The VESP Model: A Conceptual Model of Supply Chain Vulnerability

Arij Lahmar, Habib Chabchoub, François Galasso, Jacques Lamothe

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 of 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).

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;

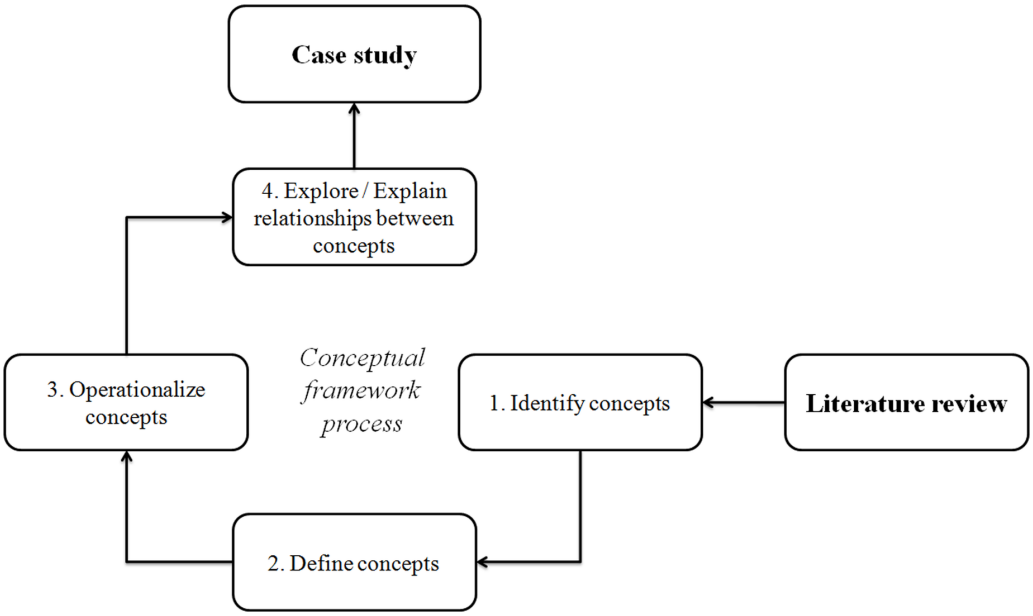
5. **Develop relational propositions between concepts:** State the relation between the final selected concepts. At this stage, different possible hypothesis are developed from these relations and are considered as the first basis of the conceptual model. This provides ideas for the test and the development of hypothesis. It provides an explanation for expected relationships by explaining why the posited mechanisms bringing about these relationships should be present;
6. **Develop the conceptual model:** By identifying and selecting the key words and the inter-relationships validated from the previous steps.

In order to test the applicability of this model and to contribute to an understanding of real-world phenomena theory building, a case study research is an essential research methodology. The research methodology is described in the Figure 1.

3. LITERATURE REVIEW ABOUT SCV

There is a growing body of scientific frameworks that has studied Supply Chain Risk, Risk Management practices, and decisions related to risks (Ho et al., 2015). However, according to literature (Nowakowski and Wojciechowska (2014), Jury and Matteo (2015), Peck, (2005), Wagner and Neshat (2012) and Thung and Hoeing (2011), Supply Chain Risk Management research cannot be investigated without understanding the vulnerability drivers. These drivers distinguish why certain companies face huge risk impacts and another more or less severe consequences (see for example, the Nokia and Ericsson) (Wagner and Bode, 2006). This is where hides the importance of vulnerability analysis, which has been presented as a condition in which a disruptive event could turn (or not) into a serious risk (Liu et al., 2014; Thung and Hoeing, 2011). As a result, the concept of vulnerability has been considered as a critical factor in the process of risk management within supply chain networks and a powerful analytical tool for describing states of exposure to disturbance and risk, and also for guiding analysis and investigations of actions in order to mitigate and manage risks (Jury and Matteo, 2015, Lahmar et al., 2015; Peck, 2006). As risk has been considered in the previous researches as the result of the exploitation of vulnerable assets within supply chain (Vlajic, 2009), investigating supply chain vulnerability and why and how supply chain are susceptible and exploited by unexpected disruptive events is becoming one of the fundamental pillar of any supply chain risk management approaches.

Figure 1. Research methodology



Referring to the literature, few frameworks have been developed as an essay to understand and investigate the concept of vulnerability (Briano et al., 2009). Thirty-two publications have been found that deal with the topic of Supply Chain Vulnerability. This scarcity of research publications could explain why Supply Chain Vulnerability meaning still ambiguous (Nowakowski and Wojciechowska, 2014). Figure 2 presents the number of Supply Chain Vulnerability publications over 13 scientific journals.

The following section will first investigate the definitions of supply chain vulnerability, in the light of the various definitions provided within the current literature. Subsequently, the research approaches undertaken in the area of supply chain vulnerability modeling, basing on the understanding of its causing factors or drivers, is discussed in more details.

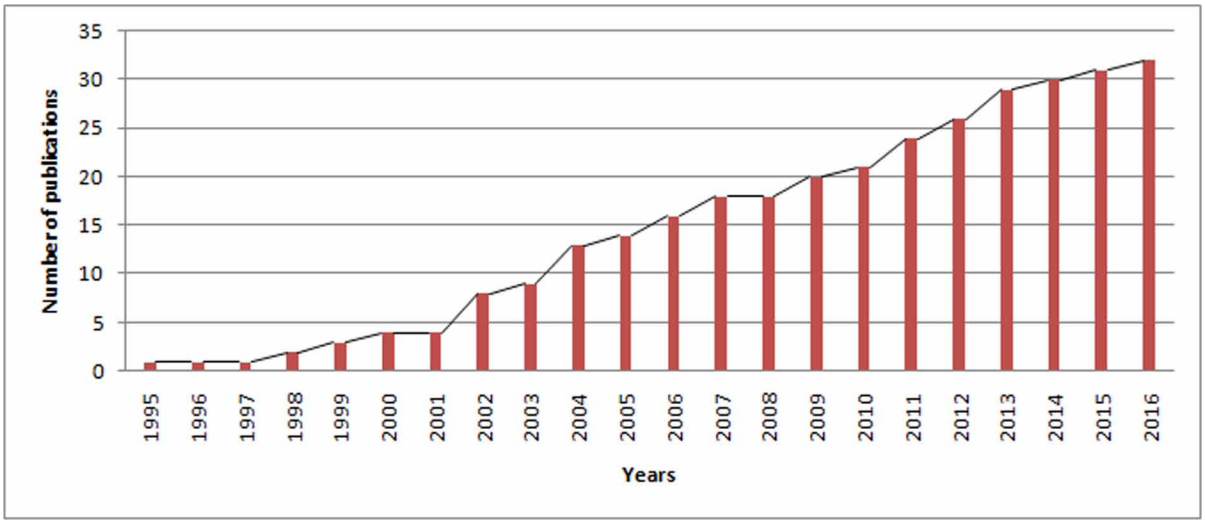
3.1. Definitions of Supply Chain Vulnerability

While the concept of vulnerability is frequently used within supply chain and risk management research, there is no common and well accepted definition among scholars. Researchers recognize the significance of vulnerability rely on the fact that it is considered as a source or a driver of risks, but the differing opinions of what this concept entails are clearly apparent in the numerous ways of defining this concepts, developed by both scholars and practitioners. One important definition is presented by Svensson (2000) in his research in which he defines this latter as:

…the existence of random disturbances that lead to deviation in the supply of components and materials from normal, expected or planned schedules or activities all of which cause negative effects or consequences for the involved manufacturing and its sub-contractors…

This definition has been used by several others researchers (for instance Norrman and Jansson, 2004; Christopher and Peck, 2004). However, Albino and Garavelli (1995) followed by Asbjornslett (1999) have dealt with the concept of vulnerability in the production system and JIT philosophies, defining the vulnerability as a "…sensitivity to external or internal events, caused by lack of robustness or resilience." According to these authors, the vulnerability could be seen "…as a set of system (i.e. supply chain) characteristics that could be used to evaluate the level of exposure to risks and the severity of its impacts by measuring the system sensitivity and ability to deal with disruptive events…" They stressed through their articles the two types of vulnerability: external and internal vulnerability. Following the same line of thoughts, Wagner and Bode (2006) suggests that the vulnerability is

Figure 2. Number of cumulative publications on supply chain vulnerability



inherent in the characteristics of the supply chain and could be defined as the susceptibility to risks. They defined supply chain vulnerability as:

…a function of certain supply chain characteristics and that the loss a firm incurs is a result of its supply chain vulnerability to a given supply chain disruption…

Basing on the results of their analysis, the authors confirm that vulnerability is considered as a supply chain characteristic that lead to risks (Craighead et al., 2007; Stecke and Kumar, 2009). However, the concept of SCV is not only limited to exposure to risks (Christopher and Peck, 2004; Peck, 2006) but includes also supply chain sensitivity or fragility, deviation to the expected performance and estimation of risk impacts. The literature reveals the fact that this latter can encompass various key-terms and features, which are linked to supply chain risks.

