Foreword

Modern supply chains are highly interconnected on a global scale. Products often traverse multiple countries and regions before reaching their final destination. This complexity increases the number of potential vulnerabilities and points of attack, making it essential to understand and address security threats. These security threats to supply chains pose significant challenges and can impact businesses, consumers, and the economy. Among the threats most mentioned, one finds theft and sabotage, both resulting in significant financial losses for businesses and disruptions in the supply chain. Smuggling undermines the legitimacy of supply chains, resulting in negative economic and social consequences. Tampering with products, contamination, or introducing counterfeit goods can pose severe risks to the health and well-being of consumers. Ensuring the security of the supply chain is vital for maintaining consumer trust and safety. Therefore, addressing supply chain security is critical to overcoming modern supply chains' evolving challenges and complexities. It helps organizations develop proactive strategies to safeguard their operations, protect consumers, comply with regulations, and maintain the trust of stakeholders in an increasingly interconnected and dynamic global environment.

Transportation plays a critical role in supply chain security as it is the crucial link in moving goods from suppliers to customers. Any security vulnerabilities within the transportation process will affect the entire supply chain. Compared to other areas of the supply chain, such as production and warehousing, transportation is the most vulnerable to supply chain threats due to more limited control options. In addition to the above-mentioned threats, transport must consider compliance with customs regulations and border security procedures when transport crosses international borders. Failure to comply with these regulations can result in delays, penalties, or the confiscation of goods. Strict adherence to customs procedures, proper documentation, and communication with customs authorities are essential to ensure goods' smooth and secure movement across borders.

The supply chain of parcel delivery is of specific relevance considering transportation security. The volume of parcels delivered in Germany has risen significantly over the last few years due to eCommerce and the demand for fast deliveries. This growth is also reflected in rising international parcel deliveries from outside the European Union. For these parcel mail services, security is especially relevant, as the law of postal secrecy restricts anyone, including postal service providers, from investigating the contents of postal consignments. On the other side, every European country has appointed a national universal postal service provider responsible for offering postal services under the universal service obligation, stating that every item that does not violate rules and regulations must be accepted for delivery. As more and more parcels need to be delivered by postal service providers, ensuring the supply chain's security is a great challenge for them. Looking at the research done in this domain until today, one finds very few works considering supply chain security from an overall viewpoint, missing a methodological approach to consider supply chain security in the architecture of a logistics service provider from a strategic down to an operational level. This is especially true for postal service providers specializing in parcel mail deliveries.

Mr. Middelhoff addressed this research gap by developing a comprehensive security methodology for parcel services that guides the design and evaluation of security measures for physical transportation. Methodologically he approaches this research gap through the conceptual lens of Enterprise Architecture Management as a well-known approach in Information Systems.

To achieve this security methodology, Mr. Middelhoff developed three artefacts that represent a valuable contribution to the problem domain.

The first artefact, the Secure-by-Design Architecture Development Method, is a significant step in integrating security considerations within an enterprise architecture. This method is a specialized iterative procedure guiding the specification, design, evaluation, and implementation of an enterprise security architecture based on the well-known Open Group Architecture Framework TOGAF®, ensuring a broad base of understanding. Furthermore, the Secure-by-Design Architecture Development Method is independent of the domain of supply chains and thus applicable to any security considerations of an enterprise.

The second artefact addresses how security measures handling physical transport goods in parcel mail services can be modelled in business processes. For this, Mr. Middelhoff extended the broadly used Business Process Modelling Notation (BPMN) with security-relevant process elements. This modelling language makes it possible to de-scribe the security context in the parcel service's processes.

The final artefact combines the two artefacts mentioned before. With the security analysis and compliance assessment, security requirements stemming from the enterprise security architecture in the business processes can be analyzed regarding their compliance with security and business objectives.

The results of Mr. Middelhoff's dissertation are undoubtedly a relevant contribution to research and, at the same time, of great interest to practitioners. I can only warmly recommend to both groups reading his work.

Prof. Dr.-Ing. Bernd Hellingrath

1 Introduction

1.1 Motivation and Problem Statement

Theft, smuggling and sabotage are the primal categories of threats to security in supply chains (Closs and McGarrell 2004, p. 7; Hintsa 2010, p. 108). Handling these threats is part of supply chain security management (SCSM), which Closs and McGarrell define as the "application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain" (Closs and McGarrell 2004, p. 8). Damage and terrorism can be subsumed by the broader category of sabotage (Hintsa et al. 2010, p. 20). SCSM therein deals with various means of protection for all kinds of supply chain assets. To address this complexity, members of a supply chain need to identify major risk elements, sources of uncertainties, the activities affected and, from that, the stakeholders who own and share risks (Cagno et al. 2007, p. 3).

