layer to enhance supply chain visibility, which is the basis for supply chain security. In this section we describe the current IT systems in the port of Rotterdam, the IT technologies and platforms used to respond to security requirements and a further specification of the components of supply chain visibility platforms.

6.2 Current IT systems in the port of Rotterdam

We distinguish four categories of IT systems in the maritime transport supply chain. Table 2 provides an overview of these systems.

¹ Bill of Lading – Official legal document representing ownership of cargo, a negotiable document to receive cargo, and the contract for cargo between the shipper and the carrier (Rila, 2007)

Table 2: Comparison different IT systems

Layer	Community	Authority	Container Integrity	Business
Governance	X	X		
Transaction	X		X	X
Physical			X	X
Geographic Focus	Regional/ National	National (port) EU (Customs)	Global	Local/ Global

We will now shortly describe the four types of IT systems:

1. **Community systems.** This group can be divided into closed community systems (aimed at or representing a specific user group, like the booking system INTTRA) and open / neutral community systems. The neutral community systems are used by the companies and the regulatory authorities to exchange information. These systems act as an information broker between the different actors and fulfil the following functions: information aggregation, conversion and relay. An example of a neutral or open community system is Port infolink, the Port Community System (PCS) of the port of Rotterdam. This platform adds value to the business parties enabling them to exchange information more efficiently. The PCS uses a centralized information model, where data is stored centrally and made available to all parties who have access to the information. Another example is the PortKey / Cargo Card system, storing personnel (authentication) data (e.g. from truck drivers).
2. **Authority systems.** In these IT systems much information resides that can be considered security relevant. Parts of this information are shared between the different regulatory authorities, but are not made available to the companies. When the regulatory authorities do communicate with the companies, this is often on a bilateral basis. Important information that resides within the authorities' systems is (nuclear) scanning information and information about physical inspection of the (contents of a) container. Customs systems are fed by pre-arrival manifest information, which is used for risk analyses and data-mining purposes.
3. **Container Integrity Systems.** Examples of such systems are CommerceGuard and Savi Networks. These systems supply information about the integrity of the container during transport. An RFID reader infrastructure is used that communicates with devices attached to the container to check the integrity of the container. In the most basic form, these devices measure if the container was opened, but more advanced measuring instruments can be added. Measuring light intensity, humidity and temperature are several of the many possibilities when using these extra modules. The RFID-reader

infrastructure uses point-to-point monitoring of the container integrity devices. Besides point-to-points based infrastructures, also real-time monitoring integrity systems are deployed in the market (e.g. IBM, Impeva Labs), based on a combination of e-seals and GPS communication. Most Container Integrity Systems store the integrity data in a centralized system, which can be accessed by the customers or by authorities (on request). Some systems are developed using a distributed data model, based on a service oriented architecture (IBM, 2006a, 2006b).

4. **Business systems.** Information systems of individual companies, like terminal systems, shipping line systems.

6.3 Security requirements and IT technologies used

Table 3 presents the key security requirements and measures as discussed in section 4.1 and the IT technologies and systems used to operationalize these measures. Supply chain wide visibility platforms (SCVP) are based on a combination of these technologies and IT systems.

Table 3: Security requirements and IT technologies

Security requirement	Layer	IT technologies used
1. Assuring integrity of conveyance loading, documentation and sealing	Physical Transaction	<ul style="list-style-type: none"> • Container Integrity Systems (which combine electronic container seal technologies, Global Positioning Systems, RFID reader infrastructure and a centralized or distributed IOS architecture) • Anti tampering Devices • Tracking & Tracing systems (Wireless communication and GPS) • Videos loading process
2. Reduce risk of tampering in transit (with comprehensive monitoring of tampering and intrusion)	Physical Transaction	<ul style="list-style-type: none"> • Gamma & X Ray devices • Radiation & Detection devices • Route planning systems
3. Provide accurate, complete and protected information about shipments to those who need it in a timely manner	Transaction	<ul style="list-style-type: none"> • Authorization & Authentication via smart cards with biometric identification details • Information brokers i.e. Port Community Systems (PCS) • Alerts (e.g. SMS, mobile) • Container Integrity Systems
4. Overall improvement of risk assessment	Governance	<ul style="list-style-type: none"> • Advanced data analysis via data-mining and risk assessment technologies • Combining and comparing (meta)data which are transferred e.g. via the PCS • Smart agent technologies

