Towards the design of Secure Supply Chains

Marcel Ludema
Delft University of Technology
Faculty or Technology, Policy & Management
Jaffalaan 5
2628BX Delft
The Netherlands
+31 278 1885 (phone)
+31 278 2719 (fax)
m.w.ludema@tudelft.nl

Abstract
Supply chains are the life-lines of society and disturbances or disruptions should be avoided where possible. Secured by adequate protection is possible, but this is based on supply chain designs that are already in place. Designing secure supply chains means to understand security in relation to other supply chain design issues. What the right issues are and how to apply them and with the support of what type of tools is not well understood yet. In this article a set of suitable concepts from desk-research from several scientific fields are identified. These concepts compiled in a descriptive supply chain design framework can guide supply chain designers during the design of (secure) supply chains.

Introduction
Supply chains are the life-lines of societies. If these supply chains are vulnerable for disturbances and disruptions the supply of goods and services may be in jeopardy. Reliable and invulnerable supply chains will decrease the probability of failures.

Only in the case of re-design, reconfiguration or complete new design of a supply chain, invulnerability can be built in to make them more secure and/or resilient for unwanted or unanticipated external forces.

The approach used in this research is the selection of a set of suitable concepts from desk-research from several scientific fields. These selected concepts were compiled in a descriptive supply chain design framework that guide supply chain designers to design more secure supply chains.

The need for secure supply chains
Traditionally supply chain management has it focus on the physical flows of services and goods either pushed or pulled. More often it is the informational and financial flow that plays an important role in supply chains. So what can be the result when disturbances or disruptions in one of these flows occur? It will result in situations where the supply of services and goods is in jeopardy or will loose considerable quality.

In some situations some types of security may only be needed in case of a threat situation. It is not yet comprehensive enough how one increase the security of supply chains by addressing the right issues in a balanced way during the design or the redesign of supply chains in respect to all three flows; physical, informational and financial.

Internal & external influences
Supply chains are vulnerable to adverse events causing supply chain malfunctions and supply and demand disturbances & disruptions; like: interfering by third parties, labour strikes, natural hazards, human errors, changes in customer taste, technological failures, financial distress, etc. etc. Failures in supply chains also occur when it cannot respond to large fluctuations and uncertainties in demand and supply.
External influences on the supply chain can be natural disasters like earthquakes, flooding, extreme weather conditions, or technology like the crash of an airplane, tunnel accidents, or terrorist attacks. Natural causes often strike randomly. Causes of human nature might strike randomly or are planned ahead and can hit the most vulnerable locations of a supply chain depending on the motives of the attacker. Hitting a specific area might lead to more casualties and bring big headlines but will not necessarily lead to supply chain distortion or disruption. A smart attack to security flaws. [1]

Security & Resilience

Security is the scale of safeguarding against unwanted external effects. It is clear that this is security after the fact. Instead of waiting if security is up to level it is better to incorporate security issues during the design phase of supply chains. One of the built-in qualities a supply chain can be resilience; the ability to mitigate or avoid disturbances and return to the normal situation as soon as possible. [1] Security is what is experienced as the effect of several drivers of supply chain disruptions and resilience as the number of possibility companies or supply chain can pursue to avoid possible consequences from security flaws. [1]

Secure Supply Chain Requirements

Based on experiences from a wide range of fields, some of them closely related to supply chain management and others distantly or not at all related, a selection was made of “known” concepts. These concepts were derived by means of eclectic analysis using analogy with concepts directly or indirectly taken from several scientific and professional fields. The concepts that will be addressed are:
1. Value network & logistics utility analysis;
2. Bottleneck identification;
3. Customer order decoupling point;
4. Logistics pyramid
5. Multi-layer perspective on supply networks;
6. Supply chain stakeholder analyses & engagement;
7. Transaction cost theory & organizational interfaces;
8. Design for (high) reliability
9. Supply chains as nearly decomposable systems;
10. Scale-free supply networks;
11. Swarm intelligence;
12. Design to X-ability;
13. Low vulnerability by right partnerships;
14. Design for (high) reliability;
15. Design for (low) risks;
16. Designing secure supply chain interfaces.

Ad.1. Value network & utility analysis

Porter’s value chain/system/network (fig. 2) is always a good way of communicating the value-adding process. [2] This value-adding process is based on four utilities, each are in need of a different set of security measures.