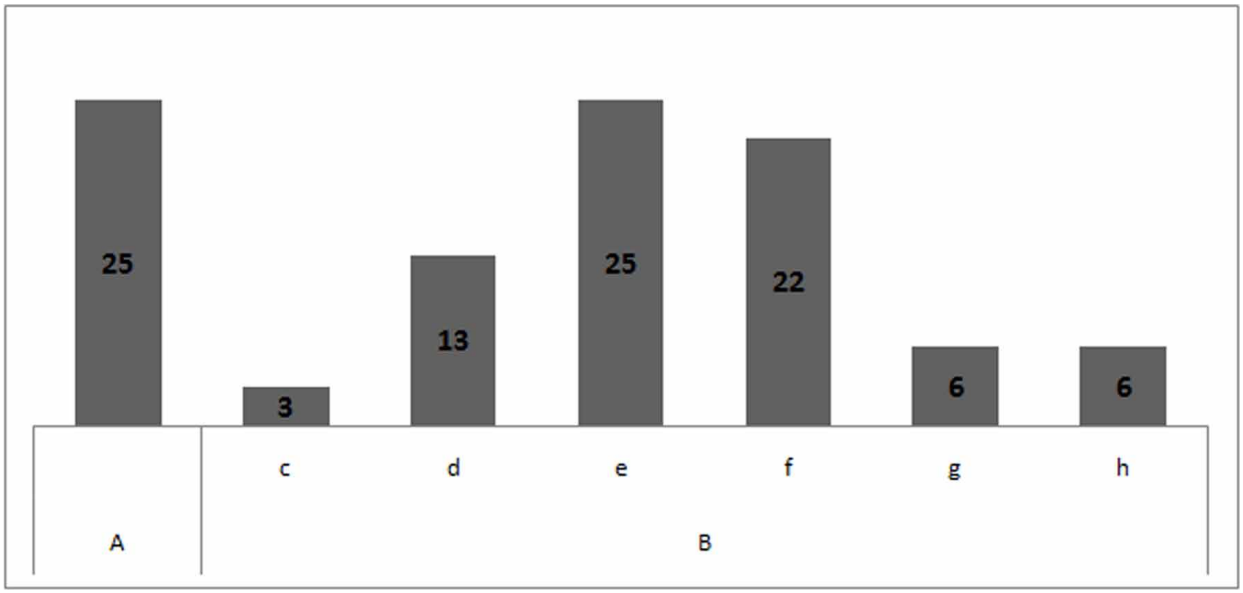
Peck (2005) defines supply chain vulnerability as an exposure to potential internal or external within supply chain. The level of exposure and sensitivity of supply chain to these risks is referred to as the vulnerability level. In the same line of thinking, Waters (2011) considers that vulnerability can be interpreted as the susceptibility of a supply chain to risks and their consequences it faces. Furthermore, "*…vulnerability highlights how prone a supply chain is to be affected by risky events…*" (Waters, 2011). In the same line of thinking, Juttner et al. (2003) define vulnerability as:

…he propensity of risk sources and risk drivers to outweigh risk mitigating strategies, thus causing adverse consequences and jeopardizing the supply chain's ability to effectively serve the end-customer market.

How sensitive a supply chain is to risks and disruptions is measured by its vulnerability, which in turn depends on its structural agility and resilience. This is where risk management plays a crucial role. So, the vulnerability is on one hand, a driver for the susceptibility, propensity or sensibility to risk and on the other hand a result of such kind of propensity.

Figure 3 shows the result of the paper analysis with respect to the definitions of supply chain vulnerability. 25% of papers analyzed, however, miss to define supply chain vulnerability, even

Figure 3. Analysis of supply chain vulnerability definitions. Articles (a) do not offer explicit definitions. Majority of reviewed articles (b) provide explicit definitions and identify vulnerability to be c) a failure, d) anexposure to risk, e) a susceptibility to risks, f) a disturbance, g) inability to resist or to cope, or h) sensitivity to variability.



though their emphases are put on this topic. Taking the above references into account, the different definitions and interpretations of SCV show that it is not clear what vulnerability stands for as a scientific concept and what makes it different regarding to the risk perception.

In Figure 3, the susceptibility to risk appears as the most concept linked to SCV. The concept of disturbance appears significantly and highlights the need for exterior elements from which a perspective about vulnerability can be adopted for its definition.

Among these varying opinions, three predominant interpretations of supply chain vulnerability which as illustrated in Figure 3, are: sensitivity, exposure and susceptibility to risks and can be used to distinguish risk and vulnerability concepts. Referring to the framework of Abjornslett (2008), the difference between vulnerability and risk is a matter of focus. Risk focuses on events (the initial disruptive event and its consequences), while the vulnerability focuses on the components of the affected supply chain. On the other hand, the advantage of vulnerability is that there are few types of components, while there are many potential disruptive events that could lead to risks occurrence. In other words, the difference between risk and vulnerability is expressed in terms of the exposure element and sensitivity factors.

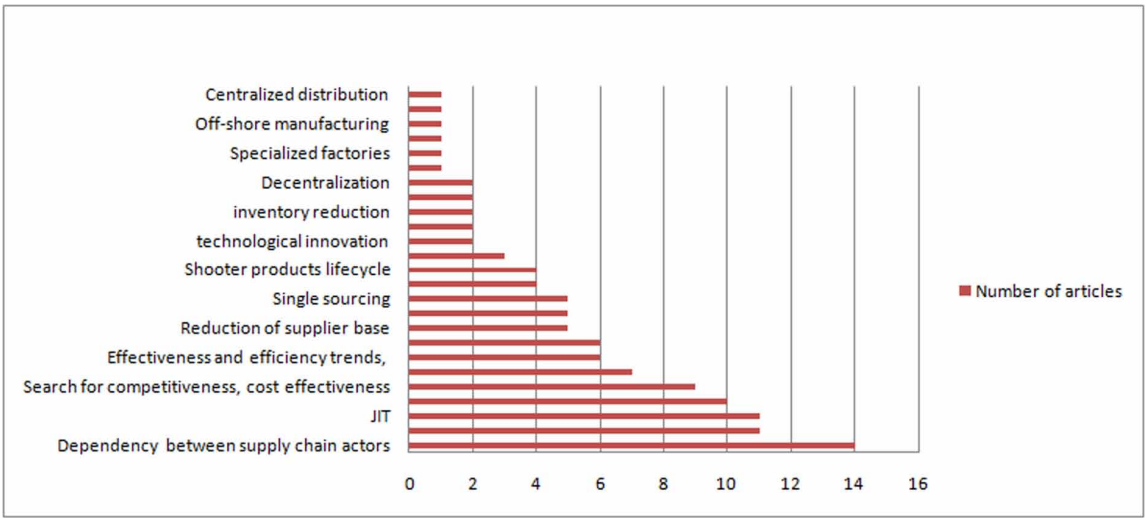
Another issue has been revealed in the literature which is the need to understand how supply chain vulnerability is generated, how it is increased and how it is build up. Researchers tried to provide an answer to this question using different multidimensional approaches. The section 3.2 gives insights into different factors linked to supply chain vulnerability.

3.2. Drivers of Supply Chain Vulnerability

Supply chain vulnerability drivers refer to the set of antecedents, sources, factors or causes that might drive, decrease or increase the level of vulnerability of the supply chain. Referring to literature review results (Peck, 2005; Wagner and Bode, 2006; Christopher and Peck, 2004) and reports surveys (Chartered Institute of Procurement & Supply, 2013), there is a common view among supply chain academics and practitioners over the past years: vulnerability of supply chains to risks or disruptions has increased apparently to be management practices and trends applied in order to increase the performance of supply chains (Fiskel et al., 2015). Managers face today a huge pressure to make their supply chains even more competitiveness and more efficient, and this pressure has resulted in developing a new business approaches and initiatives to achieve these objectives. Minimizing cost, increasing profit and satisfying customers have been always the top priorities of managers and the reasons behind creating new business methods. Although their valuable contributions to achieve business objectives, these new methods, often introduce unexpected events and unforeseen problems into a supply chain (Waters, 2011; Fiskel et al., 2015and Chowdhury et al., 2012). Furthermore, according to (Craighead et al., 2007), supply chain characteristics, such as node criticality or the design of supply chain play a major role in the variation of the vulnerability level. In the same line of research, Neureuther and Kenyon, (2009) and Pettit et al. (2010) have introduced the resilience level that could decrease the level of supply chain vulnerability while presenting different possible strategies in order to mitigate supply chain risks and therefore supply chain vulnerability. Later, Jury and Matteo (2015) and Gualandris and Kalchschmidt (2014) have tried to summarize all the previous researches developing a conceptual model called “a MISFIT model” in order to evaluate the level of vulnerability. However, this model is limited to the analysis of the downstream side of a supply chain and defines vulnerability as a type of risk, which appears to be restrictive compared to other visions described in section 3.1.

Considering the literature, the main variables and drivers leading to supply chain vulnerability cover so many aspects of a supply chain and can be described at a so specific level which require a generic point of view in order to classify these variables (see Figure 4). Three main types of factors are discussed in the following:

Figure 4. Supply chain vulnerability drivers



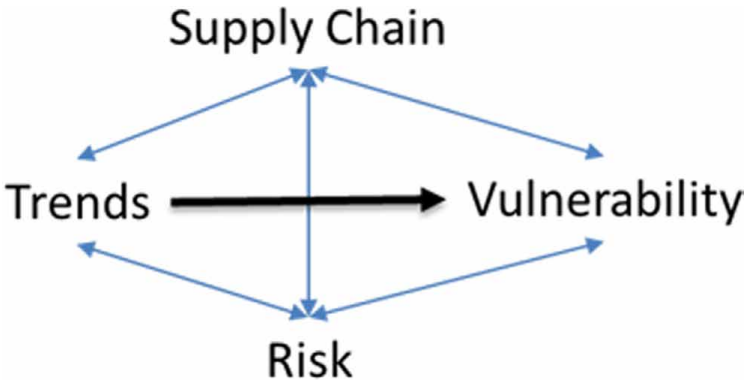
1. **The increase of business competition:** The pressure on supply chains to be both more efficient and more responsive has increased and this can be achieved only by applying news practices to reduce waste, costs and inventory and to be able to respond quickly to customers' demand. As a result, Lean strategies, JIT philosophies, reduction of suppliers' base, and responsiveness practices (Waters, 2011) are introduced. This results in more longer, faster and leaner supply chains with lower inventories, shorter lead times and product life cycles (Zsidisin et al., 2005);
2. **The interdependencies strategy:** One of the indirect effects of the competition in the supply chain environment is the increasing of the number of links and collaboration relationships. A supply chain is no more a simple chain of businesses with one-to-one relationships. This change in the number and type of relationships has created greater mutual dependencies and sensitivities and has contributed to the increase of the complexity of global supply chains (Craighead et al., 2007). Referring Normal Accident Theory (Skilton et al., 2009), the increase of the number of links and nodes within a system will result in multiple relationships and interactions which will create a more sensitive supply chain to a variety of internal and external disruptions that could occur at any node or link within the chain. And if these nodes and links are complex and tightly coupled, the propagation and the severity of any disruption will be increased and will affect faster the entire supply chain network;
3. **The trend of globalization:** Globalization made it easier to find diverse, qualified and cheaper sources overseas with both suppliers and customers in foreign markets. However, this has increased the time and distance factors of supply chain causing more fragile and exposed supply chain to risks due to a lack of visibility and control capacities of the supply chain as a whole.

