VOLUNTARY SUPPLY CHAIN SECURITY PROGRAM IMPACTS: AN EMPIRICAL STUDY WITH BASC MEMBER COMPANIES

Ximena Gutiérrez, Juha Hintsa, Philippe Wieser and Ari-Pekka Hameri

This paper is an abridged version of presentations given previously at conferences and meetings about supply chain security.¹

Abstract

Managing security in global supply chains has been gaining increasing attention in business and governmental agendas since the terrorist attacks in the United States in 2001. Since then several new voluntary government-business partnership programs have emerged to enhance security in end-to-end supply chains. However, a few programs have existed for a longer time, one of them is the BASC (Business Alliance for Secure Commerce) program, active as a business alliance in Latin America since 1996, originally fighting narcotics smuggling, and later converted into a holistic supply chain security management program. Understanding the implications – costs, trade-offs, benefits, etc. – of security management programs is a complicated task, with very limited existing literature. This paper, being the first survey of its kind, presents the results of the survey carried out with 102 BASC member companies, including: (1) the most commonly implemented security measures; (2) the most (and least) efficient security measures; (3) the relationship between the cost and effectiveness of the measures; and (4) the benefits obtained while implementing these security measures. Finally, the paper provides recommendations for governmental and company decision makers on designing future ‘win-win’ supply chain security programs.

Introduction

The paradigm of managing and regulating security in global supply chains is changing. Before 2001, security management decisions – security measures, investments, documentation, etc. – were primarily taken at individual company level, with no or very limited interaction with other supply chain participants or governmental agencies. Since 2001 the situation has changed: governmental agencies, mainly the customs administrations, have entered the field, with their vested interest to protect their respective nations against terrorism and other serious international crime. The first country to move was the US (C-TPAT program since 2002), followed by Australia, New Zealand, the European Union, and a few others, later on.

One exception to the ‘pre-9/11 era’ is the BASC (Business Alliance for Secure Commerce) program, which was established in 1996 to fight narcotics smuggling, exploiting existing supply chains and logistics networks, from some Latin American countries, mainly to North America. The abbreviation ‘BASC’ stood originally for ‘Business Anti-smuggling Coalition’, and was later converted to ‘Business Alliance for Secure Commerce’. The mission statement of the BASC organisation is to ‘facilitate and stimulate agile international trade through the implementation and management of security standards

¹ This paper is an abridged version of presentations given previously at conferences and meetings about supply chain security.
International Network of Customs Universities

and procedures applied to the international supply chain. BASC has around 1,500 member companies, located in 13 Latin American countries, which are grouped in six organisational chapters: Colombia, Ecuador, Peru, Costa Rica, Pacific region and Dominican Republic.

The following questions were considered in a survey of BASC member companies:

- Which security measures are commonly implemented by the BASC member companies?
- What is the cost for companies to join the BASC program?
- Which security measures turn out to be most appealing, that is, low cost and high efficiency?
- Which types of benefits the member companies have obtained while implementing the BASC program?

This paper provides an overview of the survey questionnaire and the survey sample. The study findings follow by describing the implemented security measures, the cost of implementing the BASC program, the expected benefits versus obtained benefits related to the program, and a qualitative cost-benefit analysis. Next, the relationship between the number of security measures and the number of obtained benefits is analysed, followed by the analysis of the relationship between implemented applicable security measures and obtained benefits. A 2x2 matrix for classifying security measures in high-low cost versus high-low effectiveness is provided. Finally, other study findings are summarised, followed by conclusions.

The study was carried out by two doctoral assistants at Ecole Polytechnique Fédérale de Lausanne (EPFL) and Hautes Études Commerciales (HEC) University of Lausanne, supervised by two professors at those universities. The President and several Directors at the BASC organisation played a critical role in facilitating the study process between the research team and the BASC member companies.

The survey questionnaire

The study involved a five-page questionnaire, addressed to 800 BASC member companies in ten different countries. The questions were created in collaboration with BASC management and fine-tuned in a validation exercise with five BASC chapter directors from different countries. The final document contained 20 questions which followed the structure presented in Figure 1 below.

![Figure 1. Summary of questionnaire structure](image)

Sample characteristics

Out of 800 companies contacted, 102 completely answered surveys were received (response rate of 13% and sample error of 10%). The survey covered 78% of the member countries; represented companies involved in different international trade-related operations (that is, manufacturers, traders, port operators, logistics service providers and others providing support services such as security monitoring and rental vehicles); covered different company sizes, and annual turnovers; and included companies which were certified in different years. Figure 2 presents the distribution of respondent companies in terms of four different categories: country of main operations, commercial activity, size, and annual turnover.