6.4 Components of Supply chain security platforms

Supply chain visibility platforms (SCVP) consists of three important components (Veenstra et al, 2005). SCVP facilitate data capture of the physical processes in the logistics by means of technologies such as RFID tags, electronic seals or anti-tampering devices that collect information opening and closing containers, movement, stand still, entering and existing gates with dates, times, and personal authorizations. This information in itself is not sufficient to make the supply chain more secure. In fact, its only information value is that it records what actually physically happened. To use this information from a security point of view, one would have to know what was expected to happen. This information might contain data on the times that the cargo should be moving, times that is should be stationary, times that it is being inspected, times that it should have arrived at some location, exact weight and description of the cargo, optimal cargo conditions and so on. Matching these expectations with what actually happened will result in the type of insight that is required for securing the chain. Deviations from the expected will raise alerts that need to be followed up by immediate actions. Progress that closely follows the expected raises the confidence in the security of the flow of goods. Thirdly, SCVP should facilitate the exchange of other security relevant information, such as nuclear and X-Ray scan images and results of physical inspections.

7. Gap analysis

Based on the information need specified by the different

stakeholders in the port supply chain (section 5), we conducted a mapping on the existing data in the various IT systems in the port of Rotterdam (section 6). This results in a gap analyses (information need versus information availability). In figure 4 it shows that a lot of security relevant information is available at supply chain actors and in electronic format, however in different IT systems and sometimes the same information can be found in different systems. Currently, some data elements are not available or not stored at all. These relate mainly to data blocks 3 (nuclear scan) and 8 (certificate information). A first glance on the gap analysis and ERD in figure 4 shows that complete visibility might be created by combining local information from supply chain actors, port community systems, nuclear detection infrastructure and authority systems (e.g. Customs) with the information available in global Container Integrity Platforms (e.g. Savi, Commerce-Guard/GE and IBM) and global Cargo Booking platforms (e.g. GT Nexus, INTTRA).

Besides the gap analysis we made an analysis on the coverage in various IT systems in the Port of Rotterdam community (see Figure 5). With coverage we distinguish between coverage in width (number of different data-elements which are in the IT system) and coverage in depth (number of containers which are in the IT system that are shipped via the port of Rotterdam). Figure 5 shows the PCS in itself already contains 72% of the number of different data elements relevant for supply chain security, while also providing sufficient depth coverage for most of the data-elements (close to 100%).

