2014

Security at the source: securing todays critical supply chain networks

Véronneau, Simon; Roy, Jacques

Springer Science and Business Media

Véronneau, Simon, and Jacques Roy. "Security at the source: securing todays critical supply chain networks." Journal of Transportation Security 7.4 (2014): 359-371. https://hdl.handle.net/10945/57008

J Transp Secur (2014) 7:359–371
DOI 10.1007/s12198-014-0149-z

Security at the source: securing today's critical supply chain networks

Simon Véronneau · Jacques Roy

Received: 22 August 2014 / Accepted: 24 September 2014 / Published online: 22 October 2014

Abstract This paper focuses on the re-engineering of supply chain security processes of an international organization with global operations. This research project is based on a multimethod field study designed to evaluate, over a 12 month period, the implementation of a new security concept downstream of the central warehouse. During a 12 month field study, it was found that after new processes were in place, the organization was able to achieve substantial benefits, including increased velocity, enhanced security, and lower security costs. This research introduces the new concept of security at the source, which defines security as a fundamental criterion of quality; it borrows from quality management theory to implement a new perspective on supply chain security; and it offers a new avenue for researchers to further study this concept as a cost-effective solution to secure supply chains. The results of this research outline new processes for industries requiring enhanced security in their shipments due to the vulnerability of high-profile targets, such as high risers and transport systems, to terrorist or criminal activity.

Keywords Robust supply chain · Secured supply chain · Security operations · Explosives detection · Value-added services

Introduction

At a time when organizations are asked to reassess their vulnerability, supply chains are under tight scrutiny. A new quality criterion for a supply chain is a level of security sufficient to preclude any organizational weakness. Some high-risk organizations are

S. Véronneau (✉)
Graduate School of Business and Public Policy, Naval Postgraduate School, 555 Dyer Road, IN-314, Monterey, CA 93943, USA
e-mail: sveronne@nps.edu

J. Roy
Department of Logistics & Operations Management, HEC Montréal, 3000, Chemin de la Côte-Ste-Catherine, Montréal, Québec, Canada H3T 2A7
e-mail: jacques.roy@hec.ca

now assiduously screening all shipments before they enter their premises. A quick stroll during morning delivery hours around business centers in Manhattan, or any other major city, offers a telling view of the new problem of security inspection at the final delivery point. Not surprisingly, these heightened logistical activities can prove very costly to a supply chain. While the necessity of such activities cannot be questioned for these high-risk organizations, the process to achieve secured shipments must be reviewed in order to avoid bottlenecks and inefficiencies. This research has explored the benefits of a new "security at the source" model, similar to the "quality at the source" philosophy, and includes an investigation of the benefits and challenges of secured physical distribution channels.

We have known for quite some time now that there are significant advantages to adopting a good quality-control policy (Shewhart 1931; Juran and Gryna 1951; Feigenbaum 1951; Deming 1982; Ishikawa and Ishikawa 1982) in terms of operations streamlining and accrued business due to a higher level of client satisfaction (Garvin 1984). Furthermore, some high-technology or high-reliability organizations require suppliers to adhere to an exacting level of quality because of the importance of zero failures of equipment and processes in their line of work. The relatively recent phenomenon of terrorism and the 9-11 event, which has impacted North America severely since 2001, has elevated security screening to the new "quality requirement" of our time. Today, many industries require not only that products meet manufacturing quality standards but also that they are not tampered with so as to have adverse effects on consumers. Whereas in days gone by, a malfunctioning toaster could be seen as posing a threat, today companies are concerned with such dangers as the presence of toxins or explosives that could release at their clients' site or on their own premises. Security requirements such as the above are a new component of the relationships between organizations and their customers (Giunipero and Eltantawy 2004). Therefore, preventing product tampering that would affect the consumer and the securing of the supply chain and its nodes across its entire span have become a dual paramount objective for today's secured networks. Despite the variable ease or difficulty with which some new threats can be detected and the inherent differences among industries that render some more vulnerable to particular threats than to others, in most cases organizations need to revise their supply chain integrity strategy. However few tools are available to achieve this end. One of the challenges to security measures implementation in transportation and supply chain is the perceived tradeoff between efficiency and security (Burns 2013). We purport that serious security screening can be implemented in supply chain without having a negative impact on velocity or efficiency

