Dual Sourcing in Supply Chain Design: A Multi-Dimensional Framework of Risk

Mario NORBIS
Management Department, Quinnipiac University
Hamden, CT 06518 USA

and

Mary J. MEIXELL
Management Department, Quinnipiac University
Hamden, CT 06518 USA

ABSTRACT

Sourcing decisions are a key factor in supply chain security. In this research the authors posit that there are multiple risk types involved in the sourcing decision, and develop a model framework for analyzing these risk components. Specifically, increasing the number of sources minimizes risk related to supply disruptions, but intensifies risk related to security failures. This paper, which is a part of an ongoing research effort that develops a supply chain approach for international logistics, concludes that the best structure for single or dual sourcing from a risk minimization perspective depends on whether the suppliers operate in series or in parallel, and if in parallel, as a backup or as an alternative with a prescribed percentage.

Keywords: Supply Chain Security, Risk Analysis, Supplier Selection, Dual Sourcing, Supply Chain Management

INTRODUCTION

Sourcing decisions have become so important in the life of a corporation to the extent that they can define the corporation its growth and the firm’s competitive advantage [1]. The importance of these decisions is underscored in the supply chain. Dependency on suppliers is such that even for service industries half of their purchased services are from other companies [2]. In a supply chain, where firms are linked through bidirectional flows of materials, information, and monetary resources, any change occurring at an upstream stage of the supply chain may affect the performance of firms downstream, through changes in quality, price or availability of material [3].

The work by Anton and Yao [4] concluded that under complete information and with suppliers that have strictly convex costs, a buyer is better off selecting a single source. Since that time, numerous works have analyzed single versus multiple sourcing, including Inderst [5], Zeng [1], Szweczywski [6], Li [3], Mishra [7] and Jayaraman [8]. Some of these studies include a practitioner’s point of view as they focus on the effects that the multiple source has on price along with preventing disruptions in the supply line. Berger [9] analyzes the effect that multiple sourcing may have on risks for the buyer and for the whole supply chain.

In this research the authors start with the premise that there are multiple risk types involved in sourcing. While increasing the number of sources minimizes risks related to supply disruptions, security risks may increase with the inclusion of more members in the supply chain. To explore this premise we build a model that analyzes the effects on security as a buyer moves from single sourcing to dual sourcing.

This introduction is followed by a literature review of published work in the area. The quantification of supplier security, a problem description, and model development are then presented. We introduce a case example and then close the paper with conclusions and ideas for next steps.

LITERATURE REVIEW

Research that compares single and multiple sourcing procurement includes both theoretical and empirical studies. Some of this research is academically focused while others are more practitioner-oriented.

Our review starts with the contributions by Anton and Yao [10] [4] in which second sourcing and split awards were analyzed in comparison with single sourcing scenarios. Under the conditions analyzed in these cases, single sourcing was preferred. The results from Anton and Yao [4] were extended by Inderst [5], allowing multiple buyers and concluding that the optimality of single sourcing depends on the relative size of the buyer.

Surveys by Szweczywski [6] and by Larson [11] provide evidence that single-source suppliers deliver higher quality at a lower cost to the buyer. Single-sourcing is also credited with improvement in quality and better pricing by Tullous and Utecht [12] and by Christopher [13].
A descriptive work by Zeng [1] synthesizes available sourcing alternatives into 4 categories: single sourcing, multiple sourcing, single/dual hybrid network, and global sourcing. Single sourcing is understood as using only one source of supply for a particular material or component [14] [15], while multiple sourcing is simply using more than one source. It is argued [16] that risk is increased by single sourcing and that emergency plans in place are needed for emergencies. The existence of little empirical research on the benefits of single sourcing is highlighted by Seitz [17]. The impact of disruptions is graphically analyzed by Li [3] and quantified from the perspective of time and cost.

The single/dual hybrid network involves the use of two or more sources per product type (e.g. an instrument panel for a specific model), with only one source being used for a single component number (e.g. that might specify color). Network sourcing is often the choice of assembly type manufacturing who use large number of parts, as in the auto industry [18]. Mishra [7] shows through an analytic model that order splitting is often the underlying reason for the improvement attributed to dual sourcing. Global sourcing may be defined in this context as the efficient use of worldwide resources [19]. In a highly interconnected world, it also can be argued that all sourcing is global.

Since the events of 9/11, risk has become an important concern for management along the supply chain - in some cases, risk is prioritized over price or quality [20]. For these firms, the “make or buy” decisions previously based on “cost-benefit” analysis are now based on risk-value analysis.