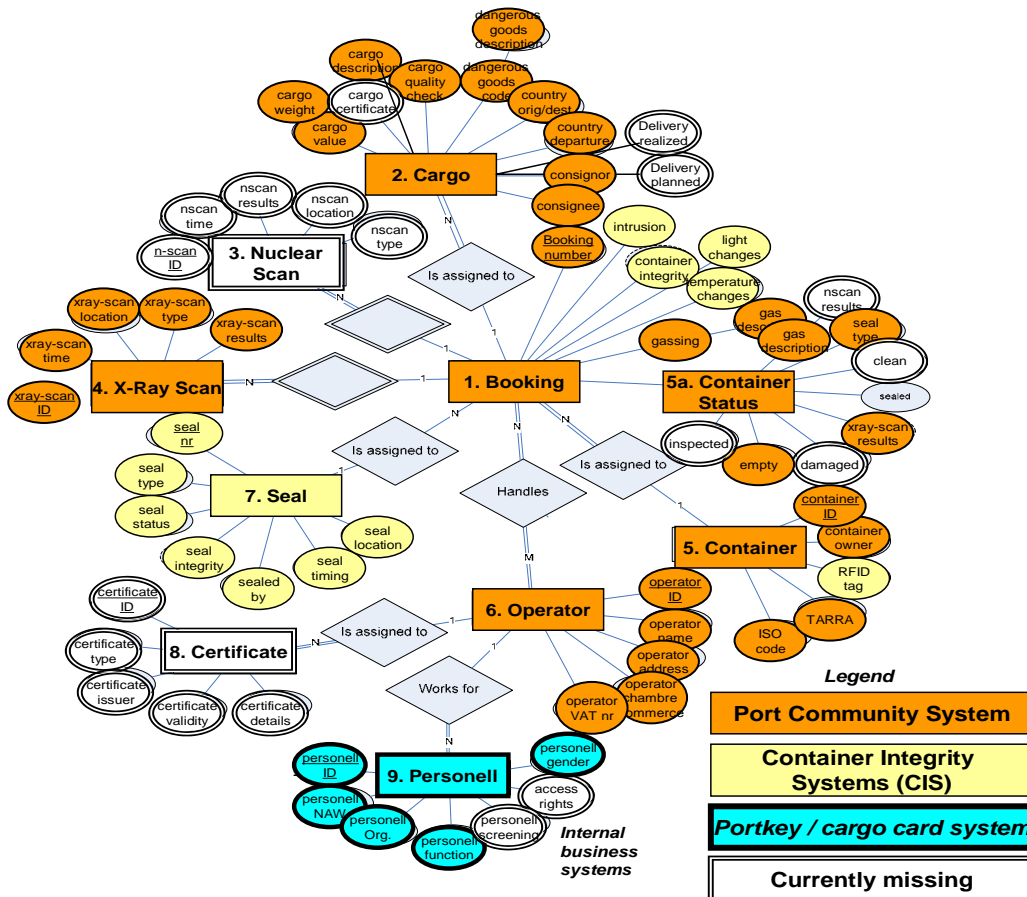


Fig. 4: ERD of information blocks and coverage (in width) in Port of Rotterdam IT systems

A coverage (in width) of about 80% of all relevant data elements can be achieved by combining data from the PCS, the Container Integrity Systems (CIS) and Customs authority systems (Meijer, 2007). However, the coverage in depth of CIS so far is very limited, as is shown in figure 5. Only a few high value containers are equipped with the relatively expensive security devices and e-seals. The introduction of the WCO bold seal, as a cheap alternative to ensure container integrity, will boost the number of containers equipped with such a seal – however with a limited set of data elements from information block 7.

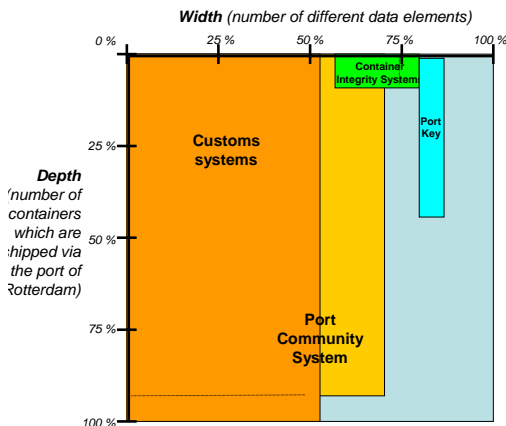


Fig. 5: Coverage security relevant data in Port of Rotterdam IT systems

Ultimately, from a supply chain security perspective, coverage of security relevant data elements by combining data from different IT systems of 100% (in width and depth) would be favourable. However, achieving 100% coverage will be a very difficult challenge, given the number of parties involved, the limited readiness to share data and the complexity of a typical port supply chain. We expect that increased information visibility only can be achieved, if organizations can achieve business benefits from sharing security related data.

Therefore, a selection should be made of the most relevant data elements on the one hand (which can lead to business benefits and enhance supply chain security), while scenarios should be developed for the migration of different IT systems to combine into a broader visibility platform, covering the most relevant supply chain security data elements (to achieve coverage in width and depth). In section 8 we will elaborate on a number of possible scenarios.