Hence this research project's goal is to increase supply chain security while improving security-screening procedures and efficiency. It answers the call for more detailed applied research (Williams et al. 2008) as well as research into cost-effective supply chain security strategies (Manuj and Mentzer 2008; Williams et al. 2009b). To achieve these ends, a global supply chain's security processes were re-examined, and subsequently a new model was developed. It was quickly found during empirical work that many challenges faced in the security screening of material were similar to previous challenges posed by quality management in manufacturing. Therefore, it is from the proven theory of quality at the source that

the new model of security at the source was developed by pushing security processes upstream. After the model was developed, it was initially tested on part of the supply chain; subsequently, the processes were entirely converted to take full advantage of the benefits. However, as noted by Williams et al. (2008), it is difficult to give very detailed information about supply chain security measures given the need for those measures to remain secure and confidential. As such description of the methodology and firm examined must remain limited and vague in order to ensure the integrity of the security processes in place.

This paper is divided in four main sections: The first reviews relevant literature and concepts; the second discusses methodology; the third describes the new security at the source processes and their resultant impact on the supply chain; and the final section presents the conclusions and implications of this research project.

Relevant literature and concepts

With global sourcing and the liberalization of markets, global supply chains are currently very common to many organizations, big or small. As supply chains become more global, it becomes essential for all members of the supply chain to help secure them to ensure overall population safety (Williams et al. 2009b). Managing these supply chains in real time has become increasingly important in order to meet customer requirements and face uncertainty. As a result, safety and security issues have grown in importance and complexity. Organizations must now move from a traditional risk-buffering mindset to a risk-mitigation and -management one through better information flow and communication within the supply chain (Giunipero and Reham Aly 2004).

These new demands have significantly changed the way supply chain and operations managers envision their role in securing such chains. As reported by Whipple et al. (2009), managers operating within global supply chains now perceive a greater security risk than domestic supply chain managers and see security as a "cost of doing business." Therefore, it is now important to focus on secured physical distribution not only to control pilferage and shrinkage, but to ensure that only the product in its original form reaches the clients. Organizations recognizing this new reality and responding to the need for greater security in their supply chain (Williams et al. 2009a) are finding it is essential to establish and foster close relations with suppliers and governmental agencies in order to ensure supply chain integrity and continuity (Sheffi 2001).

Two main threats face today's global supply chains: 1) contamination or corruption could yield unsafe products for consumers, and 2) malicious appropriation could turn a supply chain into a high-velocity supply route to disrupt operations at the company or in the regions where it operates. Mitigation of these two increasingly common threats requires the enhancement of new secured distribution channels and the installation of strict security screening. These measures, however, can cause bottlenecks in operations and skyrocket costs, outcomes that signal a need for cost-efficient solutions that will not severely disrupt current processes and operations. Further complicating the matter is that most companies' supply chains operate within certain geographical constraints, which limit the number of options available.

Fragility & robustness

Organizations have grown more fragile over the years. This can be partly attributed to the increasing geographic dispersion of value chains as they become ever more global. Further, lean systems, while lowering inventory and increasing efficiency, heighten the risk of disruption as a result of reduced slack in the system (Barry 2004). As organizations have become more fragile, their vulnerabilities, both internal and external, have multiplied (Svensson 2004), meaning they are more susceptible to failures and disasters. Furthermore, evaluating and managing vulnerability prove to be complicated exercises (Kalliopi 2005). According to Rice and Caniato (2003), failure can stem from Supply, Transportation, Freight Breaches, Facilities, Communications, and Human Resources. In line with Caniato's findings, Warren and Hutchinson (2000) found that supply chains are vulnerable to cyber attacks, especially those of firms involved in e-commerce.

In addition to failures, organizations need to plan responses to potential disasters, however improbable some may seem. While disasters have been studied in a variety of settings (see: Anthony 1990), the Council of Logistics Management (now Council of Supply Chain Management Professionals) has established a disaster classification profile (Helferich and Cook 2002), according to which disaster analysis should be done along four axes:1) the primary cause; 2) the agent responsible; 3) the magnitude of impact; and 4) the organization resources impact.

While the above profile will not identify the disruption experienced by a given company, it nevertheless offers a definition so as to better focus response. The identification of disruption type requires the organization to conduct conceptualization, analysis, and deliberation—or "brainstorming"—sessions with all employees, from the shop floor to top management; everyone must come together to identify potential internal and external disruptions. As suggested in Véronneau et al. (2013), a good start is to combine the failure mode and disaster classification profile into a failure causality structure that can then be used to identify an organization's specific weaknesses. Since a firm usually has a better control over its internal operations, it would be wise to start by tackling internal challenges and then to move outwards toward external concerns and suppliers.