Thus, these three categories emphasize the indirect influence on supply chain vulnerability of business objectives and orientations toward competitiveness and efficiency. However, their associated practices and managerial philosophies have an important effect on SCV. These three categories can be called" the vulnerability dimensions". Figure 5 summarizes this idea.

3.3. Methodological Approaches of SCV

In order to gain deeper understanding, several attempts have been made to model and minimize supply chain vulnerability through different modeling and analysis approaches. Two research orientations could be determined: the first deals with identifying and analyzing different causing factors of SCV and the second orientation investigates methods to measure the level of vulnerability within supply

Figure 5. Supply chain trends influence on supply chain vulnerability



chain (Wagner and Neshat, 2012; Gualandris and Kalchschmidt, 2014; Jury and Matteo, 2015). Figure 6 gives an overview of different research orientations and methodological approaches developed in the literature review.

From Figure 6, it can be seen that the majority of frameworks have dealt with the question of defining and determining the drivers or the causing factors of supply chain (78% of articles) and only 22% of the publications have treated the question of evaluation and measure of SCV (Wagner and Neshat, 2012). This could be justified by the fact that we cannot measure something unless we understand it and understand its factors. The ability to evaluate and measure supply chain vulnerability is increasingly being seen as a key factor for effective risk management process (Wagner and Bode, 2006; Wagner and Neshat, 2012 and Lahmar et al., 2015). We are still dealing with a paradox: we aim to measure vulnerability, yet we cannot define it precisely. is immediately apparent that a mixing of several measures and scales is taking place. However, these differ according to the number of metrics manipulated, the way of interpreting and defining the vulnerability and the measurement approach applied. Regarding the number of metrics used, the majority of researchers (66%) appear to use one dimension (output) to evaluate supply chain vulnerability (see Table 1).

Figure 6. Supply chain vulnerability research objective

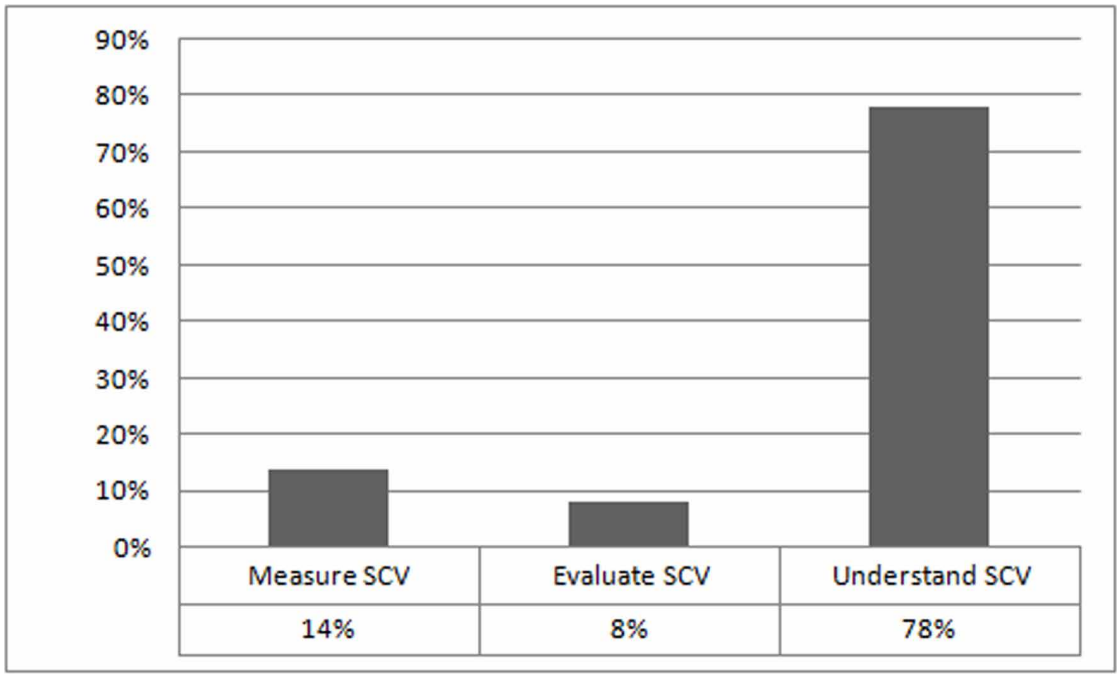


Table 1. Different measurement metrics of supply chain vulnerability

Ref.	Measures Metrics	Objective	Outputs	Inputs	Measurement and Evaluation Approach
24	Vulnerability= f(E, D)	Measure supply chain vulnerability	E= disruptive events, D= performance damage	Vulnerability level	Mathematical modelling
25	SCV = variation $(Pr)_t$	Measure supply chain vulnerability	Pr= performance, t=time	Vulnerability level	Mathematical modelling
38	Vulnerability = f(SCV_d)	Evaluate the level of supply chain vulnerability	SCV_d: Vulnerability drivers	Vulnerability level	Hypothesis tested through a survey
40	SCV = variation $(Pr_{criteria})_t$	Measure supply chain vulnerability	$Pr_{criteria}$: Performance criteria (quantity, quality lead time) t: time	Vulnerability level	Mathematical modelling
41	Vulnerability = f (SC characteristics, SCRM)	Evaluate the level of supply chain vulnerability	SC characteristics: node criticality, SC complexity, density. SCRM: supply chain mitigation strategies	Vulnerability level through evaluating SC characteristics and SCRM strategies	Hypothesis tested through a survey
43	Vulnerability = f (SCV drivers, SCRM practices)	Evaluate the level of supply chain vulnerability	SCV drivers SCRM practices	Vulnerability level through a balance between SC drivers and SCRM strategies	Hypothesis tested through a survey
45	Graph theory representing vulnerability as the interdependency between two nodes within Supply Chain	Evaluate the level of supply chain vulnerability	SCV drivers	Vulnerability level	Mathematical modelling
47	Likert scales, Vulnerability = f (SCV drivers, SCRM practices)	Evaluate the level of supply chain vulnerability	SCV drivers SCRM practices	Vulnerability level through evaluating SC characteristics and SCRM strategies	Hypothesis tested through a survey + Scale measurement
48	SCV = f(cost and time variation and it impacts on revenue)	Measure supply chain vulnerability	cost and time variation and it impacts on revenue	Vulnerability level	Mathematical modelling
49	SCV = variation $(Pr)_t$	Measure supply chain vulnerability	Pr= performance, t=time	Vulnerability level	Mathematical modelling
50	Vulnerability = f (SCV drivers, SCRM practices)	Evaluate the level of supply chain vulnerability	SCV drivers SCRM practices	Vulnerability level through evaluating SC characteristics and SCRM strategies	Hypothesis tested through a survey + Scale measurement
52	Likert scales: Vulnerability = SOMME(Vi)/ n Vi: drivers of supply chain	Evaluate the level of supply chain vulnerability	SCV drivers	Vulnerability level	Mathematical modelling
53	V = P* I,	Measure supply chain vulnerability	P: probability I: costs	Vulnerability level	Mathematical modelling

Table 1. Continued

Ref.	Measures Metrics	Objective	Outputs	Inputs	Measurement and Evaluation Approach
54	Vi = n (Vpi*Wj),	Measure supply chain vulnerability	VPI: vulnerability Wj: represents the weight of Vpi	Vulnerability level	Mathematical modelling
58	$MISFIT_i = \sqrt{\frac{D_i}{j-1}} = \sqrt{\frac{\sum_j^4 \left(W_j * \left(X_{ij} - \tilde{X}_i\right)\right)^2}{4}}$ Di is the weighted distance between the real adoption of SRM levers within organisation i and its risk profile; Wj, the weight of practice j; Xij, the standardised degree of adoption of lever j in organisation i; and ~X i, the risk profile score of organisation i, which is given by the weighted sum of its k risk conditions	Measure supply chain vulnerability	SCV drivers SCRM practices	Vulnerability level through evaluating SC characteristics and SCRM strategies	Mathematical modelling + survey