Figure 1: Supply chain security & resilience [1]

Security measures make the supply chain longer (in time & costs), but following some of the approaches and concepts discussed below might avoid unnecessary costs, time and money.
locations makes the supply chain less vulnerable for disturbances and destructions.

Stability is keeping and storing goods in facilities. In case of fast movers it is wise to stabilize goods in smaller quantities close to the point of consumption and in the case of slow movers it is wise to stabilize goods in larger quantities at centralized locations.

Translation means goods in transition during transport between two locations. This is almost always done in a multi-modal manner, outsourced, and with a large number of parties involved. INCO-terms are the leading measures to identify responsibility and ownership of the goods and the information that relates to it. Understanding the options for tracking and tracing, bar-coding and paperwork is crucial in setting the right security measures.

Possession is the exchange of ownership of goods and services. Sometimes goods are at the location of the potential buyer but not yet in the possession of this buyer. Very common forms that need special attention to supply chain security are Supplier and Vendor Managed Inventory.

Ad.2. Bottleneck identification

The bottleneck of a system is the subsystem with a capacity that dictates the capacity of the overall system. [3] Increasing the capacity of this subsystem increases the capacity of the overall system, while increasing the capacity of other subsystems does not increase the capacity of the overall system and can be seen as unfeasible investment. After the capacity of the bottleneck has been increased beyond the bottleneck threshold, other subsystems become the bottleneck of the overall system. This means that bottlenecks are unavoidable but understanding the interrelation of the bottlenecks gives insight in the vulnerability of disturbances or disruptions. Emphasis on supply chain security should take place on the subsystems that are indicated as the potential bottlenecks of the overall system and less on the others subsystems. Bottlenecks can be found in physical, informational/administrative and financial flows.

Understanding bottlenecks is crucial to be able to come up with the right security measures at the right location.

Ad.3. Customer order decoupling point

In every supply chain a focal company is controlling the customer decoupling point; this is the point where the demand is dictated by the customer against a supplier organizing a fulfillment structure [4], figure 3.

Figure 3: Customer order decoupling point (adapted from [4])

The customer order decoupling point dictates the coordination of the supply chain and at the same time is the most fragile part of the supply chain and the physical, informational/administrative and the financial flow, though the decoupling points of these three flows do not necessarily have to collide. Taking measures to secure these customer decoupling points is important to secure the overall supply chain.

Ad.4. Logistics pyramid

Subsistence, operational and systems logistics are different types of logistics that are pyramidal related (figure 4). [5]

Figure 4: Logistics pyramid [5]

Subsistence logistics deals with the necessities of daily live like basic food, water and shelter. It is quite easy to estimate. Subsistence logistics is always the foundation for the more complex types. Operational logistics deals with the niceties of live; making and selling all kinds of things that are consumed day-to-day but depending on the circumstances often things
humans could easy life without. Depending on the type of good this is harder to estimate and more determined by demand driven processes. Subsistence and operational logistics mostly relate to consumables. Systems logistics relates to durable systems with a long life cycle and high investment. The need for systems logistics is hard to predict.

Understanding the pyramidal relationship helps to build secure supply chains, because it gives guideline to the design of supply chain and helps to build-in robustness and the type of dependencies one has to design or that can be avoided between the different types of logistics.

Ad.5. Multi-layer perspective on supply networks

Value can be added in several ways. More and more companies outsource non-core business activities. Often these activities are part of the physical layer of the value pyramid (figure 5). While outsourcing they concentrate on those activities that generate the most value and less on those that do not. They find that innovation in how to bring services to the market (virtual layer) is more important that selling products alone. New combinations are made and knowledge of how to bring service to the market becomes the crucial business activity. Finally these companies make the value creation of using knowledge of using services of using products as their business.

Within the design of supply chains these relationships need to be understood to understand where the real value is located, how the several layers are interrelated and how to secure security.

Ad.6. Supply chain stakeholder analyses & engagement

A supply chain stakeholder is any group or individual including other companies in the supply network who can affect or is affected by the achievement of the business' objectives. [6] Regularly keeping track of the position of stakeholders that relate to the supply chain is always a crucial thing to do (figure 6). Next to that it is wise to keep a stakeholder engagement plan so if things change in the business environments of the supply chain it is immediately clear what stakeholder to engage and in what manner. In the case of threats it is even more important that a solid stakeholder engagement plan is available.

Designing supply chain with keeping the position and movements of important stakeholders in mind leads to more robust en resilience solutions that when these issues are ignored.