Pope [21] identifies four dimensions of supply chain security: security of the product, security of the information, security of the money and security of the logistics system. The first of these four dimensions pertains exclusively to the supplier. The relevance of this topic is further emphasized by Sheu [22] who concludes that international supply chain security has many issues to resolve to become a fully collaborative system.

Trust is defined by Laeaquddin and Sahay [23] as a supply chain partner’s threshold level of risk-bearing capacity. Laeaquddin et al. [24] state that traditionally the intended objective of a supply chain relationship has been to achieve lower cost and to improve product/service delivery. Lately, however, it has been argued that building trust through partnership to better manage risk is now at the heart of the supply chain objectives [25].

Another important topic pertains to security dimensions associated with the supplier selection. Closs and McGarrell [26] propose separate categorization schemes for security themes in suppliers and carriers. This scheme was utilized by Meixell and Norbis [27] when modeling the supplier and carrier choice in the supply chain to improve security as well as by Voss et al. [28] when analyzing the security in food supplier selection.

In this context, our research aligns with that of Sheffi [29] in looking at security as a double challenge. We also follow Closs and McGarrell [26] and Voss et al. [28] in addressing how to best assign security scores to suppliers. This work also contributes to the literature with a structure for the analysis of risk contributors in the environment of dual sourcing in the supply chain.

**Supplier Security**

This research starts with the premise that there is more than one type of risk involved in sourcing decisions and while increasing number of sources minimizes risks related to supply disruptions, security risks may increased with the inclusion of more members in the supply chain. The first type of risk is represented by disruption in the supply chain, motivated by a supplier’s inability to provide the right amount of products and services at the required time and with the expected quality. We argue here that this type of risk is a function of the traditional supplier selection criteria: product quality, price and delivery reliability [28]. Here, we use Zeng [1] for the categories in each of these themes as shown in Table 1.

<table>
<thead>
<tr>
<th>Supplier Security Type 1 Rating Illustration</th>
<th>Supplier 1 Score</th>
<th>Supplier 2 Score</th>
<th>Supplier 3 Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Quality</td>
<td>2 (67%)</td>
<td>2 (67%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Specifications</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Equipment Capability</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Quality Assurance Process</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Product Price</td>
<td>2 (67%)</td>
<td>3 (100%)</td>
<td>-1 (0%)</td>
</tr>
<tr>
<td>Cost Structure</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Financial Capability</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Supplier Value Analysis Effort</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Delivery Reliability</td>
<td>2 (100%)</td>
<td>2 (100%)</td>
<td>-1 (0%)</td>
</tr>
<tr>
<td>Production Schedule</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Contract Performance</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

The second type of risk is represented by the possibility of a terrorism in any of its forms (i.e. unauthorized people, contraband or weapons of mass...


They rather represent an externally forced interruption by humans that includes damage and may take the form of terrorism, sabotage or other criminal action.

We address this problem by modeling the alternatives and providing case examples of their use.

**MODEL**

Let’s consider the case of 2 potential suppliers identified as S1 and S2, each able to provide the same product or service with different qualification for price, product quality and on-time delivery. Risk is defined here, consistent with Hutchins [20], as the probability that an event or action adversely affects an organization or its associated supply chain. The probability that each supplier provides the desired product in the amount requested, in time and undamaged is represented by \( p_1 \) and \( p_2 \). The risk of service interruption or partial delivery represented by \( r_1 \) and \( r_2 \) are calculated as

\[
\begin{align*}
    r_1 &= 1 - p_1 \\
    r_2 &= 1 - p_2
\end{align*}
\]

\( p_1 \) and \( p_2 \) are evaluated for each supplier based in the characteristics provided by Zeng [1] and represented in Table 1. Also \( v_1 \) and \( v_2 \) represent the proportions in which demand is split between the two suppliers in the case parallel splitting demand.

\[
v_1 + v_2 = 1
\]

Beyond the ability of the supplier to provide the product or service on time and in the quantity and quality required, the security measures to handle the cargo have become of vital importance [30], [31]. The latter includes security in the facility, government regulation, supplier practices and others as indicated by Closs and McGarrell [26].