Besides this internal perspective, Williams et al. differentiate three classes of external security drivers in supply chains, which are *coercive*, *normative*, and *mimetic* pressure (Williams et al. 2009, p. 610). *Coercive* pressure can be formal in the sense of regulations or laws of governments and authorities but also informal, for example, through policies enforced by customers. *Normative* pressure is a more abstract expectation formed by values and norms in the environment of the supply chain and society. *Mimetic* pressure is formed on the market to compete and to create similarities with other organizations (Williams et al. 2009, pp. 598 f.). This view has not changed as a global supply chain risk report identified that only less than half of the organisations[1] "feel the root causes of supply chain risks are within their control" (WTW 2023, p. 4), but 71% say they have some influence via their risk management. Following the definition of SCSM with the internal and external influences, it is evident that supply chain security has no definite bounds in supply chain management but is achieved in coordination with other areas and in consideration of the environment.

Testing all security aspects in the whole supply chain is not achievable, which is mainly due to security preventing incidents, which then cannot be observed any longer, and the inability to prevent every possible incident, leading to unknown and hence unmeasured risks (Pfleeger and Cunningham 2010, p. 46). Attending to supply chain security is therefore driven by a better awareness of the environment and increased preparedness for risks, which is also referred to as visibility or transparency (Closs and McGarrell 2004, p. 13; Hintsa and Hameri 2009, p. 34; Sarathy 2006, p. 44). Due to the strong interdependencies between security and other supply chain operations,

[1] 800 responses from companies with over $250 million annual revenue in supply chain industry (WTW 2023).

investing in SCSM can create additional benefits for the supply chain. These so-called collateral benefits, first of all, can lower the total supply chain costs through greater visibility and more accurate shipment data (Peleg-Gillai et al. 2006, p. 29), which in turn can lead to lower safety stocks and reduced lead times (Sarathy 2006, pp. 43 f.). Countering the mimetic pressure, Sarathy further states that this can lead to additional market benefits and increased customer satisfaction.

Various supply chain security investments have the potential to create collateral benefits, like higher employee loyalty through a secure working environment and fewer safety incidents through controlled operations, to only name a few (Rice and Spayd 2005, pp. 9–17). Yet, Rice and Spayd highlight that there is no direct link between security investment and its collateral benefits (2005, p. 18) and that "security investments by their nature do not directly increase revenues but are intended to prevent costs" (2005, p. 7). Martens et al. studied the perception of firms on their security performance and identified contrary to expectations that "firms with more advanced measurement processes or methods may have a deeper understanding of their security issues, and, therefore, perceive their security as less effective" (Martens et al. 2011, p. 163). They conclude that measuring security may help firms identify supply chain vulnerabilities, yet they also realize that they are making less progress than desired (Martens et al. 2011, p. 163).

With the difficulty of measuring security on a supply chain scale and the various collateral yet only vaguely attributable benefits, evaluating supply chain security is challenging. Security threats cannot be seen as independent, as theft, for example, can cause sabotage, leaving statistical quantifications of threats mostly as a conjecture (Hoffer 2010, p. 10). Law enforcement data on security incidents are not public and is in itself limited to identified cases leaving out dark figures, while organizations at the same time keep this data secret due to competition (Hoffer 2010, pp. 10 f.; Rice and Spayd 2005, p. 7). These difficulties lead to the 'principle of maximum complacency', stating that organizations invest only as much into security to satisfy external bodies but neglect their own interests (Anderson 2020, pp. 1032 f.). External bodies create the coercive, normative and mimic pressures described above (cf. Williams et al. 2009; Anderson 2020, p. 1033), which are experienced by an organization and drive security investments. In the absence of a direct link from security investments to collateral benefits, the own interests of organizations in security are not valued as much. Larger organizations tend to push off the responsibility for security risks to service providers, like transportation, who, in turn, are incapable of recognizing dependencies in the supply chain (Hoffer 2010, p. 49). If security investments can be linked to supply chain performance and thereby evaluating the collateral benefits, the likelihood of maintaining and dedicating resources to security rises greatly (Williams et al. 2008, p. 268). This dependency is also mentioned by Closs and McGarrell, who state that "firms must implement continuous improvement processes that enhance both supply chain execution and security" (Closs and McGarrell 2004, pp. 7 f.).

Cagno et al. state that this combined design requires a methodological approach that can handle security risks along with regular business risks. As this changes over time, the supply chain needs to consider the overall system life cycle and differentiate between conceptualization and execution of the affected parts in the organisation (Cagno et al. 2007, p. 3). Potential guidelines to increase supply chain security can come from governmental initiatives, management strategies, operative routines and technical systems (Urciuoli 2010, p. 7). The limitation of supply chain security programs is that they are neither self-explaining nor self-executing, leaving it open to the individual organization how to implement requirements and how to pursue collateral benefits (Ahokas et al. 2010, pp. 6 f.). The most effective and efficient security is reached by considering it in the early phases of a system design and developing it continuously in line with other components, which became known as "security-by-design" (Cavoukian and Dixon 2013, pp. 7–9; Bygrave 2022, pp. 126 f.).

