Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

> “*Business is all about risk taking and managing uncertainties and turbulence.*”
>
> Gautam Adani
> Business magnate

Risk management and resilience strategies in supply chains have an important role in ensuring business continuity and reliability in a cost-efficient manner. Preventing or recovering from disruptions requires access and analysis of large amounts of data. Yet, given the multiple stakeholders, operations, and environmental contexts in which a global supply chain operates, managing risks and resilience becomes a challenging task. For this reason, information and communication technologies (ICT) are being developed to support managers with tailored tools and services to monitor disruptions, enhance instantaneous communication, and facilitate the quick recovery of supply chains. Hence, the objective of this article is to shed light on managerial strategies to improve the resilience of supply chains and thereby to point out how these could be automated by means of innovative ICT systems. In particular, this article concludes by warning about existing challenges to implementing such systems. If these challenges are not correctly addressed by managers, there is a major risk of further jeopardizing supply chains.

Introduction

Recent catastrophic events, such as terrorist attacks, natural disasters, and pandemics, have drawn attention to the vulnerability of global supply chains to risks (Jüttner, 2005). Vulnerability means that supply chains are susceptible to disruptions, meaning interruptions in business operations that result in undesirable consequences such as delayed deliveries or lost sales (Svensson, 2002). For example, the earthquake that hit Taiwan in September 1999 had a severe impact on the personal computer industry worldwide – 10% of the world’s computer chips and 80% of the world’s motherboards were produced in Taiwan – resulting in lost revenues of more than 200 million dollars due to production shut-downs (McGillivray, 2000). Supply chain trends such as globalization, specialization, complexity, and lean processes have been largely indicated as the main drivers of these risks (Pfohl et al, 2010; WEF, 2012). Hence, in such a scenarios, supply chain managers are asked to improve their risk management skills in terms of identifying, analyzing, mitigating, and finally monitoring risks.

Supply chains are often described as sets of organizations joining a virtual network through which flows of services/products, information, and money are moved and exchanged. The common goal of these networks is to transform raw materials into components and products that are delivered to final consumers, at the right time, quantity, quality, and place. In these networks, strategies to manage risks and resilience have an important role in ensuring business continuity, delivery reliability, responsiveness, etc.

To ensure the optimal management of risks and resilience, managers of supply chains need to identify, access, and analyze large amounts of data through different information technology platforms and sources. In particular, specific ICT systems based on a combination of push and pull services are indicated as the most promising approaches to support risk management and resilience in a cost-effective manner. The principle behind these systems is very simple: such systems consists of web-services providing common and consistent access to data for all the different actors in the supply chain (e.g., suppliers, transport providers, manufacturers, distributors, importers, retailers) but also for governmental agencies worldwide (Williams et al., 2002). Yet, given their novelty, there is still much uncertainty about how these systems should be best integrated in companies.

Hence, the objective of this article is to provide a general overview of resilience strategies applied in supply chains and thereby shed light on how ICT systems can be exploited. By understanding and putting into practice these conceptual links, this article aims to contribute a visionary perspective of cyber-resilience in supply chains, illustrating how resilience in supply chains can be enhanced through the exploitation of innovative information technology services.

The article is structured in a manner to build up and lead to the cyber-resilience topic: after the introduction, it provides an overview of risk management and resilience strategies in supply chains. Next, it enumerates known challenges of these approaches, and thereafter it sheds light on the role of ICT in cyber-resilience. Finally, the article concludes by providing managerial implications and recommendations.

Risk Management and Resilience Strategies in Supply Chains

Besides risk management strategies, both researchers and practitioners point out that particular attention has to be given to strategies improving the resilience of supply chains, that is, the capability of supply chains to bounce back to stable conditions after a disruption. Resilience is important for two reasons: first of all, sooner or later, companies will have to face unexpected risks, for which no mitigation strategies have been planned in advance. Hence, the capabilities to respond to these events need to be built into the management of the companies. Second, the reactions of governmental agencies triggered after large catastrophes (e.g., terrorist attacks, earthquakes, hurricanes) may also give rise to unexpected events that supply chain companies need to deal with in order to ensure business continuity and survival (Sheffi, 2001).