8. Scenarios and IT architecture for supply chain visibility

8.1 Introduction

To make recommendations for the future information architecture for supply chain security, different scenarios for the need for security relevant information are analysed. These scenarios vary in the degree of market and government driver. Before 9/11 both drivers were

relatively low. Since then and currently the government driver is relatively high, while the market driver is still relatively low.

We expect three possible scenarios. In scenario 1 the government driver remains relatively high and the market driver for exchanging security relevant information remains relatively low. In this scenario the information architecture will change only marginally with limited costs in order for the system to be acceptable to the parties that use the system. In scenario 2 the government driver becomes even stronger. A lot of new regulations require extra information to be exchanged. In this scenario businesses find some benefits, but the business driver remains relatively medium to low. In scenario 3 both the business and government drivers are high. We expect this scenario, in case there are sufficient (logistics) effects and benefits for the various stakeholders in the supply chain, while supply chain security is seen as *by-product of excellent supply chain management practices* (Lee and Wolfe, 2003). In this scenario the system can change more radically and can be more complex. The users of the system will invest more time, effort and money in the system, because of the high perceived value of security relevant information. Figure 6 describes the three possible scenarios.

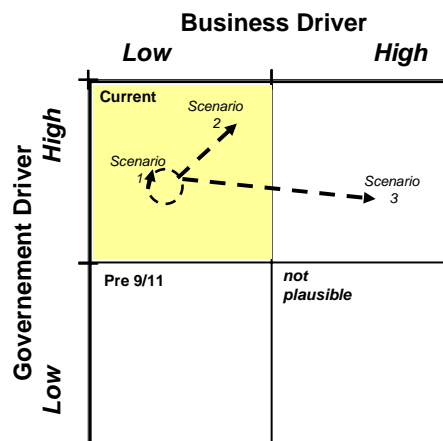


Fig. 6: Drivers of Supply Chain Security and possible future scenarios

Information brokers like the PCS Port infolink in Rotterdam play an important (regional) role in all three scenarios. They provide connectivity, conversion services, aggregation and re-usage of data. Given their central – and in most cases neutral - position as information node in the transaction layer, they are an excellent candidate to provide the backbone and coverage in width and depth of the data-elements which make up supply chain wide visibility platforms. Besides data from the transaction layer, PCS can provide security profiles and business performance management information up to the level of individual containers, to provide insight in security relevant information and present visibility information to responsible parties and authorities. A next step is to connect the PCS to information from the physical layer.

8.2 Discussion of the scenarios

In the first scenario, where the drive for exchanging

security relevant information is low compared to the current situation, only the most important data elements are exchanged. For the information security architecture, most security relevant information is already available in the PCS. Important new information elements that have to be added are the operator certificate details (from the Customs authority systems) and container integrity information (from the CISs). Linking these systems to the PCS will ensure that a high degree of coverage in width can be reached. This scenario is not very likely, given all the requirements and increasing government legislation on supply chain security.

In scenario 2 the government driver becomes even more pressing than currently, while businesses still perceive limited benefits and therefore have a low business driver. In this scenario the information requirements – especially from Customs – causes the overall information requirements to increase significantly. It is shown in Meijer (2007) that by linking the PCS, the CISs and the authority systems coverage of the security relevant information can be reached only to a certain degree. To achieve a greater coverage the companies active in the supply chain have to gather and exchange additional information. The companies can be enforced to exchange this additional information or they can be positively motivated via advantages offered by the regulatory authorities (for instance offering green trade lanes and reduced checks). Information brokers can play an important role in the exchange of the additional information between the transaction layer and the governance layer.