![Sample characteristics diagram](image)
Implementation of various security measures

Most of the existing voluntary supply chain security programs comprise general guidelines which describe the security measures that should be implemented to become a certified company. However, there is much variability regarding the level of detail in which these measures are presented. For instance, BASC is a program with one of the most highly detailed security standards lists, with approximately 100 security measures. Nevertheless, the researchers believe that most of the security measures can be implemented in different ways. There is still a great degree of freedom in the implementation of security standards, depending on each company’s particular situation.3

A consolidated list of security measures which summarised the most recurring measures in nine different security initiatives worldwide was established. The resulting 25 measures were classified into the following five categories: Facility management, Cargo management, Human resources management, Information management, and Business network and company management systems. It should be noted that the list contains some measures that are not explicitly required in BASC security standards guidelines (the use of cargo inspection and tracking technology, the use of international standards for data management, etc.). However, they may contribute to the creation of an appropriate supply chain security management system within companies or as part of other existing or future security programs.

Respondents specified which security measures from the consolidated list were implemented by their companies. For each implemented measure, they were asked to explain if it was done as a requirement for obtaining BASC certification, or if it was in place prior to the certification process. For each of the non-implemented measures, respondents were asked to explain if they had plans to implement them in the near future or if the measures were not applicable for their company.
Figure 3 below presents the implementation reasons and the future plans for each security measure and ranks them from the most to the least implemented by BASC companies.

**Figure 3. State of implementation for set of security measures (sample size 102)**

The most popular measures include employee hiring and exit processes, which cover background checks, exit interviews, etc. Defining organisational roles and responsibilities regarding security management; protecting the facilities with basic tools and methods; protecting the business information; and arranging security training programs belong also to the top five most popular implemented security measures. At the other end of the spectrum, one has more technology orientated security measures, including access/presence control technologies; cargo and vehicle anti-tampering and tracking technologies; international data standards; and using cargo inspection technologies. One possible reason for their unpopularity could be the higher cost than in some of the more popular measures; in addition, a large number of companies claimed that these five least popular measures are not applicable at all for their companies.
BASC implementation costs

Respondents were asked to estimate the total cost incurred to implement the security measures required by the BASC certification and the annual cost of maintaining these measures. These costs include expenses caused by the implementation of the security measures themselves (security training courses, investments in technology or facility reinforcement, etc.), and the administrative fees that the World BASC Organization charges their members for covering organisational running costs. These administrative fees can vary from 800 USD to 2,500 USD for the certification and from 800 USD to 2,000 USD for annual maintenance. The tariff varies according to the socio-economic situation of the country and the economic sector to which the company belongs. BASC certification is valid for one year and can be renewed after passing a second security audit.

Table 1 below presents the average certification and annual maintenance cost for companies with different turnovers.

<table>
<thead>
<tr>
<th>Annual turnover</th>
<th>Number of companies</th>
<th>Implementation Cost</th>
<th>Annual Maintenance cost</th>
<th>Maintenance/certification cost</th>
<th>Certification cost/Turnover</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 50,000</td>
<td>4</td>
<td>28,625</td>
<td>2,888</td>
<td>10%</td>
<td>≥ 57%</td>
</tr>
<tr>
<td>50,000 - 500,000</td>
<td>13</td>
<td>17,176</td>
<td>8,539</td>
<td>50%</td>
<td>3% - 34%</td>
</tr>
<tr>
<td>500,000 - 1 Million</td>
<td>13</td>
<td>13,585</td>
<td>6,698</td>
<td>49%</td>
<td>1% - 3%</td>
</tr>
<tr>
<td>1 Million - 5 Million</td>
<td>25</td>
<td>61,820</td>
<td>15,826</td>
<td>26%</td>
<td>1% - 6%</td>
</tr>
<tr>
<td>&gt; 5 Million</td>
<td>35</td>
<td>52,742</td>
<td>28,484</td>
<td>54%</td>
<td>≤1%</td>
</tr>
<tr>
<td>Total</td>
<td>90</td>
<td>34,790</td>
<td>12,487</td>
<td>38%</td>
<td></td>
</tr>
</tbody>
</table>