Lee and Whang compare the benefits of cost reduction through supply chain security to lessons learned from total quality management. They conclude on the following statements: (1) product screening at the end of processing is expensive and subject to error, (2) in-process control is preferable to assure that deviations from the norm are detected as early as possible, (3) awareness of potential threats is important for all employees and proper training is required, (4) prevention is the preferred strategy, which requires that response and recovery processes are in place, (5) and security, like quality, should be part of the design of products and processes (Lee and Whang 2005, pp. 291 f.). These lessons learned emphasize the need for a secure-by-design approach because control and recovery processes, as well as awareness and training, require an alignment with business operations. Ahokas et al. summarize this as "a need for a model, which supports strategic and operational design and planning and confines operational, quality management and crime prevention theories under same conceptual model" (Ahokas et al. 2010, p. 8). Operational design is not to be confused with operative planning in supply chain management. Instead, it refers to the strategic design of business functions. Strategic and operational design thereby means the long-term design of every day operations (cf. Ahokas et al. 2010, p. 2; Lee and Whang 2005). Current publications in supply chain security still refer to the literature mentioned above, continuously discussing identified research gaps (cf. Lu et al. 2019; Zomer 2019; Urciuoli and Hintsa 2017). The need for more advanced methods that integrate security into the design of supply chain operations has not been answered yet.

While all organizations, as members of a supply chain, are responsible for the provision of security, a special role lies with the shippers of physical transport goods, who need to have security policies, procedures, contracts, proper visibility and audit compliance (Burges 2013, p. 11). Transportation experiences an increased vulnerability due to reduced control capabilities as many supply chain security programs target the protection of facilities and stationary assets, making transit the weakest link in supply chain security (Closs and McGarrell 2004, p. 12).

Parcel mail services present a challenging case among logistic service providers. They experience an increasing trend of international parcel deliveries within and into the European Union (UPU 2022, p. 462; Statista 2022). After a small dip in the corona years, also national parcel deliveries in Europe are increasing again (UPU 2022, p. 455). This includes private correspondence and commercial freight. For Deutsche Post AG, the business sectors global freight forwarding and postal and parcel services form nearly half of the business (47,1%), besides express deliveries (29%) and supply chain and eCommerce (Deutsche Post AG 2022, p. 14). Postal services have some additional challenges that influence security considerations. The most prominent is postal secrecy, which restricts anyone, including postal service providers, from investigating the contents of postal consignments (cf. Federal Republic of Germany 2022, p. 18). Every European state has appointed a national universal postal service provider, who is responsible for the provision of postal services under the universal service obligation, stating that every item that does not violate rules and regulations has to be accepted for delivery (van der Lijn et al. 2005, p. 45). Under postal secrecy, this means that postal service providers have limited capabilities to protect themselves and recipients from potentially dangerous goods contained in the shipments. Considering the huge amounts of deliveries, adversaries can, so to say, “hide in the masses”. In achieving security, the postal sector aims for two managerial directions, which are (1) finding the most cost-effective way of meeting regulations and (2) mitigating security risks to contribute to business goals (Männistö and Finger 2013, p. 2320). This aligns with the theory of external pressures and the aligned security and business development.

The challenge of security operations in the postal sector has been investigated in the international research project INPOSEC in collaboration with two of the largest European postal operators, technology providers and research institutes[2]. Industry partners in the project affirmed the need for a conceptual model for strategic and operational security design, and first prototype developments could confirm the supportive value of such a model. Yet, the project was not designed to develop a general methodology. Multiple follow-up workshops among research and industry experts, together with several European postal service providers under the lead of PostEurop, a European public postal service trade association, emphasized the lack of security design methodologies to consider security in the operational business from a strategic perspective.

Based on these challenges, this thesis aims to investigate possibilities for a methodology that supports the strategic and operational design of supply chain security in consideration of business objectives. As it was pointed out, this must be achieved already in the design phase of the supply chain operations to achieve effective and efficient security. The developments are discussed in the scope of parcel mail services as a prominent case for vulnerable supply chains. While supply chain security has been motivated as a diverse area of research and practice, also the term security itself is often

[2] Franco-German project INPOSEC (2012-2015) funded by BMBF (Germany) and ANR (France)

used ambiguously (cf. Zedner 2017; Anderson 2020). Before discussing the research objectives in more detail, the next section elaborates on the versatile perspectives on security in literature and its colloquial usage for a better understanding and distinction from other works in this research domain.