Finally, in scenario 3, both the market and the government have a large incentive to exchange security relevant information. In this scenario the information needs from the actors in the supply chain are the most extensive. A larger proportion of the information required is only available in individual business systems or has to

be gathered by the companies themselves. Because of the large market driver and the increased value of security relevant information companies can become hesitant to share information for competitive purposes. Having certain information can provide a competitive advantage. In this scenario information brokers co-exist with a more distributed approach. In a distributed architecture access rights can be managed locally which puts the control over the information more into the hands of the organization owning the information. Furthermore, the growth of container transport and the number of data elements exchanged between the companies and the regulatory authorities will effectuate a more distributed architecture. However, this poses many constraints on the level of ICT sophistication, and therefore is mainly interesting for larger companies.

8.3 IT architecture for supply chain visibility

We expect scenario 2 to be most probable in the short term. Governments (Customs, Port Authorities) increasingly require more security relevant information, while companies are not (yet) aware of the business benefits increased supply chain visibility can bring. In the longer term we expect a move towards scenario 3. A possible future IT architecture for supply chain security in scenario 2 for the port of Rotterdam is shown in figure 7. In this architecture the PCS, different Container Integrity Systems and authority systems are linked. The architecture will probably be a combination of a centralized data model (sharing of data via a broker) and a distributed data model (authorizing access to authorized users on distributed databases i.e. a Service Oriented Architecture).

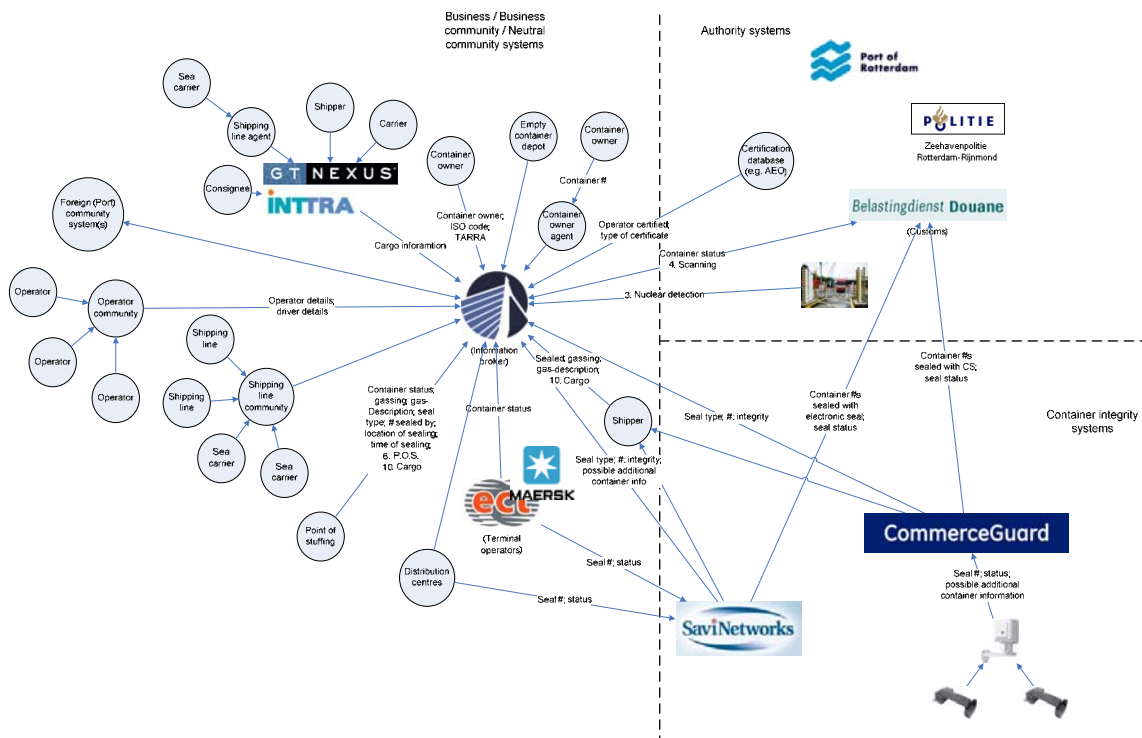


Fig. 7: Possible future IT architecture for Supply Chain Security in Port of Rotterdam

9. Conclusions and recommendations

9.1 Summary and conclusions

Supply chain security is an important topic for shippers, operators and authorities. In the field of supply chain security physical and non-physical measures can be taken to reduce or prevent these threats. Better visibility and control is the focal theme found in most of the measures and requirements.