Thung and Hoeing (2011), Pettit et al. (2010), Liu and Zhuang, (2013) and Vlajic et al., (2013) evaluate the level of vulnerability (low, medium, high) by combining and assessing different determined by variables that drive supply chain vulnerability, so-called drivers of vulnerability (inputs). Other researchers refer to vulnerability as an indicator of negative change with respect to performance such as fluctuations in lead time, quantity, costs and customer service, etc. (Albino and Garavelli, 1995; Bogataj and Bogataj, 2007; Juttner and Maklan, 2011 and Vlajic et al., 2012). For example, Albino and Garavelli, (1995) computed a vulnerability index for production systems based on backorder frequency and increases in the mean transport and throughput time of an order. The authors, to quantify vulnerability, adopt a time perspective calculation related to production' system. Basing on their hypothesis, they measure vulnerability as a delay time occurred within delivery time. In the same line of thinking, Bogataj and Bogataj,(2007) use frequency space to measure supply chain exposure to risk. They use lead time as a measure metric. Quantity and quality are also integrated in the model. The variation of these variables are used to evaluate the exposure level to risks. The other 34% papers deal with vulnerability as a balance between causing factors (SCV drivers) and assessment options. This approach provides two metrics to evaluate and measure vulnerability and base on two sequential steps. The first step consists of determining and quantifying the drivers of vulnerability (SCV) characterizing a supply chain. The second step provides an evaluation of SCRM implemented practices. By comparing these two dimensions (SCV and SCRM), the vulnerability level was determined (Craighead et al., 2007; Stecke and Kumar, 2009; Thung and Hoeing, 2011; Wagner and Neshat, 2012 and Gualandris and Kalchschmit, 2015). Other point could be reveal when evaluating and measuring vulnerability which is the perception of vulnerability. Three perspectives are investigated: The first category measures and evaluates SCV as only a set or a combination of different drivers or causing factors. And it level depends only the type and the number of drivers involved in the combination process (Wagner and Bode, 2006; Stecke and Kumar, 2009; Wagner, 2009; Thung and Hoeing, 2011; Wagner and Neshat, 2012 and Pettit et al. 2010). The second research orientation define vulnerability as a disturbance or a factor that contribute to performance variation ((Albino and Garavelli, 1995; Bogataj and Bogataj, 2007; Vlajic et al., 2012; Liu and Zhuang, 2013 and Wagner et al., 2014). For the third theoretical orientation, vulnerability is evaluated basing on a set of supply chain characteristics such as node criticality, density, etc. And more of these characteristics have been considered high, the more the level of vulnerability will be higher (Craighead et al., 2007).

In order to achieve the objective, the researchers referred to some measurement approaches which are: mathematical modeling, scales development and survey techniques. These three methods are the

frequent methods used to measure and to evaluate supply chain vulnerability. (Wagner and Neshat, 2012 and Vlajic et al., 2013) combine survey and analytical methods to define and evaluate supply chain vulnerability by developing an analytical model called "a Misfit Model". This model underlines the relationship between two factors which are the context riskiness and the preparedness in supply risk management (Wagner and Neshat, 2012). Using deviation measures, and regression analysis relationship between misfit which is defined as the difference between a firm's preparedness and the riskiness situation of the firm. Other essays have been presented in literature review to give an answer to the measurement and evaluation issue. Albino and Garavelli, (1995) computed a vulnerability index for production systems based mathematical equations. In their framework, the vulnerability has been defined as the degree of supply chain sensitivity to changes in the context of JIT. Since unexpected events influence the behavior of the supply chain, the measures of vulnerability can be obtained by evaluating the performance. This latter could decrease by the occurrence of disruptive events. The authors, to quantify vulnerability, adopt the time perspective calculation related to production system. They identify vulnerability as the impact of time variability on system performance and they defined as an estimated delay occurred within delivery time. This delay is estimated in function of product mix and its delivery times, referred as a vulnerability index (IV). Wagner (2009) proposed a four-step algorithm using graph theory to calculate an estimation of vulnerability indices for various industries. Vulnerability can be measured or estimated directly as potential for harm or loss and its impacts on performance criteria. It is assessed by measuring the variability of key performance indicators However, this requires hypotheses of the potential impact of events that have not occurred but are likely to. This explain the use of hypotheses and survey to understand this theoretical purpose. Vulnerability can also be measured indirectly as a balance between SCV drivers and SCRM practices, translated into the failure to be robust or resilient in the face of a threatening event. The combination of mathematical model and surveys techniques was used to investigate this balance and then evaluate the vulnerability level through scales development (High, medium, low vulnerability).

3.4. Summary Notes

In this article a review of thirty-two scientific articles, covered a broad spectrum of this field was performed. Although this research is not exhaustive, the thirty-two selected papers constitute a significant and representative portion of scientific research carried out on Supply Chain Vulnerability. The analysis of these publications provides insights into the evolution, conceptualization, modeling and methodological foundations in the field of supply chain vulnerability. It serves as a comprehensive base for understanding the different scientific attempts and research issues developed. Although several authors attempt to broadly cover all of these general areas within their studies and researches, individually each area has received little systematic based study. As a result, a diverse theoretical base has developed. The term was first introduced by (Albino, 1998; Svensson, 2000). Their work has formed the foundation for most studies of the concept of supply chain vulnerability and a new introduction to the risk interpretations and assessment. The authors stress the fact that the severity of risk isn't only a function of risk profile but also the result of the level of vulnerability within the supply chain. They present a new way to apprehend and evaluate risk and also vulnerability by investigating and categorizing this concept. Since, combining the definitions of several authors, supply chain vulnerability has been defined as an exposure to serious disturbance arising from internal and external supply chain risks causing negative effects. Other researchers have noted that vulnerability describes supply chain characteristics that under the effects of an internal or external disruption and/or risk, can lead to a supply chain failure and then can increase the severity of risk. Other research issue has been investigated, which is the causing factors of supply chain vulnerability. An exposure or a type of risk, several researchers agree that certain supply chain management practices and trends are the drivers of supply chain vulnerability. Other consider that the environment conditions are behind the increasing level of exposure to risk. There is a third research perspective emphasizing that vulnerabilities are linked to certain characteristics of the supply chain design, such as its network structure, business

function and value, the degree of supply chain complexity, node criticality, etc. Some authors have gone beyond defining vulnerability and identifying its drivers and have proposed different essays to integrate these factors in a comprehensive way to measure and mitigate the vulnerability level within supply chain, offering a fourth research issue related to this domain: How to assess and mitigate supply chain vulnerability. Managing vulnerability has become more critical, but also more challenging as this concept is both multidisciplinary and multifaceted. The current body of literature with regard to supply chain vulnerability illustrate that many key elements have been revealed and analyzed. However, key issues related to this field (such as: the relationships among them, the links to supply chain trends, and the methodologies to manage) are poorly understood. Most of the reviewed researches have dealt with the key issues separately either by defining the vulnerability concept or by identifying their characteristics and components. But the causal link or relationship between the reviewed concepts is missing. The links between exposure and vulnerabilities are implicitly modeled in each of the reviewed approaches. However, among these frameworks describing the components and the constructs of SC vulnerability, only a few frameworks also have introduced the preparedness level to a supply chain regarding vulnerabilities. A second limitation is the scarce use of empirical evidence. Other research gaps have been identified and discussed in this article. Although the different frameworks dealing with supply chain vulnerability, scarcity of them have developed guidelines on how to develop indicators to assess vulnerability. Furthermore, it is evident that measuring vulnerability requires first and foremost a clear understanding and definition of the concept of vulnerability. The need for a holistic conceptual framework has been perceived. Many key elements have been revealed and analyzed. However, key issues related to this field (such as: the relationships among them, the links to supply chain trends, and the methodologies to manage) are poorly understood (Craighead et al., 2007; Gualandris and Kalchschmidt, 2014). Most of the reviewed researches have dealt with the key issues separately either by defining the vulnerability concept or by identifying their characteristics and components.

Aiming to address this gap, section 4 proposes a new conceptual model to identify Supply Chain Vulnerability main drivers. Such a model is not just new conceptualization of vulnerability but provides continuity and integration of previous research, offering a holistic picture of Supply Chain Vulnerability to enhance a deeper understanding of this scientific area.

4. PROPOSED MODEL OF SUPPLY CHAIN VULNERABILITY

This section initiates by defining the concept of supply chain vulnerability and then by breaking down into its main attributes, with evidence derived from a number of previous frameworks. However, reviewing attributes of supply chain vulnerability in clusters cannot provide an appropriate level of synthesis and interpretation. Considerable conceptual advances emerged from the early recognition that there is an interaction between vulnerability attributes. This critique is required to analyze different identified attributes and to define a step-by-step conceptual approach for assessing supply chain vulnerability. As there was no universal view of supply chain vulnerability and until now researchers still present various models and approaches to manage and to assess supply chain vulnerability, a careful examination of each of these views is important to choose the most appropriate model attributes to address supply chain vulnerability.