Except for companies with a turnover between 50,000 and 500,000 USD, the average cost of certification appears to be positively related to turnover (increase in turnover, higher cost of certification). However, the increase in the cost of certification is not proportional to the increase in turnover. For instance, for companies with an annual turnover of less than 50,000 USD the certification cost was on average more than 57% of their turnover, while for companies with a turnover between 50,000 and 500,000 USD this percentage decreases drastically to a range between 1% and 34%. One more relevant result is that the maintenance cost in relation to the certification cost (see column: Maintenance/certification cost) appears to be smaller (10%) for companies with turnovers of less than 50,000 USD per year and higher (on average 45%) for companies with higher turnovers. It could be concluded that the certification cost appears to be more expensive for companies with small annual turnovers (less than 50,000 USD) while the maintenance cost is proportionately more expensive for more companies with higher turnovers.

The company internal work required throughout the certification process, average values for time required and human resources spent are presented in Table 2 below.

<table>
<thead>
<tr>
<th>Time</th>
<th>Average Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Months necessary for certification process</td>
<td>8</td>
</tr>
<tr>
<td>Total hours of work for certification</td>
<td>2,337</td>
</tr>
<tr>
<td>Resources</td>
<td></td>
</tr>
<tr>
<td>Number of employees involved in certification process</td>
<td>48</td>
</tr>
<tr>
<td>Number of employees involved / Total employees</td>
<td>23%</td>
</tr>
<tr>
<td>Time per resource</td>
<td></td>
</tr>
<tr>
<td>Hours per person</td>
<td>49 (~ 6 working days)</td>
</tr>
</tbody>
</table>
Benefits of joining the BASC program

Based on an exhaustive supply chain security literature review, 16 potential benefits related to voluntary supply chain security programs were identified and classified in the following three categories: (I) Direct security benefits (II) Benefits for the company’s efficient functioning, under normal conditions, and (III) Benefits for the company’s efficient functioning, under high alert or post-disaster conditions. Respondents were asked to evaluate the degree of importance of these benefits for their companies. Figure 4 presents the list of benefits ranked from the most to the least important based on the respondents’ answers.

Figure 4. Potential security programs benefits ranked by degree of importance (sample size 102)

There was general agreement regarding the most and least important benefits. More than 70% of respondents considered that the top five most important benefits belong to categories I (Direct security benefits) and II (Benefits for the company’s efficient functioning, under normal conditions). An average of 60% of companies considered the direct, indirect cost savings and the reduction of insurance premiums benefits of medium or low importance.

On the other hand, there is certain disagreement concerning benefits such as quick recovery from general disasters and better Customs regulations and processes compliance, where 50% of respondents believed that these are highly important and the other half believed that their importance is medium, low or not applicable for their company.
Furthermore, respondents were asked to explain which benefits they were expecting when the company engaged in the certification process versus which benefits they gained after the certification was complete. Figure 5 presents, as percentages, the expected and obtained benefits.

**Figure 5. BASC expected vs obtained benefits (sample size 102)**

<table>
<thead>
<tr>
<th>Expected vs Obtained Benefits</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-smuggling</td>
<td>I. Direct Security</td>
</tr>
<tr>
<td>Anti-theft</td>
<td>I. Direct Security</td>
</tr>
<tr>
<td>Anti-loss and damage</td>
<td>I. Direct Security</td>
</tr>
<tr>
<td>Anti-counterfeit</td>
<td>I. Direct Security</td>
</tr>
<tr>
<td>Reduction of insurance premiums</td>
<td>I. Direct Security</td>
</tr>
<tr>
<td>Improve company image and credibility</td>
<td>II. Efficiency under normal conditions</td>
</tr>
<tr>
<td>Reduce supply chain vulnerability</td>
<td>II. Efficiency under normal conditions</td>
</tr>
<tr>
<td>Improve supply chain performance</td>
<td>II. Efficiency under normal conditions</td>
</tr>
<tr>
<td>Fast/stable/predictable border crossing process</td>
<td>II. Efficiency under normal conditions</td>
</tr>
<tr>
<td>Better Customs regulations &amp; processes compliance</td>
<td>II. Efficiency under normal conditions</td>
</tr>
<tr>
<td>Direct cost savings</td>
<td>III. Efficiency under high alert/post disaster conditions</td>
</tr>
<tr>
<td>Indirect cost savings</td>
<td>III. Efficiency under high alert/post disaster conditions</td>
</tr>
<tr>
<td>Quick recovery from direct disasters</td>
<td>III. Efficiency under high alert/post disaster conditions</td>
</tr>
<tr>
<td>Preferential treatment in alert situations</td>
<td>III. Efficiency under high alert/post disaster conditions</td>
</tr>
<tr>
<td>Quick recovery from general disasters</td>
<td>III. Efficiency under high alert/post disaster conditions</td>
</tr>
<tr>
<td>Preferential treatment in post-disaster situations</td>
<td>III. Efficiency under high alert/post disaster conditions</td>
</tr>
</tbody>
</table>