The largest security risks (or gaps) are found in those nodes or activities in the supply chain, where vulnerability for disruption is relatively high and security controls or measures in place are relatively low. The largest security risks are the point of stuffing and stripping of the container, the transshipment processes and the stops during in-land transport. Furthermore, a currently underexposed process where breaches of security can occur is the handling of empty containers, since there are hardly any security controls or measures in place at the empty container depots and in the transport of empty containers from depots to points of stuffing.

Taking measures that especially help counter threats in these processes will make the supply chain more secure and will protect both human and economic entities. Information needs that correspond with these risks can be summarized by the following categories of information elements: booking, cargo, nuclear detection, X-ray scan, container (status), operator and location, seal, certificate and personnel information. For each of the information blocks the total information requirement and importance was identified and mapped on the current information availability in the IT systems that are used in the port of Rotterdam.

Currently the information resides within 4 main categories of systems: community systems, authority systems, container integrity systems and internal business systems. A lot of information is available in electronic format; however the various systems differ in coverage with regards to width (type of data elements) and depth (coverage of the total container flows).

Three scenarios were defined towards the development of a wider supply chain visibility platform for the port of Rotterdam. The scenarios differ in the degree of market and government driver and ultimately define the number of information elements exchanged between the different supply chain actors. The scenario which has the highest probability in the short term is the scenario where governments (Customs, Port Authorities) require more and more security relevant information, while companies are not (yet) aware of the business benefits increased supply chain visibility can bring. In the longer term we expect a move towards a scenario where both the market and the government have a large incentive to exchange security relevant information – each with their own objective.

The IT architecture for such a supply chain visibility platform supporting these scenarios will be developed in a number of steps. The first step is to link the PCS, different Container Integrity Systems and the authority

systems and share data – to provide for a wider coverage of the total data set needed for supply chain security. In the future, this centralized data model will be supplemented with a more distributed data model (where authorized users get access to distributed databases i.e. a Service Oriented Architecture).

9.2 Recommendations for further research

Although the research so far has resulted in a number of interesting management insights and research results, there are a number of open issues from a business perspective and directions for further research.

From an organizational point of view more research is needed on the adoption factors and implementation process of IOS aimed at increasing supply chain visibility. To enhance adoption and usage, more analysis is needed and measurement tools need to be developed on costs, benefits and (logistics) effects of such platforms. This research can build upon the work of Lee & Whang (2003) and Rice & Spayd (2005). This research can be the basis for the development of new incentive and business models.

There is a contradiction in the way supply chain security is dealt with at the moment. On the one hand there is the trust based paradigm (certificates and trusted parties, e.g. AEO). On the other hand there is the control and monitoring paradigm (increased controls via (100%) scanning, eSeals etc). What is the exact position of both paradigms in enhancing supply chain security? What are new concepts for trust and control - based on information transparency? And how can existing processes and procedures be redesigned to optimally make use of the supply chain visibility platforms?

Previous research has shown that increased network horizon (or increased supply chain visibility) has positive effects on network (or supply chain) performance (van Liere, 2007). However, our research shows there are different perspectives towards network horizon – from an (information) security perspective increased network horizon might lead to higher security risks and lower network performance. This new perspective on network horizon requires further empirical research.

With regards to supply chain visibility platforms more research is needed on the exact scope and the type of services. We expect a trend from tracking & tracing of containers to tracking & tracing of individual cargo units. Tracking & tracing is merging to a sensing and pacing concept throughout the complete supply chain. From a technical point of view this means more research and pilots are needed to couple centralized architectures and IOS with decentralized architectures and devices into the physical layer.