4.1. Research Approach for the Model

Dealing with supply chain vulnerability can be a complex, challenging assignment for both academics and practitioners (Nowakowski and Wojciechowska, 2014; Wagner and Neshat, 2012). To deal with it effectively, key issues need to be considered and include: firstly and foremost the necessity to define and understand what is meant by vulnerability and to distinguish vulnerability from the risk notion; secondly, the need to precise and categorize the main factors that lead to supply chain vulnerability among the countless causes increasing the level of supply chain vulnerability; then, the determination

of the main interrelationships between the defined drivers and the supply chain vulnerability. By giving an answer to these questions, a multi-dimensional measure could be developed to support managers in the evaluation of the vulnerability level of their supply chains. However. this measure should also be simple to assist managers in evaluating their vulnerability level and in the same time consistent to offer a guideline how this measure is computed in different types of supply chains and how can be considered and integrated into risk assessment. Many frameworks have tried to reach these objectives either by defining the vulnerability and linked it to risk or by developing different methods to evaluate and to assess the vulnerability level. However, none of the previous frameworks have addressing the myriad issue related to supply chain vulnerability. A generic view or approach, capable of comprehensively addressing all supply chain vulnerability dimensions, simply does not exists. This necessitate a conceptual model that integrate and align all the attributes, issues and concepts, to get the complete picture of supply chain vulnerability and to go beyond the analytical models. Based on these statements, the conceptual model need to be built based on existing and refined literature review to cover all the attributes of supply chain vulnerability. This necessitate defining supply chain vulnerability, determining its attributes and underling their relationships. Despite various frameworks developed for defining and assessing Supply Chain Vulnerability exist, there is no common definition of supply chain vulnerability. This latter can be seen as situation-specific, interacting with am unexpected disruptive event to generate risk. Accordingly, we consider SCV: "SCV" is susceptibility of the supply chain to the likelihood and consequences of disruptions It is therefore captures the risk exposure of the supply chain and it is often conceptualized together with supply chain risks" (p. 248)" (Juttner and Maklan, 2011). This definition is in line with previous researches stressing that supply chain characteristics could increase or decrease the vulnerability level. The state of being exposed or susceptible to risk can be interpreted under specific circumstances of a supply chain facing specific environment characteristics. However, vulnerability is usually not stable or fixed but it varies significantly within a supply chain to another. Thus, the vulnerability analysis requires first and foremost identifying the determinants and analyzing the results of possible combinations of such determinants. Some common features of vulnerability could be identified (Wagner, 2009) from the cited definition which are the following.

An exposure to serious disturbance (Svensson, 2000; Christopher and Peck, 2004)which is a set of supply chain characteristics that could either reduce the impacts of disturbance or that make the supply chain more susceptible to risks (Svensson, 2000), (Norrman and Jansson, 2004; Wagner and Bode, 2006; Craighead et al., 2007).

4.2. Defining the Determinants of Vulnerability

Due to different perceptions and definitions of supply chain vulnerability, as well the various drivers and approaches developed to apprehend and analyze this field to address the causes of vulnerability, we examine commonalities and differences between all developed frameworks and research to identify the key attributes of supply chain vulnerability. Four approaches to understanding vulnerability and its causes can be distinguished, which are: sensitivity, exposure, susceptibility and preparedness level. And in order to define the links and the relationships between these elements, a definition is presented for each concept:

1. **Exposure:** The nature and degree to which a system is exposed to significant risks (SC trends, environment' turbulence);
2. **Sensitivity:** The extent to which a supply chain or its components (processes, products or assets) are likely to experience risks and the magnitude of that risk. In other words, the degree to which a supply chain is affected by risks. It depends on the criticality of the supply chain components that could be measured by its positioning, mission, or objective within the network (Craighead et al., 2007). Vulnerability, hence also security, depend on the specific features of a supply chain and its weakest link (e.g. the gate to the warehouse that is left ajar) (Wagner and Bode, 2006);

3. **Susceptibility:** The degree to which a supply chain or its components are likely to experience losses due to an exposure to perturbations or risks. It could be evaluated in function of exposure and sensitivity;
4. **Preparedness level:** The set of attributes that enable the supply chain to adapt or to overcome potential disruptions. It could be linked to SC trends (to determine the possible future risks) (Christopher and Peck, 2004; Peck, 2006) and maturity level (the degree of awareness of managing supply chain risks within supply chain networks) (Anđelković et al., 2015).

By analyzing each key element, different conclusions could be drawn, either from the previous publications or from reports of practitioners.

Exposure is necessary, but not sufficient to determine the level of vulnerability. It is possible to be exposed but not vulnerable (Wagner and Neshat, 2012; Jury and Matteo, 2015). However it is important to understand the reasons behind an exposure to a risk. Referring to the literature review in section 2, the main factors that could influence the exposure to risk are: (1) product variants (2) outsourcing (3) lean manufacturing (4) globalization (5) single sourcing (6) decentralization (7) JIT philosophies and (8) reduction of supplier base. According to Albino and Garavelli (1995) and Jury and Matteo (2015), these practices have been developed under specific requirements and conditions to achieve the best performance. If these conditions were not validated, these trends could turn up to be one of the vulnerability causing factors (Andreoni and Miola, 2015). Taking for example JIT philosophies: this approach requires a stable environment. However, Supply Chain environment is characterized by instability and turbulence, causing a high level of variability (Buhler et al., 2016). The association of an unstable environment with the use of JIT could lead to more vulnerable supply chain networks (Albino and Garavelli, 1995). Fiskel et al. (2015) state in their research on supply chain vulnerability and resilience capabilities that: "Supply chain practices designed to keep costs low in a stable business environment can increase risk levels during disruptions. Just-in-time and lean production methods, whereby managers work closely with a small number of suppliers to keep inventories low, can make companies more vulnerable…"[1]. This leads to the following statement (1):

Exposure depends not only on the applied trends but also on the characteristics of their environment.

However, researchers have demonstrated that every supply chain has different exposure degree to risk and then, different level of vulnerability (Wagner and Neshat, 2012). So the main question is: Why and what makes the difference? By posing and seeking answers to this two-part research question, we argue that exposure to risks is not completely avoidable and, as a consequence, that all supply chains are inherently risky. However, not all firms have experienced risks within their networks. According to (BCI, 2015), only 74% of firms report at least 1 instance of supply chain disruption. It means that specific factors could determine if a company is susceptible to risk or conversely not. These factors represent the degree of sensitivity or fragility of the supply chain to unexpected events and could be determined through the position and/or the criticality of each node of the supply chain. This leads to statement (2):

The more a supply chain is sensible to unexpected change, the more it is susceptible to propagate disruptions.

On the other hand, by understanding the reasons behind susceptibility and exposure to disruptions, managers are become aware of what may threaten their business and could apply different practices and strategies to protect their activities. Thus, the Supply Chain maturity level in using or implementing supply chain management and risk management practices could acts as a preventive way to reduce the susceptibility effect in establishing the SCV (Accenture, 2015). In this framework, we intend,

therefore, to integrate the preparedness level of companies to risk as a fourth dimension of our model that would reduce SCV, leading to the following statement:

The level of preparedness to disruptions helps reduce the level of supply chain vulnerability.

The lack of a comprehensive conceptual framework that facilitates a common multidisciplinary risk evaluation impedes the effectiveness of disaster risk management.

As a result, the proposed model (see Figure 7) links the four dimensions and suggests a broader understanding of Supply Chain Vulnerability. The level of this latter depends on the balance between susceptibility level and the preparedness level.

In order to give more insights into the developed model, an alignment phase between the VESP model and the previous frameworks developed in the field of supply chain vulnerability was proposed. This step of alignment, presented in Table 2, positions the references found in the literature regarding supply chain vulnerability according to the dimensions of the VESP model and indicates synonymy or other semantic relationships when the previous SCV frameworks use different terms. It shows SC trends and environment turbulences as a common baseline when discussing about SCV. However, the other concepts do not exclude nor overlap each others. This shows a distinction between the dimensions of the VESP model.

Different levels of Supply Chain Vulnerability could be defined by evaluating each dimension, presented in Figure 7. Moreover, in order to compare the vulnerability level resulting from the different possible combination scenarios of these dimensions, it is necessary to normalize the evaluation of each factor which could be done using either quantitative or qualitative approaches.

4.3. VESP Model Instantiation Approach

Methodologies regarding how to assess vulnerability or risk in supply chain already exist (see for instance (Juttner et al., 2003). A three-point ordered scale was used for each indicator of exposure, sensitivity and adaptive capacity, according to their functional relationship with vulnerability, i.e. if the indicator was directly related to vulnerability; higher ranks were given for higher values and vice versa. For deriving weights of each indicator in their respective component of exposure, sensitivity and adaptive capacity, pair-wise comparison approach of Analytic Hierarchy Process (Saaty, 1980) was employed. The overall consistency ratio of 0.09 was achieved, suggesting that weights were generated randomly (Figure 2). Once the scores were standardized and weight established for factors, exposure,

Figure 7. Conceptual model of supply chain vulnerability (VESP model)

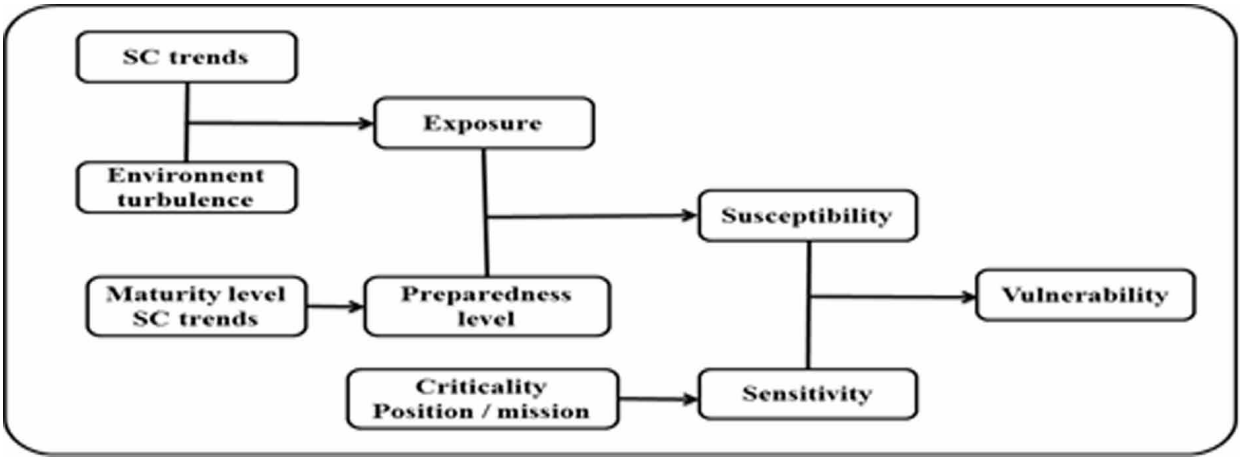


Table 2. Literature review terminologies positioned according to the VESP model dimensions