The risk or the probability of these events is difficult to evaluate because of lack or irrelevance of historical data [30] and belong more in the area of prediction rather than forecast. This risk is represented as \( t_1 \) and \( t_2 \) which are a function on the security scores (SS1 and SS2). It would be expected that \( t_1 \) and \( t_2 \) are much smaller than \( r_1 \) and \( r_2 \); we can also assume for the sake of discussion and without loss of generality, that

\[
t_1 < t_2 \quad \text{and} \quad r_1 < r_2
\]

We discuss three different scenarios for the arrangement of suppliers, one in series and two in parallel. For each scenario two alternatives are considered, single supplier or two suppliers [32], [33]. These scenarios and alternatives are summarized in Table 2.
For the series scenario, two independent suppliers in series are continuously and simultaneously active. The risk of undersupply in this case is
\[ r_1 + r_2 - r_1 \times r_2 \]
while the risk of a catastrophic event is
\[ t_1 + t_2 \]
because any of the two can independently at any time be the origin of a catastrophic threat. In the first parallel scenario, both suppliers are active simultaneously, splitting demand in every cycle. In this parallel-splitting scenario the probability of undersupply becomes
\[ v_1 \times r_1 + v_2 \times r_2 \]
and the probability of fully stopping supply becomes
\[ r_1 \times r_2 \]
Likewise the risk of a catastrophic event in every cycle is
\[ t_1 + t_2 \]
for the same reasons as in the series scenario.

In the second parallel scenario, suppliers in parallel, one serves as a backup when the first supplier fails to deliver. For this case the risk of undersupply is given by the probability of both suppliers failing
\[ r_1 \times r_2 \]
which is also the risk of total stop of supply. Meanwhile, in any cycle the risk of a catastrophic event is given by the probably of any of the two suppliers independently and not simultaneously providing a threat, which in worst case scenario will be
\[ \max (t_1, t_2) \]
For the three scenarios and the two alternatives, single and dual suppliers, the two types of risks are tabulated in Table 2.

### Analysis of Results
The results in Table 2 are analyzed for the three scenarios. For the series scenario Table 2 indicates that if a second supplier is added to the more reliable one, the risk of interruption increases as
\[ r_1 + r_2 - r_1 \times r_2 \geq r_1 \]
and the risk of catastrophic event also increases as.

\[ t_1 + t_2 \geq t_1 \]

If a second source is utilized in parallel and the demand is split in every cycle so that both suppliers are providing part of the demand simultaneously, the risk of undersupply increases as

\[ v_1 r_1 + v_2 r_2 \geq r_1 \]

and the risk of catastrophic event also increases because

\[ t_1 + t_2 \geq t_1 \]

Finally if a second supplier is added as a backup of the best one in a way that only one is active at a time, the risk of undersupply decreases because

\[ r_1 \cdot r_2 \leq r_1 \]

while the risk of a catastrophic event increases because

\[ \text{Max} \{ t_1 , t_2 \} \geq t_1 \]

generating a tradeoff situation.

**EXAMPLE**

A numerical analysis is included in Table 3 below as an illustration for the parallel backup case.

Table 3. Illustration

<table>
<thead>
<tr>
<th>Case 1</th>
<th>Case 2</th>
<th>Case 3</th>
<th>Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r_1 )</td>
<td>.18</td>
<td>.12</td>
<td>.09</td>
</tr>
<tr>
<td>( r_2 )</td>
<td>.21</td>
<td>.18</td>
<td>.12</td>
</tr>
<tr>
<td>( t_1 )</td>
<td>.0002</td>
<td>.0001</td>
<td>.0002</td>
</tr>
<tr>
<td>( t_2 )</td>
<td>.0003</td>
<td>.0002</td>
<td>.0005</td>
</tr>
<tr>
<td>Risk of under supply</td>
<td>.038</td>
<td>.0216</td>
<td>.011</td>
</tr>
<tr>
<td>Catastrophic risk</td>
<td>.0003</td>
<td>.0002</td>
<td>.0005</td>
</tr>
</tbody>
</table>

**CONCLUSIONS AND NEXT STEPS**

In this research we propose that there are multiple risk types involved in a supplier sourcing decision. Specifically, increasing the number of sources minimizes risk related to supply disruptions, but intensifies risk related to security failures. We develop a model framework for analyzing these risk components and show that the best structure for single or dual sourcing from a risk minimization perspective depends on whether the suppliers operate in series or in parallel, and if in parallel, as a backup or as an alternative with a prescribed percentage.

The next steps in this research are to develop an approach for estimating \( t_1 \) and \( t_2 \), given supplier security scores from the risk assessment matrix along with other related information in the supply chain. Also, the expected loss may be factored into the analysis, so that supplier selection reflects the overall impact along with the probability of a negative event occurring.

**REFERENCES**