10. Acknowledgements

The authors acknowledge the funding from the BSIK Transumo project. We are grateful for the contributions from the partners in PROTECT, especially we would like to mention Iwan van der Wolf (Port infolink). Furthermore, we would like to thank the organizations which cooperated in the field research and the col-

leagues from the department of Decision and Information Sciences of the RSM Erasmus University, who provided constructive feedback on previous versions of this paper.

References

- BS 7799-1:1999 (1999), "Information security management - Part 1: Code of practice for information security management", BSI/DISC Committee BDD/2.
- Christopher, M. , Lee, H. (2004), "Mitigating supply chain risk through improved confidence", International Journal of Physical Distribution and Logistics Management, Vol. 34, No 5, pp 388-396.
- Dove, R. (2001), "Response ability: the language, structure and culture of the agile enterprise", John Wiley & Sons.
- DNV Consulting, (2005), "Study on the impacts of possible European legislation to improve transport security", Report for the European Commission DG TREN.
- Giermanski, J. (2007), "Is it safe?", Cargo Security International, Vol. February/March 2007.
- Goedhart, E.J. & Hulsebosch, B., (2001), "Risk Analysis of Container Import Processes", Virtuele Haven Project report.
- IBM (2006a), http://www.ibm.com/news/nl/nl/2006/10/nl_nl_news_20061025a.html (Accessed on: 2007-04-24).
- IBM (2006b), <http://www.nesdis.noaa.gov/space/library/workshops/2006-01-25/beckner.pdf> (Accessed on: 2007-04-24).
- Lee, H. ,Wolfe, M. (2003), "Supply Chain Security Without Tears", Supply Chain Management Review, Vol. January/February 2003.
- Lee, H., Whang, S. (2003), "Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management", GSB Research Paper No. 1824, October 2003
- Meijer, M., (2007), "Supply Chain Security in Container Transport – Recommendations for an IT architecture for Supply Chain Security", PROTECT report.
- Overby, E. Bharadwaj, A. , Sambamurthy, V. (2006), "Enterprise agility and the enabling role of information technology". European Journal of Information Systems Vol 15 No 2
- Popal, N. (2007), "Supply Chain Security in Container Transport – Information Needs", PROTECT report.
- Rice, J.B., Spayd, P.W. (2005), "Investing in Supply Chain Security: Collateral Benefits:", IBM Centre for the business of the government, <http://www.businessofgovernment.org/> accessed on 21-2-2007.
- Rice, J.B. (2006), "Supply Chain Response to Disruption: Advantage through Resilience and Security", Presentation at Cross-Border International Industry Conference on Supply Chain Security Management, SCSM2006, Montreux / Vevey, Switzerland.
- Rila (2007), http://rila.interactive.biz/scs_glossary.htm (Accessed on: 2007-01-12)
- Sheffi, Y (2005), "The Resilient Enterprise – overcoming vulnerability for competitive advantage", Cambridge: The MIT Press.
- Turban, E., King, D., Viehland, D., Lee, J. (2006), „Electronic Commerce 2006: a managerial perspective“, Pearson Prentice Hall, New Jersey
- Unisys (2005), "Secure Commerce Roadmap Whitepaper"
- Van Liere (2007), "Network Horizon and the Dynamics of Network Positions", PhD Thesis Erasmus Research Institute of Management
- Veenstra, A.W., Becker, J.F.F., Vrijenhoek, N. (2005), "Secure global supply chains: Towards a theoretical framework", PROTECT paper.
- Veenstra, A.W. (2005a), "Supply chain security Definitions, PROTECT report D1.2", RSM Erasmus University Rotterdam.
- Verduijn, T., Becker, J. (2005), "IT tools for security", PROTECT report.
- Wikipedia (2007), <http://en.wikipedia.org/wiki/Non-repudiation>, accessed on 21-2-2007.
- Willis, H.H. & Ortiz, D.S. (2004), Evaluating the Security of the Global Containerized Supply Chain, TR-214, RAND Corporation.