Looking at the literature, diverse strategies to manage resilience have been enumerated. Some of those are:

- **Diversification of suppliers:** The access to a wider supply base enables firms to exploit additional production lines and quickly shift volumes and production in case of a disruption (Sheffi, 2006; Tang, 2006; Tomlin, 2006). In addition, companies may use flexible contract agreements, inspections to qualify suppliers, and make-and-buy strategies to split production across different factories (Sheffi, 2006).

- **Inventory management:** Safety stocks can be increased in order to avoid stock-outs in case of missed demand. Inventory redundancy may build additional capacity in firms, yet they are well known to generate additional costs as obsolescence, product lifecycles, and inventory holdings (Sheffi, 2006; Tang, 2006; Tomlin, 2006).

- **Ensure additional transport capacity and multiple consignment routes:** Plan in advance possibilities to transport cargo by means of multiple transportation modes, multiple carriers or providers, and consequently multiple routes and distribution channels (Tang, 2006; Tomlin, 2006). Additional transport capacity can also be ensured by investing in and maintaining a dedicated transportation fleet (Sheffi, 2006).

- **Product-centric design:** Aligning the design of the products with the supply chain efficiency targets. This process cannot happen in isolation, but it implies vertical cooperation and early involvement of suppliers in product concept development and design (Khan et al., 2012; Zsidisin et al., 2000). Multiple designs of products can become useful in emergency situations, for example, in case a specific raw material or component is unexpectedly not accessible (Sheffi, 2006).

- **Information sharing:** Information sharing may improve flexibility of supply chains or enable monitoring of risks and the establishment of preventive actions (Skipper & Hanna, 2009; Tomlin, 2006).

Challenges in Managing Risks and Resilience

Given the multiple stakeholders, operations, and environmental contexts in which a global supply chain operates, managing risks and resilience is a challenging task. These challenges are especially acute in the domain of cross-border trade, where the organizations in the virtual network need to be managed as single entities across national borders, and where several regulatory compliance frameworks exist. In practice, this means that supply chain companies need to deal with different cultures, geopolitical and organizational issues, regulatory compliance frameworks, and ultimately with different ICT systems, standards, and technologies operated by different actors and under different business logics (Urciuoli et al., 2013).

Cyber-Resilience: A Strategic Approach for Supply Chain Management

Luca Urciuoli

The latest R&D initiatives are putting their efforts on the development of ICT tools that may support companies with this complex process. These tools aim to enhance visibility of risks along the supply chain by enabling information collection through sensor technologies, sharing of data, and application of advanced business intelligence rules to analyze data; in particular, data are not being shared merely between the supply chain companies, but also between the supply chains and the governmental agencies. This practice is fundamental to reduce the administrative costs that cross-border supply chains entail (Urciuoli et al., 2013).

To give a sense of the burden experienced by companies, it can be reminded that, to import goods into a country, companies have to produce export and import declarations, with licenses and other permits to be attached, in order to demonstrate compliance with customs regulatory frameworks. In Europe alone, customs administrations are processing almost 200 million declarations every year; for example, in 2007, it was 183 million (IBM, 2008). Each of these declarations consists of roughly 40 typologies of documents and in total about 200 data elements need to be exchanged between business and governmental entities, resulting in highly complex and costly data transfer, processing, and storage challenges (ADB, 2005).

The Role of ICT: Towards Cyber-Resilient Supply Chains

Cyber-resilience may be achieved by smartly combining technologies and services that exist today on the marketplace or that are being developed in R&D projects. These are presented in this section as ICT systems for B2B (Business to Business) and B2G (Business to Government) information sharing and analysis.