Ad.7. Transaction cost theory & organizational interfaces

The issue of outsourcing was already discussed before. The type of relationship companies seek while outsourcing is determined by the length and intensity of co-operation among companies within a logistics network. To design effective logistics networks one needs to take the type of co-operations into consideration [7]:

- traditional customer-supplier relationship for sources that can be found everywhere no real co-operation is necessary;
- supply management for sources that can be found everywhere but where the finding time and effort is minimized;
- supply chain management for sources that are of crucial important and long-term and intensive co-operation is necessary to avoid failure;

Figure 5: Multi-layer perspective on supply networks

Figure 6: Supply Chain Stakeholder Analysis
• virtual organizations, in full grown markets like in the automotive industry products and services (highly specialized and complex) are modular and standardized so switching between suppliers is possible.

During the design of supply chains one needs to understand that choosing the right co-operation is always necessary. The chosen structure determines for an important part the inherent security. But on top of that it is important that building into the negotiation especially what the impact of security is and what to agree upon to can make the supply more secure in situations of supply chain impacts.

Ad.8. Design for high reliability

High Reliability Theory seeks to understand the reliability of organizations. The theory characterizes organization high-reliable if they enjoy evidence that high safety or reliability over long periods of time: “How many times could this organization have failed resulting in catastrophic consequences that it did not? If the answer is on the order of tens of thousands of time, the organization is ‘high-reliable’” [8].

Important characteristics that can be treated during design are flexibility and redundancy. This can be identified as not to rely too much on a small group of suppliers, input products, production locations, warehouse locations, transport facilities, and customers. In case of many decisions the Pareto Optimum Rule applies. 20% of the supply chain suppliers are responsible for 80% of the costs, and 20% of the customers are responsible for 80% of the revenue, and so on. If this 20% is a very small base and something happens to this base, the possibilities to restore functionalities are limited. So even the trend is at some market towards fewer organizations to deal with the advice is to have a base that is large enough in size with the knowledge that if one of the members of this base fails the other members can compensate for the capacity.

Special supply chain attention to what the A-articles and fast-movers are seems necessary. In case of supply chain impact it are often the C (subsistence) articles that needs to be secured first. Track ABC changes during all phases of the Product Life Cycle seems a wise thing to do.

Ad.9. Supply chains as nearly decomposable systems

Within decomposable (hierarchic) systems boundaries are determined by significance differences between the internal and external interactions. These interactions have different orders of magnitude (frequencies and importance) on different levels. In reality most systems are near-decomposable in nature; interaction between sub-systems is weak but not negligible. In a near decomposable systems the short-run behaviour is independent but in the long run behaviour is aggregated. [9]

Suggested for the designing secure supply chain is makes sense to determine the boundaries of organizations, supply chains and clusters by mapping (matrix) the frequency, duration and relevance communication processes of day-to-day supply chain processes, and compare and analyze transitory of these matrices over time.

Ad.10. Scale-free supply networks

Random network like some highway systems consist of nodes with random placed connections that are vulnerable for random exclusion failure or attacks (the network breaks down).

In a scale-free network a few nodes exhibit extremely high connectivity (essentially scale-free) while the vast majority is relatively poorly connected. [10] Scale-free networks, like hub-and-spoke systems in the international airline systems, are far more common than random networks. Scale-free networks are robust against random exclusion, failures or attacks, and will usually survive such attacks. Scale-free networks are very vulnerable for coordinated exclusions, failures and attacks.

Figure 10. Scale-free network [10]
The following steps to use this concept in the design of secure supply chains can be taken: (1) Determine the random and scale-free structures in the supply network businesses operate in. (2) Analyse the network structure will give insight in the vulnerability of the networks businesses are part of. (3) Determine the ideal number and share of suppliers and customers of your business.

**Ad.11. Swarm intelligence**

Swarm intelligence-related concepts are based on self-organization, where smaller parts can operate independently and are not controlled by a central body. [11] The ‘spider’ is controlled centrally, taking away the head and the spider dies. The legs of the starfish operate even being part of the same body independently, cutting a leg doubles the starfish. [12] The Borg in the TV-series of Star Trek is a good example of what swarm intelligence is. Another is the terrorist cells of Al Qaida.