1.2 Versatile Perspectives on 'Security'

Security "is a slippery concept" (Zedner 2017, p. 400) and "a terribly overloaded word" (Anderson 2020, p. 16). It can mean many things, which requires a proper definition for using the term (Bygrave 2022, p. 155). First of all, the word 'security' itself originated from the old French 'securite' or Latin 'securitas', from 'securus', translated to 'free from care' in the sense of not having to give attention to something (Oxford University Press 2023). This already tells that security has something to do with the liberation of some regard.

The possible interpretations of security become clearer in contrast to safety. Hollnagel states that security problems are attributed to intentional events, whereas safety problems are stochastic or probabilistic by nature (Hollnagel 2021, p. 45). Similarly, according to Herrmann and Pridöhl, safety is concerned with natural disasters and facing human error, while security focuses on malicious acts of humans (Herrmann and Pridöhl 2020, p. 14). Both comparisons agree that security incidents are driven by intent and accordingly require a human to perform a malicious action. Safety incidents instead are caused by natural events or human error. Following this distinction, safety is concerned with primary effects, while security is mostly concerned with secondary effects (Hollnagel 2021, p. 46). That means the severity of an accident is mostly rated by the direct inflicted harm to individuals or assets. For security, the severity is valued not only by the direct damage but primarily by the losses following the incident. Valuing security is even more complicated because it "is not a zero-sum game. [...] There is no exact equivalence between the losses incurred by the asset owner and the gains of the attacker" (Haley et al. 2006b, p. 37). This can swing in both directions, with the attacker gaining more than the victim's loss and vice versa.

Bygrave highlights an issue in distinguishing security and safety in the limitation of many languages other than English. "German, for example, uses 'Sicherheit' for both concepts, Spanish uses 'seguridad', Norwegian 'sikkerhet' and Italian 'sicurezza'" (Bygrave 2022, p. 157). Using the same word in both contexts naturally hinders the appreciation of two different concerns, contributing to the often ambiguously used terminology. Security is further differentiated into the subjective condition of feeling secure and the objective condition as the state of being secure and neutralization of threats (Zedner 2017, p. 401). It is widely established that in the objective condition, security has two ambiguous interpretations. It is the activity to protect against potential harm and the absence of potential harm caused by malicious activities (Wolfers 1952, pp. 484 f.; Brooks 2010, p. 226; Zedner 2017, p. 401; Hollnagel 2021, p. 52). As the timeframe of the identified sources highlights, this has not changed over a long period of time and not in recent years. Security is generally concerned with entities or assets that someone places value upon (Ross et al. 2016, p. 2). It is therein not a standalone property or feature, as it often is a proxy for other interests or values “such as personal privacy, human safety, business profitability or state sovereignty” (Bygrave 2022, p. 155). This highlights that security and safety can be distinguished quite clearly, yet not separated. This thesis is primarily concerned with designing a system that can provide objective protection against malicious actions, which in turn contributes to a secure environment strengthening the subjective perception of security.

1.3 Research Objective

As pointed out in the problem statement, the objective of this thesis aims for a methodology that combines the strategic and operational design of supply chain security in consideration of business objectives in the design phases. While SCSM is a supply chain-wide concern, it builds on coordinated security measures within the scope of individual organizations. Every organization has its own objectives and experiences different external pressures creating individual collateral benefits of security, which requires that security measures are designed and evaluated in relation to these objectives and pressures on the organizational level. Nevertheless, interests among supply chain members have to be considered as external interests of each organization. A methodology following the security-by-design concept has the most potential to achieve efficient and effective supply chain security. The special role of transportation in supply chain security is driven by the handling of goods in transit (Burges 2013, p. 11; Closs and McGarrell 2004, p. 12), like in the context of parcel mail services, in which parcels, on the one side, need to be protected and, on the other side, impose potential threats to the supply chain. Special interest in parcel mail security therefore lies in the handling of physical transport goods. Information security concerns are equally important but less specific and more generalizable across industries. Security therein is achieved by providing evidence that the delivery operations achieve the security objectives and the service obligation with sufficient quality. From the above problem statement, the major research question for this thesis is stated as:

> **Major Research Question:** How can security measures handling physical transport goods in parcel mail services be designed and evaluated regarding their compliance with security and business objectives to be secure-by-design?

The strategic and operational design addresses human, organizational, operational, information and technological components, which are referred to as a *system.* The ISO/IEC/IEEE 15288:2023 standard defines a system as a combination of interacting elements organized to achieve one or more stated purposes. The systems security engineering published by the National Institute of Standards and Technology builds on this standard to give a multidisciplinary approach to designing secure systems (Ross et