B2B information sharing

Several IT companies are struggling to develop multiple data interfaces in order to guarantee full interoperability and access to data to supply chains stakeholders. Data is actually being shared between companies in a supply chain, however, often in paper and sometimes in electronic format. In particular, the usage of paper-based information exchange has been indicated as not effective, because of the risk for mistakes, data loss, as well as redundant transfer and collection of the same data. Hence, the usage of sophisticated electronic systems to collect, store in a common repository ecosystem, and analyze data has received a lot of attention because of the abundant cost savings that could be earned. For instance, in an international shipment, files of data containing bills of lading, invoices, packing lists, country of origin, cargo quantity and type, etc. need to be shared by supply chain companies in order to improve the prediction of estimated times of arrival (ETAs). According to ETA estimations, transportation and diverse resources can be optimally scheduled and allocated, market campaigns can be punctually started to strategically retain major market shares, etc. Likewise, customs declarations in import and export countries can be submitted simultaneously by different stakeholders (Urciuoli et al., 2011).

Nowadays, web-services based on service-oriented architectures (SOAs) seem to be widely exploited to ensure connectivity of the supply chain in a plug-and-play fashion. These services enable electronic data sharing, and with it may reduce the risk for mistakes or incomplete data. In addition, web-based push and pull services can be exploited to avoid data redundancy and speed up response procedures in case of unexpected disruptions:

- **B2B pull services:** Data may be pulled by a supply chain company in order to obtain the current status of a consignment/container or to interrogate the inventory levels of suppliers, distribution centres/wholesalers, retailers, transport infrastructure capacity, traffic conditions, etc.

- **B2B push services:** Push services are instead used to trigger alerts to companies whenever the status of inventory levels, demand, containers conditions. or position change in an unexpected manner. In other words, the service is able to sense whenever data outrange previously established upper and lower control limits (UCLs and LCLs). These data ranges can be determined by means of advanced business intelligence techniques.

The combination of the above push and pull services enables full visibility and control in the supply chain. By pulling key data, managers may monitor, in real time, inventory levels, shipping statuses, environmental conditions of cargo and containers, arrival time at specific nodes in the supply chain network, etc. This information improves decision making in terms of optimizing inventory levels, scheduling and planning transport assignments, allocating resources, designing networks, etc. On the contrary, push services are more suitable to handle risks and manage resilience. Hence, in case of deviations from planned routines, alerts may be triggered to recover or activate response procedures. Examples of push services could be alerts triggered by environmental sensors in containers, alarms installed in vehicles, panic buttons, geofences, timefences, etc.

B2G information sharing
Nowadays, to enable resilience strategies, supply chain companies work with different contract typologies and portfolios of suppliers located in various countries across the globe. However, despite contracts being in place, in case of a disruption, companies will suddenly need to deal with several different regulatory frameworks and customs procedures. Not only that, different countries require different data formats or usage of different information technology interfaces, implying higher costs in terms of translation and adaptation efforts needed to bridge between different national systems. Experts believe that future information technology systems will ensure that companies' systems can easily connect to customs administrations' web-platforms (i.e., e-Customs) and facilitate filing of customs declarations or provide easy access to international trade-related documentation (Urciuoli et al., 2013). In addition, push and pull services developed in prototype platforms may play a fundamental role in managing resilience:

- **B2G pull services:** Pull services connected to e-Customs platforms may be used to control existing trade regulations, necessary documentation for import/export procedures, status of release and clearance of containers, customs declarations, licenses, etc.

- **B2G push services:** Push services are instead planned to include alerts in case of changed trading regulations, tariffs or taxes, deviations of containers inspections and release, etc. These systems may eliminate unnecessary delays, reduce paper redundancy, and in this way, reduce costs to companies and governments.

Conclusion

ICT has already been indicated as playing a major role in controlling and managing more complex value networks in a cost-efficient manner. However, additional capabilities, mainly aiming to improve cyber-resilience, may be exploited to ensure quick response to risks and disruptions in supply chains. These capabilities are supported by the development of common repository IT ecosystems where B2B or B2G push and pull web services are created and contemporarily accessed by supply chain actors, but also governmental agencies.