**Ad.12. Design to X-ability**

Some requirements are functional requirements and some are non-functional requirements. The chosen architecture or structure of the design relates to both the functional and the non-functional requirements. Security as not being one of the main functionalities of supply chains is identified as a non-functional requirement that are part of what is called Design to X-ability (see figure 8) and determines amongst others the focus of the qualities that are planned to be incorporated in the system design, in this case being a security in the supply chain design.

**Figure 8: Design for X-abilities, adapted from [13]**

**Ad.13. Low vulnerability by right partnerships**

Vulnerabilities within supply chains cause risk of common supply chain failures [14]. Vulnerability may result from many internal factors as well as external factors. Besides under catastrophic conditions normal every-day circumstances may also face severe failures, which might increase due to vulnerabilities within the supply networks these supply chains are part of. Vulnerabilities can be found on several levels:

- Infrastructure and Asset Level, called as hard-ware;
- Process and Value Stream, called as flow-ware;
- Inter-organizational Network Level, called as org-ware.

**Figure 9: Levels of Supply Chain (based [14])**

Designers should not only focus on securing the levels themselves but also the interfaces between these levels have to be secured.

Moreover instead of heavy investments in physical assets and infrastructures which lock-in companies’ options with high fixed cost, efforts towards building right partnerships is one of the effective solutions in dealing with building secure supply chains uncertainties and risks. However, once a firm has chosen its key customers and key suppliers, mainly based on its basic requirements, it is possible that this firm may easily overlook the vulnerabilities hidden in the partnership.

**Ad.15. Design for (low) risks**

Supply chain risk management (SCRM) is the “management of external risks and supply chain risks through a coordinated approach between the supply chain partners in order to reduce supply chain vulnerability as a whole” [15].

The field of SCRM is still very new and often the root causes of only disruptive events and forget all kind day to day uncertainties that occur in the supply chain. “Frequently, only disruptive events (such as bankruptcy, natural disaster or the
possibility of a terrorist attack) are included, whereas continuous changes due to a turbulent environment (e.g. change in customer tastes, technology shifts or supplier priorities) are ignored.” Trkman and McCormack [16] propose a conceptual model based on supply chain characteristics, its structure and a supplier’s attributes and performance, modified by factors in the supplier’s specific environment. Their model ties market, technology and environment turbulences as important influencing factor of the relations, (figure 10).

Figure 10. Conceptual model for managing supply chain network risk [16]

Ad.16. Designing secure supply chain interfaces

Whenever a system is decomposed into a number of subsystems a new set of interfaces is created. Interfaces might be temporal or continuous. In all situations for each (newly created) interface a set of interfaces requirements are necessary. Interface requirements will also include security related requirements.

Another aspect that relates to interfaces is the boundary of the system or subsystem that is under investigation. On the outside of the boundaries of this system are external interfaces. These external interfaces can go from several possible aggregation levels to an outside system also on several possible aggregation levels. What is on the inside of the system is also decomposed and has the same type of interfaces interrelations as can be identified have from inside the system to outside of the system.

The relationships within systems are more frequent and stronger than the relationships between the system and the environment of the system. Following this design rule will lead to more secure, robust and sustainable systems.

Above interfaces where discussed in a more general sense. Several types of interfaces can be distinguished, like:

- Technical interfaces;
- Technological interfaces;
- Organizational interfaces;
- Informational interfaces.

Depending on the type of interface several interface requirements that relate to security have to be taken into consideration during the design of the system.

Supply chain design framework

Beside an increased understanding of the concept security in respect to supply chain management another output (intermediate results in the overall research this work is part of) is a supply chain design framework was developed that contains basic information of concepts (briefly described in this paper) appropriate for addressing issues around supply chain security problems and opportunities.

For each concept that is addressed in this paper the following issues are elaborated on in the supply chain design framework [10]:

- A short explanation of the concept;
- Advisable design criteria;
- Common constraints;
- Requirement Interrelationship Issues;
- Successful examples;
- References.

Before the supply chain design framework can be further developed the current result has to be improved and evaluated. One important activity that is elaborated on in more detail is the plan to conduct enquiries with experience supply chain and logistics analysts to update it so it can be used as a guidance tool in the professional world.
Conclusions and recommendations

Supply chain security has many faces and often security is seen as an after the fact (design) effort. This paper identified a number of useful concepts that can be used as guides to design more robust, less vulnerable and more secure supply chains. The first step towards a framework that can guide supply chain designers has been made. Now this framework should be expanded, and evaluated in practice.

References