Ref.	VESP Model					
	SC Trends (Drivers of SCV)	**Environment Turbulence**	**Exposure**	**Criticality / Sensitivity**	**Maturity Level**	**Preparedness Level**
1	JIT	Variations and environment change		Criticality		Flexibility
2	Competitiveness, Lean approaches	Perturbations in environment		System fragility		Flexibility
3	Complexity	Environmental instability: technical failure, criminal acts, accidents, etc.		criticality ranking	awareness of the threats that the system is exposed to and the vulnerable situation	robustness and resilience level
4-8/11-12	Cost effectiveness trends, JIT, competitiveness					
9	Globalisation, Outsourcing, competitiveness, focus on efficiency	Environmental risk sources (lack of ownerships, chaos, inertia)			Awareness	
10	Global sourcing, effectiveness and efficiency trends, competiveness	Unpredictability and changing environment	Exposure to serious disturbance	Critical path of supply chain: (long lead time, single sources of supply, linkage where visibility is poor)	Awareness (sharing information, collaboration, SC intelligence knowledge)	Resilience level, adaptability
11	Outsourcing of manufacturing and R&D, globalization, reduction of suppliers base, buffers reduction (inventory and lead times), shorter products lifecycle, capacity limitation	Environment pressure	Exposure to high risks	Significant link in SC	Need to a new SC principles taking into account risk perspectives	
14	Longer and leaner SC, reduction of suppliers base to single sourcing	Constant changes in environment characterising by many uncontrollable forces	susceptibility to external effects	Critical nature	SC maturity	
15	Globalisation, Lean and agile SC	Instable environment	Exposure to risk	Fragility		
17	Globalization, outsourcing	volatility of trading environment	Exposure to risk		Safety measures	
18	reduction of suppliers base, Global sourcing,		Exposure to severe disruptions	Node criticality	Knowledge of SC trends	SC mitigation capabilities and recovery warning
20	Focus on efficiency, globalization, decentralization, outsourcing, product/ process complexity, JIT	External factors	Exposure to disruption	Critical components that company depend on, sensitivity		Proactive strategies that reduce SCV level through reducing exposure points

Table 2. Continued

Ref.	VESP Model					
	SC Trends (Drivers of SCV)	Environment Turbulence	Exposure	Criticality / Sensitivity	Maturity Level	Preparedness Level
21	Leaner approaches, outsourcing, inventory reduction, single sourcing,	External events	Exposure to disruption			
22	Demand side (customer dependency, complexity and lifecycle of product, distribution and transportation), supply side (reduction of supplier base,,,), SC structure	Changes in economic business and ecological environment			Event readiness measures	
23	globalized supply chains, specialized factories, centralized distribution, outsourcing, reduction of suppliers base, technological innovation, volatility of demand	Continual turbulence, dynamic of turbulence	Susceptible to disruptions			Adaptability concept
24	globalization, complexity		Susceptibility to SCR			preventive SCRM
25	global sourcing, single sourcing	SC environment	Susceptibility and /or exposure to SCR		SCRM knowledge	SC resilience capabilities
26	Internationaliztion and lean approaches				Awareness of existence of SC disruption	
27	Globalization of sourcig network, customer or supplier dependency, supply chain complexity, JIT, JIS, Lean approaches (Scholten, 2014) and (Liu et al., 2014)	changes in environment	Exposure to risk / Susceptibility to SC disruption	Sensitivity of operations	Supply chain risk planning	
29	Turbulence, deliberate threats, external pressures, resources limits, sensitivity, connectivity, supplier/ customer disruptions	Chaotic external pressures and turbulent changes	Susceptibility to disruption			SC capabilities
30	outsourcing, globalization, off-shore manufacturing, reduction of inventory, lack of preparedness	Unpredictability and increasingly uncertain environment / turbulence and uncertainty of SC	Exposure to serious disturbance			SC capabilities
31	Leanness and effectiveness supply chains	Unexpected business environment	susceptibility to disturbance	Critical SC characteristics		

Table 2. Continued

Ref.	VESP Model					
	SC Trends (Drivers of SCV)	**Environment Turbulence**	**Exposure**	**Criticality / Sensitivity**	**Maturity Level**	**Preparedness Level**
32	Market and technological turbulence, business complexity, critical purchase portfolio	Context riskiness = degree of criticality and turbulence that characterize the context in which companies operate, market and technological turbulence	Exposure to SCR	Criticality of purchase portfolio	Extend to which SCRM practices are applied	Preparedness to deal with SCR, prevention practices
35	Outsourcing, delocalisation, increase of products variety, environmental turbulence, difficult market, global sourcing, critical purchases and firm conditions	Environment turbulence	Exposure to risk / Susceptibility to SC disruption	Critical purchase		SCRM practices
37	Outsourcing	Environment turbulence	Exposure to risk / Susceptibility to SC disruption			SCRM practices

sensitivity, adaptive capacity and vulnerability maps were prepared varying from 1 to 5 ('very low', 'low', 'moderate', 'high' and 'very high') by taking weighted sum of the rank of all relevant indicators.

Thus, the VESP conceptual model can be used through the following steps:

1. Determine the degree of exposure:
   a. Identify the mains SC trends applied;
   b. Describe the environmental condition:
      i. If the environment is turbulent, SC trends are considered as vulnerability drivers. Go to step 2;
      ii. Else, SC trends are not considered as vulnerability drivers;
2. Determine the sensitivity level of SC asset;
3. Identify the susceptibility level of the SC:
   a. If the SC is exposed and at the same time it is sensitive to disruption, the level of susceptibility to disruption will be high (Go to step 3);
   b. Else, the level of susceptibility will be low;
4. Evaluate the preparedness level through maturity assessment;
5. Determine the level of supply chain vulnerability: A score is determined from a qualitative assessment of the three predefined dimensions (exposure, criticality and preparedness level):

$$\text{Vulnerability index} = (\text{Exposure} \times \text{sensitivity})^{1/3} \times \text{preparedness level})^{1/3}$$

The vulnerability level is assigned to five relative vulnerability categories form slightly vulnerable to extremely vulnerable. The indicators build upon data from literature and expert valuation. They are scored on a scale from 0 (very low) to 1 (very high). Establishment of Assessment Set. We establish the assessment set by selecting, "very high," "high," "higher," "medium," "lower," "low," and "very low," seven semantic items:

V={very high (VH), high (H), little high (VH), medium (M), little low(LL), low(L), very low(VL)}

In order to evaluate the different level of components and then the to calculate an overall vulnerability score (V), the index combines all information on exposure and corresponding susceptibility (Ss) as well as preparedness level in the following algorithm: The value of each component is standardized on a scale from zero to one, with higher index values indicating higher vulnerability (see Table 3).

The order and the signs used for the methods of calculation of vulnerability define the relationships between the three components. However, in a metric-identifying approach, the indicators come from different sources and disciplines, and are expressed in different units of measurement. Index values then need to be standardized or normalized. In many cases, data normalization is based on minimum and maximum values in the data set, and places on a scale from 0 to 1using the typical normalization method "min-max." Another issue that has to be considered is the quantitative relevance, or weight, that is associated with the different components. Different metric systems often rely on equal weights, leaving to policymakers, practitioners, and stakeholders the opportunity to apply a goal- or priority-oriented weighting system.

As a result, a three-dimensional model is developed and presented in Figure 8.

Typically, these assessment evaluations include potential supply chain vulnerability levels based on the Susceptibility to risks, the criticality of the asset which it is exposed to risk and it preparedness level if the asset was exposed. While these variables seem to be diverse and complex, it is possible to assess the potential vulnerability using a ranking process for each identified dimension. The final score, or assessment rating, determines the supply chain vulnerability index (see Figure 8).

As a result, supply chain vulnerability index or level can be determined using the following three variables, and ranking the response to each of these variables using a scale ranging from 0 to 1 point. The lower the numerical ranking in each category is, the lower the vulnerability level. However, the higher the ranking implies a greater susceptibility to risks and a higher preparedness level but a lower level of vulnerability.

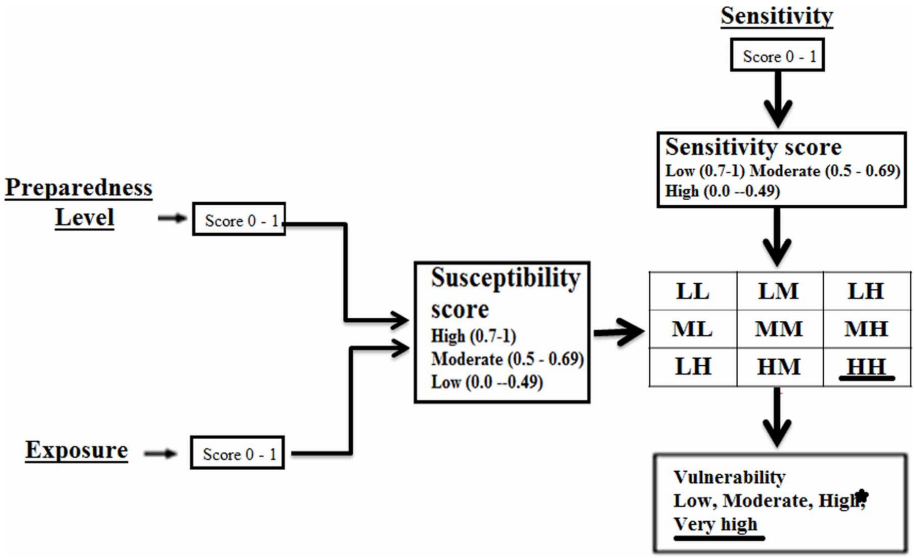
5. CASE STUDIES

In order to test the applicability of our proposition and to evaluate the level of Supply Chain Vulnerability, real case study was applied, which is international manufacturer of denture products. has been specializing for over 30 years in the development, production and marketing of dental and

Table 3. Supply chain vulnerability dimensions

Notation	Definition	
E	Exposure	
S	Sensitivity	
P	Preparedness level	$P = \sum_{i}^{n} P_i$
S_s	Susceptibility	$S_i = \sum_{i}^{n} \left(E_i - S_{si} \right)$
V	Vulnerability	$V = S_i - P$

Figure 8. Supply chain vulnerability index (VESP model)



denture care products. The products are manufactured in Switzerland under the highest standards and distributed throughout the world by dispensing chemists, dentists and other specialist sales outlets.