This being said, it is important to note that, even though the easiest task for management might be to have a robust organization design inside the company, the failure mode and disruption type with the greatest potential impact and the highest risk of occurrence should be addressed first, a procedure analogous to resolving bottleneck areas first, as explained in Goldratt's theory of constraints (Goldratt et al. 1992). The importance of disruption analysis is illustrated by a hypothetical company that strictly focuses on a failure mode, opts for a flexibility strategy by splitting its supply requirements between two suppliers, and then risks that both suppliers are exposed to the same disruption type. Without a working disruption-type analysis, it is impossible to make such a decision in a manner sufficient to preclude further disruption.

Value added security services

The supply of value-added security services is bound by the same basic free market forces as are other more common services. As a case in point, since the events of September 11th 2001, the demand for K9 screening for explosives has seen exponential

growth. After conducting a threat analysis, many companies quickly determined that their supply chain could be their Achilles' heel. With demand being high and supply being short, the fees for K9 screening quickly rose. Williams et al. (2009b) estimate that the demand for security measures will continue to increase in the coming years as will their cost for organizations.

The increased demand for detection as well as its rising associated costs has made the market attractive for new competitors and the development of new technologies: While dogs take years to train, once an electronic sniffer is developed, it can be reproduced massively. This is not to suggest increased security demands have incited a market free-for-all. After the initial wave of securing supply chains with a blind eye to rising costs, we have now entered a phase characterized by scrutiny, in which managers question the high cost of K9 services. As noted by Manuj and Mentzer (2008), rising supply chain security costs have become an increasingly important managerial issue.

The market is now filled with new electronic detection technologies that are starting to curb the cost of detection services by meeting the growing demand. Unfortunately, while trained dogs and electronic sniffer technology compete in the same market, filling a common need, the procedures to be followed and their inherent constraints are quite different. Whether an organization decides on its own to up the security of its supply chain or its clients now require such a level of security, the challenges are the same: How can the organization curb these costs and stay competitive? How can we prevent a loss of velocity in our supply chains?

Methodology

Given the requirement to increase security and the lack of tools and concepts available to do so, this research was inductive in nature (see: Cooper and Schindler 2002). From the idea of security at the source, as described in "Relevant literature and concepts", a field study was conducted (Van Maanen 1988) to examine the strategic, tactical, and operational levels of a company's global supply chain security process. The supply chain under study is fairly standard with global and U.S. based suppliers as well as global and U.S. based downstream client with one distribution center where supplies are consolidated. The main aim is to improve operations efficiency and thereby reduce costs.

The research methodology focuses on a multi-method (Brewer and Hunter 1989) inductive field study (Van Maanen 1988), which not only affords a good triangulation of the data (Smith 1975) but also capitalizes on the advantages of all three data-gathering methods: semi-structured interviews (Rubin and Rubin 2005); participant observations (Angrosino 2008); and empirical data gathering for cost-benefit appraisal. Taken together, these deliver a fuller, multi-perspective view of the problem (Jick 1979).

Informal interviews (see: Kvale 2008) of users and employees in functions other than supply chain management were carried out randomly when specific information required complementary information from a specific function. In both cases a semi-structured interview method was used. Through an ethnographic lens (see: Van Maanen 1988) and from the position of participant-observer, key employees were shadowed for a few hours in order to observe and record their daily interactions and challenges. These

observations were essential in painting a clear picture of operational challenges and key processes.

Average times were collected for all the security processes, both for the traditional point inspection and the new consolidated inspection model. Inspection times were also collected for the two technologies used by the company. Finally, the research was conducted in North America; therefore, all specific issues related to local operational constraints and culture at other worldwide locations were examined only through the lens of the U.S.-based head office.

Secured SCM model

The security model formerly used by the company was to inspect at the doorstep of the various locations worldwide, which is the most common first reaction to the need for increased security. As a result, security equipment and personnel had to be deployed to respond to short bursts of deliveries on specific delivery days. The lack of supply chain density meant that efficient and fast-detection technologies would be prohibitively costly, so the current process remained lengthy and expensive.

Detection technologies

At many sites, two main categories of detection technologies are in use today. The first is the canine, or K9, detection team, which involves one handler and one to two dogs specifically trained to detect specific smells. The second is an electronic detection system that uses a small air sample taken through a swab to detect chemical components that match a database of known substances. The system requires a technician to use the so-called "sniffer" in conjunction with physical swabs of the product. Each technology is discussed more fully below.