Enabling B2B and B2G data sharing may allow companies to access an unimaginable amount of data and services that can enhance the cyber-resilience of the whole supply chain. For instance, companies will be able to easily manage and control portfolios of suppliers online, make more accurate ETA estimations, monitor in real time the transport infrastructure capacity, learn and apply any sudden changes in trading regulations, rapidly submit electronic orders and comply with regulatory frameworks, etc.

Despite the promising future visions, there is still much work to be done in order to ensure that these ICT systems will be fully accepted and integrated into supply chain companies. Many challenges are being encountered and need to be solved in order to move a step forward towards cyber-resilient supply chains. These are, in sequential order, the following:

1. **Exploit/develop reliable and robust information collection and sharing (both B2B and B2G).** Collection and sharing of information is still a major concern, especially for small companies, both in terms of technical development, know-how, and monetary investments.

2. **Exploit business intelligence rules.** Develop tailored push and pull web services that enable cyber-resilience. Yet, to develop reliable business intelligence rules, resources need to be allocated to identifying, modelling, and assessing risks in a systematic manner.

3. **Ensure public–private partnerships.** Partnerships should focus on the implementation of ICT systems to exchange data with public agencies and aim at developing up-to-date standards and legislative frameworks.

4. **Solve potential data confidentiality issues.** Sharing information implies that data will need to be held in repositories or remote locations. For obvious reason, this requirement is not accepted by many business companies that fear their business strategies will be disclosed to competitors.

5. **Ensure cybersecurity.** In several instances, it has been pointed out that, although the information technology layer of supply chains is relevant to optimizing supply chain management, it may also expose companies to criminal actions (e.g., theft, fraud, forgery, industrial espionage) or sabotage, hackers, and terrorists aiming to promote ideological issues and hurt the economy of a nation or a single industry (e.g., hacktivism, sabotage). Hence, this risk naturally implies that cyber-resilience strategies should be followed by information technology security management systems.

In conclusion, it is strongly believed that, without common data access, managers may struggle to fully develop, apply, and coordinate resilience operations in companies. Resilience becomes even more challenging in global supply chains, where managers need to deal with threats and recovery operations outside their companies and in different and multi-faceted environmental contexts. Current R&D initiatives are demonstrating that ICT systems for B2B and B2G data exchange, when combined with business intelligence techniques, may provide supply chain managers with advanced capabilities to improve resilience. Hence, supply chain companies could be only "a click away" from fully automated cyber-resilience.

Acknowledgements

The author of this paper would like to thank the CORE project (Consistently Optimised Resilient Secure Global Supply Chains, Grant Agreement No. 603993), a project funded under the European Union’s Seventh Framework Programme for research, technological development, and demonstration. This publication reflects the views only of the author, and the EU Commission cannot be held responsible for any use which may be made of the information contained therein.

About the Author

Luca Urciuoli is an Associate Research Professor in the MIT International Logistics Program within the Zaragoza Logistics Center in Spain, where he teaches and performs research in supply chain network design, supply chain risk, and security management. He holds an MSc degree in Industrial Engineering from Chalmers University of Technology in Gothenburg, Sweden, and a Doctorate in Transportation Security from the Engineering University of Lund, Sweden. He has been working at the research unit of the Volvo group as a project manager developing on-board transport and telematics services. He also led the research of the Cross-border Research Association in Switzerland and collaborated in several FP7 research and consultancy projects, with a focus on topics such as e-Customs, trade facilitation, supply chain security, waste security, and postal security. He is also an editorial board member for the *Journal of Transportation Security*, and he has published his research in several scientific and practitioner journals.

Contact: lurciuoli@zlc.edu.es

References

ADB. 2005. *ICT for Customs Modernization and Data Exchange.* Manila, Philippines: Asian Development Bank.