Despite the differences in terms of industry and company size, the three companies adopt the same supply chain practice which is single sourcing with the addition of lean manufacturing for Toyota. These trends are considered in the literature review as one of the main causing factors of an increase in the vulnerability level. In the case of Nokia and Ericsson, the main reason for their exposure to risk is a fire which has destroyed the plant of their main single suppliers. For both Nokia and Ericsson, this has caused a production interruption for several weeks and important losses particularly for Ericsson. Despite of this, Nokia Market Shares have increased after this incident, making it the leading company in the field of telecommunication. For Land Rover, the company actively reduced its base of suppliers. Until 2000, the company has decided to keep one supplier of the chassis frame "UPF- Thompson" for its bestselling model. Unfortunately, UPF lost money on others ventures into foreign markets and went bankrupt at the end of 2001. This incident has put into question the Land Rover survival in the market. Nine months is the period that Land Rover has taken to find a sustainable supplier instead of UPF. This incident has caused financial losses and the dismissal of 1400 workers. Affected by the same type of risk, Toyota, in 2015, recalled more than 6.5 million of cars all over the world due to a defective airbag produced by one of its sole supplier. This quality issue could have threatened the life of car users. This is why Toyota has decided to voluntarily recall all its products from the market.

The question raised here is: why the three companies have different level of risk impacts, although they face the same type of risk and they adopt the same SC practices? In other words, why these three companies have different level of vulnerability?

In order to determine the answer, Table 4 presents the results of application of our proposition on the three case studies. Unfortunately, the analysis of the three case studies is very restricted due to a limited amount of data related to these cases. Thus, each vulnerability factor has been positioned using a definite set {low; moderate; high; very high and critical}. Even if such an assumption disables the opportunity to establish quantitative calculations leading to a final note for the vulnerability of each case, our model allows us to understand the vulnerability causing factors and the reasons of its distinctive level across the three companies. Despite the differences in terms of industry and company size, the three companies share some fundamental commonalities regarding their business model and supply chain strategies which single sourcing and lean manufacturing and faced the same type

Table 4. A brief overview of the three case studies

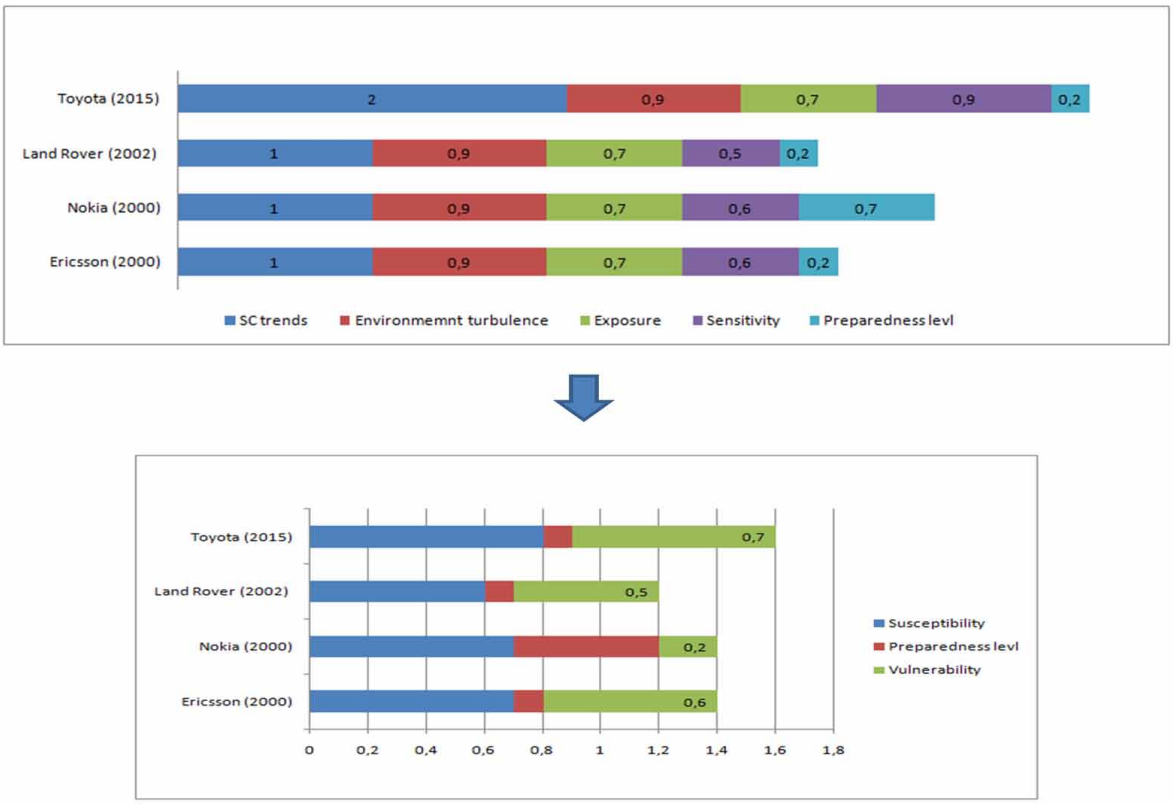
	Nokia and Ericsson (2000)	Land Rover (2002) (Peck, 2005)	Toyota (2015)
Activity Sector	Telecommunications	Car manufacturing	Car manufacturing
Disruptive events	Fire at supplier's plant	Supplier bankruptcy	Quality defect of "Airbag" component
SC trends applied	Single sourcing	Reduction of suppliers' base to single sourcing	Single sourcing + Lean manufacturing
Type of risk	Supplier risk	Supplier Risk	Supplier risk
Impacts	$1.7 billion of annual loss for Ericsson	35 million pounds loses and the release of 1400 workers	Recall of 6.5 million cars

of risk which is supplier risk due to different raison for each company, causing severe impacts. Table 4 presents a summary of the three case studies.

Figure 9 presents the results of application of our proposition on the three case studies. Unfortunately, the analysis of the three case studies was very restricted due to limited amount of data related to these cases. Thus, each vulnerability factor has been using a defined set {low; moderate; high; very high and critical}. Even if such assumption disables the opportunity to establish clear calculations leading to a final note for the vulnerability of each case, our model allows us to understand the vulnerability causing factors and the reasons of its distinctive level across the three companies.

The three cases developed herein have several levels of vulnerability. The difference between Nokia and Ericsson facing the same supplier problem can be found regarding their preparedness

Figure 9. Supply chain vulnerability index measured for the three case studies



level. This led to a global impact more negative for Ericsson than for Nokia which has not been anticipated. Moreover, for Land Rover and for Toyota, the SC trends played a significant role in the vulnerability level.

6. CONCLUSION

The field of supply chain risk management is relatively nascent and the vulnerability concept is more recent. This explains the scarceness of scientific publications related to this field. The results of reviewing the literature underline the need for more theoretical framework to understand the concept of Supply Chain Vulnerability. Most of previous research frameworks have dealt with defining the concept, determining its drivers and measurement options. However, one of the gaps revealed in the state of the art of Supply Chain Vulnerability is the missing link or conceptualization of its different constructs and their relationships. It is extremely important for any theory development to build the knowledge related to this field by gaining a deeper understanding of the interdisciplinary phenomenon of vulnerability. This is why we conduct this research trying to understand what is Supply Chain Vulnerability? What are its causing factors? And what is the link to supply chain practices? The answers to these questions are presented in our proposed conceptual model of Supply Chain Vulnerability.

This article has firstly identified the main SC trends as Vulnerability drivers. These trends, which are recognized as drivers of supply chain performance, are also exposing the supply chain to new risks. Therefore, the conceptual model developed in this article describes the link between this statement and the vulnerability.

In order to demonstrate the applicability of such a model, a case study based on 3 supply chain major disruptions intends to show that it is necessary to properly balance vulnerability factors with practices increasing the adaptive capabilities of the supply chain.The main perspective of this article is to develop an ability to deal with measures of each factor evocated in the model in order to find more precise information about past supply chain crisis.

REFERENCES

Albino, V., & Garavelli, A. C. (1995). A methodology for the vulnerability analysis of just-in-time production systems. *International Journal of Production Economics*, *41*(1), 71–80. doi:10.1016/0925-5273(95)00014-3

Albino, V., Garavelli, A. C., & Okogbaa, O. G. (1998). Vulnerability of production systems with multi-supplier network: A case study. *International Journal of Production Research*, *36*(11), 3055–3066. doi:10.1080/002075498192283

Anđelković, A., Barac, N., & Milovanović, G. (2015). Risk Factor Management: a Mechanism of Supporting Supply Chain Resilience. Economic Themes, 52(1), 81-98.