While in a security, military or law enforcement role, dogs are trained to detect narcotics or explosives, other types of agencies take advantage of dog's acute sense of smell for other purposes. Dogs have been trained to detect prohibited food items for customs and even fire accelerants in fire investigations. The dogs detect substances in real time and process as fast as the handler can walk them through the task. The origin of their use goes back decades to the military's using dogs to detect explosives and other trained-on smells. Later, dogs became popular with police agencies for use in narcotics detection and missing person's recovery, as well as explosives detection. The police also typically train their dogs to perform other tasks, such as crowd control, which is not required by most organizations seeking a detection dog.

Electronic "sniffers," a more recent technology developed to analyze vapor or particle content, can be set to detect a wide range of substances. The downside to these sniffers is the time required for analysis. The latest of these currently requires 20 s for analysis plus sample collection time by personnel (see: Smith Detection 2009). While computing processing technology will continue to reduce the time required for analysis, the human collection process is inherently time consuming and can result in damage to, even destruction of, packaging material designed to insure safe handling and transport of the essential product. As the technology, especially micro technology, evolves, the time required for detection analysis by the devices, as well as their cost, will come

down. However, the detection still requires security personnel to take physical swabs of the various products to be analyzed, which accounts for the bulk of the cost in industrialized countries where security labor is expensive. Furthermore, collecting samples compromises the pallet's packaging, which can expose the pallet to outside elements and, in some cases, destroy it completely.

Comparison of technology usage

While dogs can quickly screen tons of merchandise, electronic sniffers used for cargo inspections require lengthy collection times, but relative task duration isn't all that separates the two technologies; dogs and their handlers present on-location logistical requirements far more involved than those of sniffer devices. Taking into consideration all these variables, we can draw the following conclusion: K9s are best used for large-quantity screening where economies of scale can be achieved. It is not cost efficient to have a dog screen one pallet of goods, nor is it to have an electronic sniffer screen half a dozen truckloads. Electronic sniffers are best used for ad hoc, small-quantity analysis and for random sampling for quality assurance of security processes. Figure 1 is a simple visual representation of best technology usage along two axes.

Standard SCM inspection

While no two supply chains are exactly the same, the following generic model provides a generalizable representation. Figure 2 represents a standard supply chain with inspection point at the end delivery point.

The issue to note in the previous diagram is that all inspections are carried out at the endpoint of the supply chain. This system is currently the norm, for the locus of responsibility to inspect the goods is deemed to be the endpoint, and therefore inspection at other locations is considered superfluous. Inspections at reception points prior to final delivery are a source of inefficiency that reduces supply chain velocity and creates a bottleneck. Moreover, for some locations the volume is too small to justify K9 inspection, but other, less quickly executed methods may cause further delays.