IBM. 2008. *Implementing e-Customs in Europe: An IBM Point of View.* Somers, NY: IBM Corporation.

Jüttner, U. 2005. Supply Chain Risk Management: Understanding the Business Requirements from a Practitioner Perspective. *International Journal of Logistics Management,* 16(1): 120–141. http://dx.doi.org/10.1108/09574090510617385

Khan, O., Christopher, M., & Creazza, A. 2012. Aligning Product Design with the Supply Chain: A Case Study. *Supply Chain Management*, 17(3): 323–336. http://dx.doi.org/10.1108/13598541211227144

McGillivray, G. 2000. Commercial Risk Under JIT. *Canadian Underwriter,* 67(1): 26–30.

Pfohl, H.-C., Köhler, H., & Thomas, D. 2010. State of the Art in Supply Chain Risk Management Research: Empirical and Conceptual Findings and a Roadmap for the Implementation in Practice. *Logistics Research,* 2(1): 33–44. http://dx.doi.org/10.1007/s12159-010-0023-8

Sheffi, Y. 2001. Supply Chain Management under the Threat of International Terrorism. *International Journal of Logistics Management*, 12(2): 1–11. http://dx.doi.org/10.1108/09574090110806262

Sheffi, Y. 2006. Resilience Reduces Risk. *Logistics Quarterly,* 12(4): 12–14.

Skipper, J. B., & Hanna, J. B. 2009. Minimizing Supply Chain Disruption Risk through Enhanced Flexibility. *International Journal of Physical Distribution and Logistics Management,* 39(5): 404–427. http://dx.doi.org/10.1108/09600030910973742

Svensson, G. 2002. A Conceptual Framework of Vulnerability in Firms' Inbound and Outbound Logistics Flows. *International Journal of Physical Distribution & Logistics Management,* 32(2): 110–134. http://dx.doi.org/10.1108/09600030210421723

Tang, C. S. 2006. Robust Strategies for Mitigating Supply Chain Disruptions. *International Journal of Logistics Research and Applications,* 9(1): 33–45. http://dx.doi.org/10.1080/13675560500405584

Tomlin, B. 2006. On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks. *Management Science,* 52(5): 639–657. http://dx.doi.org/10.1287/mnsc.1060.0515

Urciuoli, L., Hintsa, J., & Ahokas, J. 2013. Drivers and Barriers Affecting Usage of E-Customs — a Global Survey with Customs Administrations Using Multivariate Analysis Techniques. *Government Information Quarterly,* 30(4): 473–485. http://dx.doi.org/10.1016/j.giq.2013.06.001

Urciuoli, L., Zuidwijk, R., & van Oosterhout, M. 2011. Adoption and Effects Extended SICIS. In *Proceedings of the 2011 Hamburg International Conference of Logistics (HICL).*

WEF. 2012. *New Models for Addressing Supply Chain and Transport Risks.* Geneva, Switzerland: World Economic Forum.

Williams, L. R., Esper, T. L., & Ozment, J. 2002. The Electronic Supply Chain: Its Impact on the Current and Future Structure of Strategic Alliances, Partnerships and Logistics Leadership. *International Journal of Physical Distribution & Logistics Management,* 32(8): 703–719.
http://dx.doi.org/10.1108/09600030210444935

Zsidisin, G. A., Panelli, A., & Upton, R. 2000. Purchasing Organization Involvement in Risk Assessments, Contingency Plans and Risk Management: An Explorative Study. *Supply Chain Management,* 4(4): 187–197.
http://dx.doi.org/10.1108/13598540010347307

Citation: Urciuoli, L. 2015. Cyber-Resilience: A Strategic Approach for Supply Chain Management. *Technology Innovation Management Review*, 5(4): 13–18. http://timreview.ca/article/886

Keywords: IT, ICT, supply chain management, cross-border trade, cyber-resilience, risk management