The VESP Model: A Conceptual Model of Supply Chain Vulnerability

Arij Lahmar, University of Sfax, Sfax, Tunisia
Habib Chabchoub, University of Sfax, Sfax, Tunisia
François Galasso, Ecole de Mines Albi France, Toulouse, France
Jacques Lamothe, Ecole de Mines Albi France, Toulouse, France

ABSTRACT

During the last decade, researchers and practitioners became more interested in the domain of vulnerability analysis. It is considered as a key element in defining and managing supply chain risks. The great complexity of a global supply chain and of its environment, coupled with managerial trends, makes such a chain more vulnerable to disruptive events. A clear understanding of the possible consequences generated by this combination is a fundamental step to build an effective risk management plan and strategies. However, more studies are needed in order to develop the understanding of supply chain vulnerability. This article provides an explorative framework in order to analyze and quantify vulnerability within supply chains. Based on the existent literature, this article explores the factors that affect the level of Supply Chain Vulnerability (SCV). Four key components of SCV are identified (i.e. Exposure, Sensitivity, Susceptibility and Preparedness level). Based on these four categories of SCV, a conceptual model is developed. Such a model enables the definition of clear metrics and can further be used by researchers and practitioners to build consistent quantification methodologies.

KEYWORDS

Conceptual Model, Practices, Risk Management, Supply Chain Risk, Supply Chain Vulnerability, Supply Chains

1. INTRODUCTION

The increasing complexity of the supply chain networks and the strong interdependencies existing between logistics organizations taking place in different business field make supply chains vulnerable to potential disruptions and risks. Environment changes and turbulence, which affect supply chains all over the world, is one of the most important factors influencing the efficiency of the supply networks by increasing the exposure level to risks. As a result, there is an increasing consciousness of the vital importance of developing risk management approaches and strategies across all actors within supply chain networks. According to BCI survey (2015), 74% of managers stress the need to manage supply chain risks. According to the same report, organizations face today more than 24 sources of risks, with different levels of impacts and consequences. The most common consequences of these risks are the loss of productivity (58%), customer complaints (40%) and increased cost of working (39%), with annual cumulative losses of at least €1 million per year due to supply chain disruptions (BCI, 2015).

DOI: 10.4018/IJRCM.2018040103

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Unfortunately, not all risks could be prevented or managed. This is why companies are striving for more secure, resilient and less vulnerable supply chains and their strategies become more oriented risk strategies (Liu et al., 2014). The urgent need to protect supply chains and to make them less vulnerable to different types of disruptions has been highlighted from both researchers and practitioners, where there is a common consensus about the need to understand the causing factors of Supply Chain Vulnerability (SCV) and susceptibility to risks. A company needs to know the current level and drivers within a supply chain to be able to deal proactively with risks and to ensure supply chain resilience. The identification and the evaluation of potential supply chain vulnerability can help companies within supply chain networks to enhance and to justify the security and resilience requirements to be applied to protect and secure their activities and their business (Wagner and Neshat, 2012).

However, it is of critical importance, only a small number of frameworks have been devoted to analyze and to quantify the effects of vulnerability on both supply chain and risk severity (Wagner and Neshat, 2012) and to identify its key elements. In light of the increasing need to investigate and to understand this domain, this paper presents some discussions and research perspectives enforcing the understanding of supply chain vulnerability. The different terminologies and definitions related to supply chain vulnerability and explored then we will discuss the results of identification of elements, drivers and assessment options founded in the literature review. We will then conclude by presenting the conceptual model of supply chain vulnerability developed to answer the needs predefined in the previous step, illustrating the argument, the conceptual background, the methodology used and the applicability of the developed model.

Following this, the body of this article is organized as follows: Section 2 illustrates the research methodology used in this paper. Section 3 provides the background of the study, drawing a brief summary of literature about vulnerability definitions and drivers. The definition of the model is presented and discussed in section 4. Section 5 provides the application of this model to a case study and analyzes the results. Section 6 presents the conclusion, limitations and future research directions.

2. METHODOLOGY

Three methods are used to support this study: a literature review, conceptual modeling (Klag and Langley, 2013), and a case study research as a theory-building method. The literature review is performed in order to understand and to define supply chain vulnerability and also to identify its causing factors and drivers. A search for keywords, including supply chain and vulnerability, was undertaken through various electronic databases, including ScienceDirect, Emerald, Taylor and Francis, Wiley, IGI Global, Springer, INFORMS, Inderscience and other relevant bibliographic references to gather pertinent findings. Although this research may not be exhaustive, it is hoped that the selection process results, in terms of identified articles, give a comprehensive and significant overview of research works being accomplished in this field and will lend credibility to the argument advanced in this paper. In order to achieve this objective, a five steps process is then followed and depicted in Figure 1:

1. **Review related literature:** In order to find how scholars have addressed the supply chain vulnerability research and to identify the assumptions from which the author(s) addressed the problem;
2. **Identify concepts:** The first step was to define the research parameters or concepts and categorize them so that the themes and subthemes could be generated and understand easily;
3. **Define concepts:** This is the main function of a conceptual framework in descriptive study/research. It express clear definitions for constructs and mechanisms theorized to bring about the expected relationships between constructs;
4. **Concepts quantification:** This step aligns the set of concepts founded and the development of measurement scales or method of selected key elements. In other words, how can be measured the identified concepts;
Related Content

A Secure Hybrid Network Solution to Enhance the Resilience of the UK Government National Critical Infrastructure TETRA Deployment
[www.igi-global.com/article/secure-hybrid-network-solution-enhance/53012?camid=4v1a](www.igi-global.com/article/secure-hybrid-network-solution-enhance/53012?camid=4v1a)

Security and Privacy Issues, Solutions, and Tools for MCC
[www.igi-global.com/chapter/security-and-privacy-issues-solutions-and-tools-for-mcc/167221?camid=4v1a](www.igi-global.com/chapter/security-and-privacy-issues-solutions-and-tools-for-mcc/167221?camid=4v1a)
The Future of National and International Security on the Internet

Disaster Management in Digital Libraries: Issues and Strategies in Developing Countries