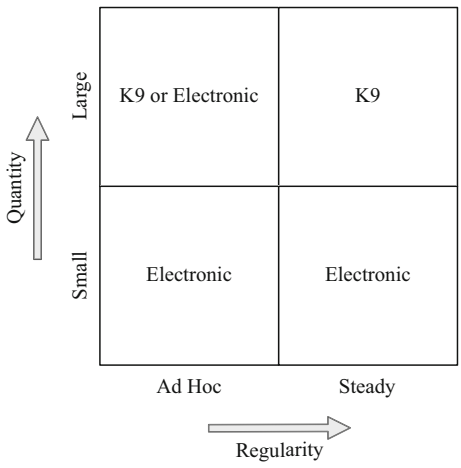

Fig. 1 Explosive detection technology usage matrix

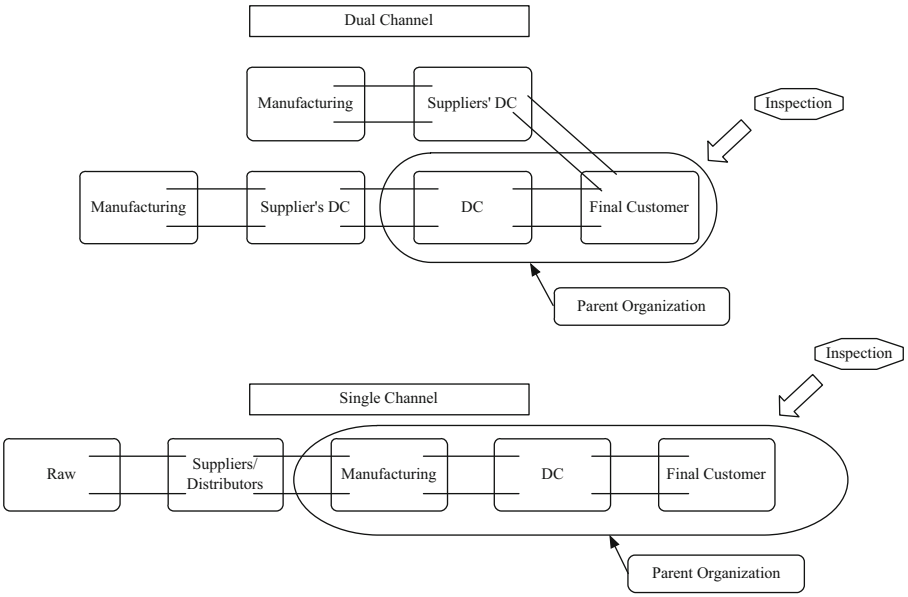

Fig. 2 Standard supply chain inspection

Quality at the source, security at the source

The "quality at the source" concept devised by Feigenbaum (1951) is frequently cited in the literature and associated with the Total Quality Management philosophy. Inspired by the quality-at-the-source movement, we suggest as a possible improvement rule for the current supply chain security process the idea of security at the source. In light of the research of Véronneau and Roy (2009), which finds that new technology implementation in supply chains requires high channel density, moving the security screening technology to higher nodes seemed natural. The idea is to secure the chain at a main consolidation point where goods are being palletized. From that point on, the security and integrity of the goods are to be maintained downstream until final delivery. This practice has the potential to reduce congestion at the delivery point, high security screening costs, and the likelihood of losing cargo en route while increasing the predictability of deliveries with remedial action taken ahead of time and upstream of consumption, thereby lessening the impact of disruption.

Overall the idea of security at the source is to reduce inefficiency by selecting the best means and sources for security inspections. Accordingly, when possible, inspections should be carried out where a significant volume and density can justify an efficient means, like a K9 inspection team. Significantly, large suppliers must now consider conducting security inspections themselves as a value-added service to their clients.

Pushing these security processes towards the source of the supply chain means that the security of the distribution channel must be maintained, a new challenge all its own, for which two options are possible: 1) simple low-tech options which can be viable for certain industries, or 2) more high-tech solutions to satisfy security needs. The following representation, in "Low-technology requirement model" and Fig. 3, delineates a relatively simple technology requirement security option.