Andreoni, V., & Miola, A. (2015). Climate change and supply-chain vulnerability: Methodologies for resilience and impacts quantification. *International Journal of Emergency Services*, *4*(1), 6–26. doi:10.1108/IJES-09-2014-0012

Asbjornslett, B. E. (1999). Assess the vulnerability of your production system. *Production Planning and Control*, *10*(3), 219–229. doi:10.1080/095372899233181

Asbjørnslett, B. E. (2008) Assessing the vulnerability of supply chains. In G. A. Zsidisin & B. Ritchie (Eds.), Supply Chain Risk: A handbook of Assessment, Management and Performance. Springer.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1–13. doi:10.1016/j.ejor.2015.12.023

Barac, N. (2011). Risk and the resilient supply chain. Facta Universitatis, 8(2).

Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management*, *11*(4), 519–540. doi:10.1016/j.intman.2005.09.008

Bogataj, D., & Bogataj, M. (2007). Measuring the supply chain risk and vulnerability in frequency space. *International Journal of Production Economics*, *108*(1), 291–301. doi:10.1016/j.ijpe.2006.12.017

Briano, E., Caballini, C., & Revetria, R. (2009). Literature review about Supply Chain Vulnerability and resiliency. In *Proceedings of the 8th WSEAS international conference on System science and simulation in engineering* (pp. 191-197). World Scientific and Engineering Academy and Society (WSEAS).

Bühler, A., Wallenburg, C. M., & Wieland, A. (2016). Accounting for external turbulence of logistics organizations via performance measurement systems. *Supply Chain Management*, *21*(6), 694–708. doi:10.1108/SCM-02-2016-0040

Chowdhury, M.H., Mohammed Naim, A.D., & Quaddus, M.A. (2012). Supply Chain Resilience To Mitigate Disruptions: A QFD Approach. PACIS.

Chrisptoher, M., Khan, O., & Yurt, O. (2011). Approaches to Managing Global Sourcing Risk. *Supply Chain Management*, *16*(2), 67–81. doi:10.1108/13598541111115338

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, *15*(2), 1–14. doi:10.1108/09574090410700275

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, *15*(2), 1–14. doi:10.1108/09574090410700275

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences*, *38*(1), 131–156. doi:10.1111/j.1540-5915.2007.00151.x

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., & Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering & System Safety*, *94*(5), 954–963. doi:10.1016/j.ress.2008.10.011

Fawcett, S. E., Waller, M. A., Miller, J. W., Schwieterman, M. A., Hazen, B. T., & Overstreet, R. E. (2014). A trail guide to publishing success: Tips on writing influential conceptual, qualitative, and survey research. *Journal of Business Logistics*, *35*(1), 1–16. doi:10.1111/jbl.12039

Fiksel, J., Polyviou, M., Croxton, K. L., & Pettit, T. J. (2015). From Risk to Resilience: Learning to Deal With Disruption. *MIT Sloan Management Review*, *56*(2), 79.

Goel, S., & Chen, V. (2008). Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process. *International Journal of Production Economics*, *115*(1), 104–112. doi:10.1016/j.ijpe.2008.05.002

Gualandris, J., & Kalchschmidt, M. (2014). A model to evaluate upstream vulnerability. *International Journal of Logistics Research and Applications*, *17*(3), 249–268. doi:10.1080/13675567.2013.860959

Gualandris, J., & Kalchschmidt, M. (2015). Supply risk management and competitive advantage: A misfit model. *International Journal of Logistics Management*, *26*(3), 459–478. doi:10.1108/IJLM-05-2013-0062

Hallikas, J., & Lintukangas, K. (2016). Purchasing and supply: An investigation of risk management performance. *International Journal of Production Economics*, *171*(Part 4), 487–494. doi:10.1016/j.ijpe.2015.09.013

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: a literature review. International Journal of Production Research. doi:10.1080/00207543.2015.1030467

Jury, G., & Matteo, K. (2015). Supply risk management and competitive advantage: A misfit model. *International Journal of Logistics Management*, *26*(3), 459–478. doi:10.1108/IJLM-05-2013-0062

Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management*, *16*(4), 246–259. doi:10.1108/13598541111139062

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, *6*(4), 197–210. doi:10.1080/1367556031000162701 6

Klag, M., & Langley, A. (2013). Approaching the conceptual leap in qualitative research. *International Journal of Management Reviews*, *15*(2), 149–166. doi:10.1111/j.1468-2370.2012.00349.x

König, A., & Spinler, S. (2016). The effect of logistics outsourcing on the supply chain vulnerability of shippers: Development of a conceptual risk management framework. *International Journal of Logistics Management*, *27*(1), 122–141. doi:10.1108/IJLM-03-2014-0043

Kumar, S., & Schmitz, S. (2011). Managing recalls in a consumer product supply chain–root cause analysis and measures to mitigate risks. *International Journal of Production Research*, *49*(1), 235–253. doi:10.1080/0 0207543.2010.508952

Lahmar, A., Galasso, F., Chabchoub, H., & Lamothe, J. (2015). Towards an Integrated Model of Supply Chain Risks: An Alignment Between Supply Chain Characteristics and Risk Dimensions. In *Risks and Resilience of Collaborative Networks* (pp. 3–16). Springer International Publishing. doi:10.1007/978-3-319-24141-8_1

Lahmar, A., Galasso, F., Chabchoub, H., & Lamothe, J. (2016). Conceptual Framework of Supply Chain Vulnerability. In *Proceedings of the 6th International Conference on Information Systems, Logistics and Supply Chain (ILS Conference)*.

Levner, E., & Ptuskin, A. (2015). An entropy-based approach to identifying vulnerable components in a supply chain. *International Journal of Production Research*, *53*(22), 6888–6902. doi:10.1080/00207543.2014.934400

Liu, L., Daniels, H., & Hofman, W. (2014). Business Intelligence for Improving Supply Chain Risk Management. In *Enterprise Information Systems* (pp. 190–205). Springer International Publishing. doi:10.1007/978-3-319-09492-2_12

Liu, Z., & Zhuang, W. (2013). Governance of global supply chains vulnerability by business-based interorganizational information platform. *Journal of Systems Science and Systems Engineering*, *22*(1), 1–20. doi:10.1007/s11518-013-5211-z

Neureuther, B. D., & Kenyon, G. (2009). Mitigating Supply Chain Vulnerability. *Journal of Marketing Channels*, *16*(3), 245–263. doi:10.1080/10466690902934532

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management*, *34*(5), 434–456. doi:10.1108/09600030410545463

Pettit, T. J., Croxton, K. L., & Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics*, *34*(1), 46–76. doi:10.1111/jbl.12009

Rangel, D. A., de Oliveira, T. K., & Leite, M. S. A. (2015). Supply chain risk classification: Discussion and proposal. *International Journal of Production Research*, *53*(22), 6868–6887. doi:10.1080/00207543.2014.910620

Skilton, P. F., & Robinson, J. L. (2009). Traceability and normal accident theory: How does supply network complexity influence the traceability of adverse events? *The Journal of Supply Chain Management*, *45*(3), 40–53. doi:10.1111/j.1745-493X.2009.03170.x

Svensson, G. (2002). (d): Vulnerability scenarios in marketing channels. *Supply Chain Management*, *7*(5), 322–333. doi:10.1108/13598540210447733

Svensson, G. (2002b). A conceptual framework of vulnerability in firms' inbound and outbound logistics flows. *International Journal of Physical Distribution & Logistics Management*, *32*(2), 110–134. doi:10.1108/09600030210421723

Svensson, G. (2002c). A typology of vulnerability scenarios towards suppliers and customers in supply chains based upon perceived time and relationship dependencies. *International Journal of Physical Distribution & Logistics Management*, *32*(3), 168–187. doi:10.1108/09600030210426511

Svensson, G. (2004). Key areas, causes and contingency planning of corporate vulnerability in supply chains. *International Journal of Physical Distribution & Logistics Management*, *34*(9), 728–748. doi:10.1108/09600030410567496

Van de Voort, M., Willis, H., Ortiz, D., & Martonosi, S. (2007). Applying Risk Assessment To Secure The Containerized Supply Chain. In I. Linkov, R. J. Wenning, & G. A. Kike (Eds.), *Managing Critical Infrastructure Risks* (pp. 79–95). Springer Netherlands. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4020-6385-5_5 doi:10.1007/978-1-4020-6385-5_5

Vlajic, J.V. (n.d.). Vulnerability and robustness of SME supply chains: An empirical study of risk and disturbance management of fresh food processors in a developing market.

Vlajic, J. V., Van der Vorst, J. G., & Haijema, R. (2012). A framework for designing robust food supply chains. *International Journal of Production Economics*, *137*(1), 176–189. doi:10.1016/j.ijpe.2011.11.026

Vlajic, J. V., van Lokven, S. W., Haijema, R., & Van Der Vorst, J. G. (2013). Using vulnerability performance indicators to attain food supply chain robustness. *Production Planning and Control*, *24*(8-9), 785–799. doi:10.1080/09537287.2012.666869

Wagner, S. M., Mizgier, K. J., & Arnez, P. (2014). Disruptions in tightly coupled supply chain networks: The case of the US offshore oil industry. *Production Planning and Control*, *25*(6), 494–508. doi:10.1080/09537287.2012.705355

Wagner, S. M., & Neshat, N. (2010). Assessing the vulnerability of supply chains using graph theory. *International Journal of Production Economics*, *126*(1), 121–129. doi:10.1016/j.ijpe.2009.10.007

ENDNOTES

[1] Fiksel, J., Polyviou, M., Croxton, K. L., & Pettit, 2015; pp. 80