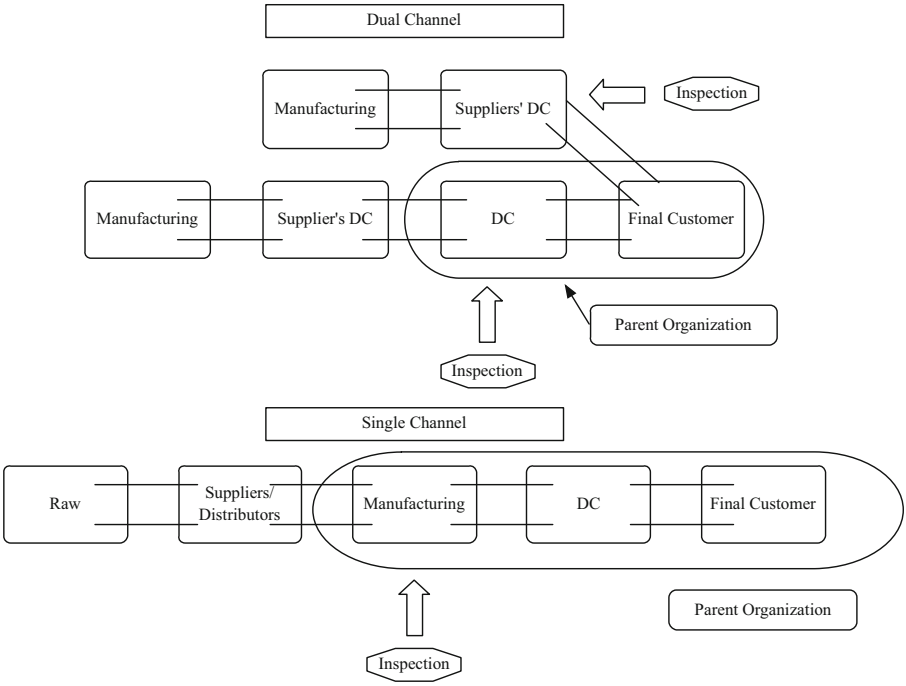

Fig. 3 Security at the source model

Low-technology requirement model

The low-technology requirement option depicted in Fig. 3 involve basic physical security features and physical seals. This model requires that a unique and tamper-proof seal must be affixed every time a trailer or container leaves the facility for transit. This seal's unique identification number is then transmitted directly from the person sealing the trailer or container to the person receiving the shipment. A secure means of transmission ensures that only the receiver knows the confirmation number. This rejoins the findings of (Kolluru and Meredith 2001) on the importance of securing information and communication channels to achieve supply chain security. In the event of a compromised seal, the shipment must be fully re-inspected. This approach further necessitates the application of a restricted decal authenticating a pallet was inspected for security. A main requirement of this concept is volume sufficient to justify large-scale inspection with dogs while cargo is sitting in warehouses in transit rather than adding a new time-consuming process at the doorstep.

High-technology requirement model

Building on the low-technology requirement model, the high-tech counterpart uses electronics to improve velocity and further guarantee system integrity. It also enhances the fluidity and invisibility of the security process, adding a layer of security to the specific knowledge of the security plan. The key element of this model is extensive use of technology such as RFID or barcode as virtual digital inspection tags. Another key

element is GPS real-time tracking, which not only enhances security but also can provide heightened visibility. Under this model, pallets are equipped with an RFID tag that can be read wirelessly by inspectors, and inspection information is updated automatically and wirelessly. Another, more conventional high-tech solution involves a barcode and barcode reader, which would yield similar virtual seal benefits but would require more manual labor. It is even feasible to have a dog wear an RFID reader that would automatically register and date stamp every piece of cargo inspected by him and store the information in the IT backbone. Some security information could also be stored in the tag to allow offline readings. While the cargo is in transit, the container must use a GPS tracking device to ensure that it remains within the intended route and experiences no unusual stops or detours. Finally, a digital sensor on the containers or trailers records the opening and closing of the door. When we couple all of these sensors and connect them to a central IT backbone, it is possible not only to gather detailed shipment information but also to set up security rules that would trigger alarms or red flags to be investigated, like an unscheduled stop with an unplanned door opening or an inspection voided for having not been completed within 24 h. Figure 4 illustrates the integration of such a system.

For organizations contemplating either of the two options, it should be noted that this high-technology model, while being the more fluid, can prove costly and, if deployed as a first step, present a steep implementation curve. However, our observation of the low-tech model suggests its implementation can be a significant task in itself and therefore points towards adopting an incremental approach in securing the supply chain.

In our study, the high-technology model was not used; the organization was not ready to implement some of the key elements of that system, e.g. RFID technology.

If a company elects to go with a high-technology model, it would be wise for it to keep a low-tech system as a back-up and a redundant layer of security. In such a case, even if the system becomes corrupted, it may be possible to avoid re-inspecting all of the items. However, having both systems will mean sacrificing some of the increased-velocity benefits of a purely wireless digital inspection system under the high-tech model.

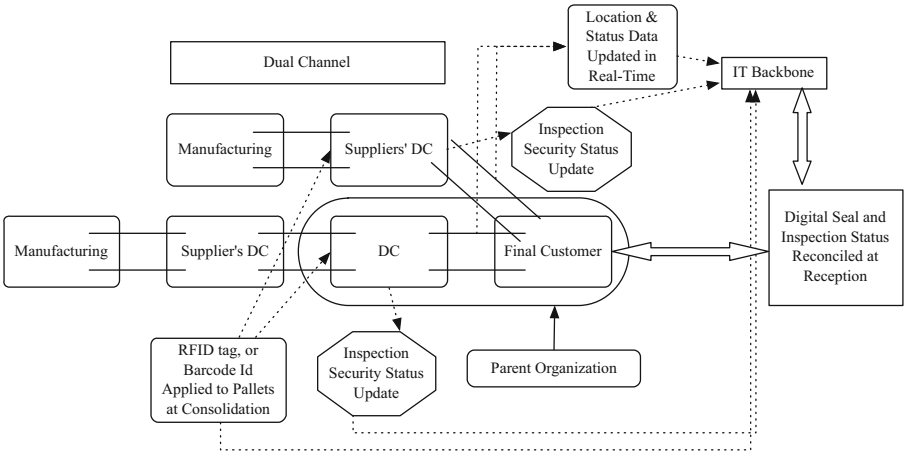

Fig. 4 High technology requirement model

Results of the low tech implementation

After some skepticism—colored with some "not in my backyard" attitude—from certain managers as to the benefit of pushing the security process upstream, the key managers in warehousing, transportation and security agreed on a test run at two sites. In line with Autry and Bobbitt (2008), we found that empowered and motivated employees in the organizations were critical in successfully implementing this new supply chain security initiative. Indeed, once everyone was onboard with the new process, the test run proved a success, reducing the receiving time at the site by 32 % on average while not affecting the warehouse's previous cross-docking operations processes. This gain in efficiency was achieved though only half of the products sent to the location had been pre-screened upstream. A full inspection of all the goods would further decrease reception time and generate savings by reducing the large labor force presently required at reception. Another substantial saving was achieved by relying less on the slower manual scanning and more on K9 teams. This gain in efficiency due to K9 technology upstream now yields substantial and continuous savings. Because the cost of both K9 and security labor varies greatly by regions, the specific savings must be evaluated in the SCM context in which the technology is applied. Nevertheless, the K9 team netted unquestionable and substantial savings in time and greatly alleviated the new security burden posed by the previous inspection techniques: the average time for security personnel to check a single pallet was 26.79 s; for a K9 team, the average time was 1.55 s per pallet. K9 teams are becoming more common as more dogs are trained every day and more firms enter this niche market, thereby reducing costs through availability and competition, whereas the labor rate for the security guards is likely only to rise. The greatest burden associated with security tests using the sniffer are that security guards must swipe numerous areas of the palletized shipment to try to get as much surface area as possible. This rather involved procedure suggests that, even with faster reading machines, the normal inspection time will remain fairly constant in the coming years, making unlikely any cost-saving gains in efficiency with such technology in the foreseeable future.

Conclusion & implications

This paper provides a new SCM-security model that can significantly improve efficiency and which is bound to evolve. Technologies to prevent theft, pilferage, or various forms of attack always have to evolve to remain ahead of ill-intentioned people, and different industries will have different needs, requiring the model to adapt to the specifics of their situations. Furthermore, this study represents only one company's process; of course, results might differ in other settings. Lastly, because the conditions for successful security at the source often require more rigor than some supply chains can handle, it is believed that this new concept will apply best to continental supply chains.

This model also suggests an opportunity for some warehouse providers to start offering value-added security services. Since some distributors or suppliers do not have the volume to justify these mass inspection technologies, private distribution centers could begin offering consolidation-point inspections, acting as a securing center for

enterprises. Another possibility is the outsourcing of the security function for companies not wishing to conduct their own security inspections. Though outsourcing would allow for potentially greater economies of density, it would translate to some loss of internal control for the organizations. Hence, the option to outsource to a security center would be more beneficial for organizations that do not have sufficient density to efficiently secure their own supply chain or do not possess the expertise to deploy such a model.

Given the security cost structure and the importance of density in achieving substantial savings, the security–at-the-source approach is deemed the best solution at this time and for the foreseeable future. Until technologies manage to outperform sniffer dogs, gaining the critical density to warrant use of K9 technology will be the most efficient approach for most organizations requiring a secure supply chain. Heightened security of supply is likely to remain important to, if not mandated by, governments. Organizations leading the way and adopting sound practices will therefore likely come out ahead of any new requirements.

While theft can be a serious problem in a number of supply chains it was not part of this study. The main concern for the organizations studied was that the supply chain could have been used as a way to deliver explosives to their locations. This concern remains today a serious issue for organizations in various industries. While addressing theft as part of an integrated holistic security system would be useful to many organizations, it was beyond the scope of this study.

Implications for academics

This paper proposed the new concept of security at the source as an emerging best practice for value-added security services. It will be interesting to test this new model in other companies and observe longitudinally where it will lead. A comprehensive survey of current high-risk industries could also be conducted to assess the current needs of these companies as well as their yearly security expenditures.

Implications for practitioners

This paper provides a framework for a secure supply chain along with tools and techniques that can help current managers make an informed decision about supply chain design. While no model will fit the particular needs of every company, the proposed model is general enough to meet various needs while being specific enough to provide a useful guide to best practice. For third-party logistics providers, this paper proposes a new range of security value-added services that companies are now seeking and ways to improve overall supply chain efficiency.

References

Angrosino M (2008) Doing Ethnographic and Observational Research. CA, Sage Publications, Thousand Oaks

Anthony O-S (1990) Post-disaster housing reconstruction and social inequality: a challenge to policy and practice. Disasters 14:7–19

Autry CW, Bobbitt LM (2008) Supply chain security orientation: conceptual development and a proposed framework. Int J Logist Manag 19:42–64
Barry J (2004) Supply chain risk in an uncertain global supply chain environment. Int Jof Phys Distrib Logist Manag 34:695–697
Brewer J, Hunter A (1989) Multimethod research: a synthesis of styles. CA, Sage Publications, Newburry Park
Burns MG (2013) Estimating the impact of maritime security: financial tradeoffs between security and efficiency. J Transp Secur 6:329–338
Cooper D, Schindler P (2002) Business Research Methods 8Ed. McGraw-Hill, New York
Deming WE (1982) Quality, productivity, and competitive position. Massachusetts Institute of Technology, Center for Advanced Engineering Study Cambridge, MA
Feigenbaum, A. V. 1951. *Quality control: Principles, practice and administration: An industrial management tool for improving product quality and design and for reducing operating costs and losses*, McGraw-Hill.
Garvin, D. A. 1984. What does product quality really mean. *Sloan management review,* 26.
Giunipero LC, Eltantawy RA (2004) Securing the upstream supply chain: a risk management approach. Int J Phys Distrib Logist Manag 34:698–713
Giunipero LC, Reham Aly E (2004) Securing the upstream supply chain: a risk management approach. Int J Phys Distrib Logist Manag 34:698–713
Goldratt EM, Cox J, Whitford D (1992) The goal: a process of ongoing improvement. North River Press, New York
Helferich, O. K. & Cook, R. L. 2002. Securing the Supply Chain. Oak Brook, IL: Council of Logistics Management (CLM).
Ishikawa K, Ishikawa K (1982) Guide to quality control. Asian Productivity Organization, Tokyo
Jick TD (1979) Mixing qualitative and quantitative methods: triangulation in action. Adm Sci Q 24:602–611
Juran J, Gryna P (1951) Juran's Quality Control Handbook. McGraw-Hill, Inc., New York City
Kalliopi S (2005) Coping with seismic vulnerability: small manufacturing firms in western athens. Disasters 29:195–212
Kolluru R, Meredith PH (2001) Security and trust management in supply chains. Inf Manag Comput Sec 9: 233–236
Kvale S (2008) Doing Interviews. CA, Sage Publications Ltd, Thousand Oaks
Manuj I, Mentzer JT (2008) Global supply chain risk management strategies. Int J Phys Distrib Logist Manag 38:192–223
Rice JB, Caniato F (2003) Building a secure and resilient supply network. Supply Chain Manag Rev 22–28
Rubin HJ, Rubin I (2005) Qualitative Interviewing: The Art of Hearing Data 2nd Ed. CA, Sage Publications, Thousand Oaks
Sheffi Y (2001) Supply chain management under the threat of international terrorism. Int J Logist Manag 12:1
Shewhart WA (1931) Economic control of quality of manufactured product. N Y 501
Smith HW (1975) Startegies of Social Rsearch: The Methodogical Imagination. Engelwoods Cliffs, NJ
Smith Detection. 2009. *Sabre 4000 Technical Information* [Online]. Available: http://www.smithsdetection.com/media/SABRE4000_VT_EN_95588355.pdf [Accessed August 25th 2009].
Svensson G (2004) Key areas, causes and contingency planning of corporate vulnerability in supply chains: A qualitative approach. Int J Phys Distrib Logist Manag 34:728–748
Van Maanen J (1988) Tales of the Field: On Writing Ethnography. Il, The University of Chicago Press, Chicago
Véronneau S, Roy J (2009) RFID benefits, costs, and possibilities: The economical analysis of RFID deployment in a cruise corporation global service supply chain. Int J Prod Econ 122:692–702
Véronneau S, Cimon Y, Roy J (2013) A model for improving organizational continuity. J Transp Secur 6:209–220
Warren M, Hutchinson W (2000) Cyber attacks against supply chain management systems: a short note. Int J Phys Distrib Logist Manag 30:710–716
Whipple JM, VOSS MD, CLOSS DJ (2009) Supply chain security practices in the food industry. Int J Phys Distrib Logist Manag 39:574–594
Williams Z, Lueg JE, Lemay SA (2008) Supply chain security: an overview and research agenda. Int J Logist Manag 19:254–281
Williams Z, Lueg JE, Taylor RD, Cook RL (2009a) Why all the changes? Int J Phys Distrib Logist Manag 39: 595–618
Williams Z, Ponder N, Autry CW (2009b) Supply chain security culture: measure development and validation. Int J Logist Manag 20:243–260