Figure 5 shows that attainments were higher or very close to expectations for most of the direct security benefits – excluding for reduction of insurance premiums; for some supply chain efficiency related benefits (such as the reduction of the supply chain vulnerability and the improvement of the supply chain performance) and in particular, to improve company image and credibility, which was the most expected and the most attained (expected by 85% and obtained by 90% of the respondents).

In contrast, it seems that benefits related to cost savings, direct and indirect, efficiency under high alert/post disaster conditions and facilitation of border crossing operations (fast/stable/predictable border crossing process and better Customs regulations and processes compliance) were on average less attained than expected. These results show that although the implementation of the BASC program has been useful in increasing security and, as a consequence, in improving corporate image, it is difficult to translate this apparently less risky situation into cost savings.

For those benefits where expectations were met, the main interest is to understand which security measures contributed to achieving them; this will be discussed in the next section. For those benefits where the expectations were not met, three potential explanations can be considered: the benefits would in reality require broader security investments than the companies had made; the benefits would require different security investments than the companies had made; companies had not been exposed to disruptions or alert situations where they would have been able to prove the effectiveness of the security measures.
Qualitative cost-benefit analysis

There is an analogy between investing in a supply chain security management program and paying insurance fees, that is, one can choose to invest in preventing security incidents as well as in developing a fast recovery capability in case of an incident – one where the company could have had a say in, for example, theft; or one which is independent of the company’s actions, for example, port closure. With the insurance instruments, by investing in advance one can become (economically) better prepared for fast recovery after an incident happens, naturally subject to the insurance terms and conditions. However, carrying out an accurate, quantitative cost-benefit analysis for security investments is not an easy task, due to several reasons, such as quantifying the investment returns in case ‘nothing happened anyway’ is difficult; and being able to show exactly which security measure contributed to which benefit is not an exact science.

One way to categorise the types of possible benefits for security investments is to determine:

• cost savings from reducing the probability or avoiding the occurrence of undesirable events (that is, decrease in theft, counterfeit, loss or damage rates, reducing supply chain vulnerability, avoiding customs fees, loss of goodwill)
• secondary positive effects on existing operations (that is, improving supply chain efficiency due to better control and traceability, indirect cost savings)
• improvements to the company’s situation in relation to external actors (that is, acquisition of new clients, preferential treatment at borders).

Benefits for the first category result in avoiding costs; therefore, their quantification requires the calculation of the potential costs that could be incurred if an undesirable event occurs. For the second and third categories, quantifiable benefits should be the result of more income, due to an increase in turnover or a decrease in operational costs. In both cases, the quantifiable benefits are not easy to estimate. In the first case, the estimated benefits will never be exact if the undesirable event never occurs, and in the second case, the benefits will be the result of other interacting variables (marketing function of the company, product quality, etc.) so it will be difficult to identify which part of the increased income corresponds to the security investments.

BASC member companies illustrate the existing difficulty in quantifying security investment benefits: while 93% of the respondents were able to estimate the total cost of implementing and maintaining BASC, only 40% were able to quantify some benefits and very few were able to explain where they originate.

Large variations were found when comparing the value invested in security with the value of the obtained benefits of the companies that quantified their benefits. Out of this set of 34 respondents, half obtained benefits which were inferior or equal to their investment and the other half obtained benefits which vary from double to ten times the total cost of implementation and maintenance. Additionally, although several companies invested similar amounts of money in security, they obtained significantly different quantifiable benefits. Even if some respondents were able to explain the reasons for such benefits, it did not sufficiently explain why companies making apparently the same effort obtained very different results.

Despite these difficulties, the researchers provide some explanations for the variation in the results:

• There are significant obstacles when quantifying benefits stemming from the prevention of an undesirable event. The estimation of these benefits depends on the perceived degree of risk faced by the company and the program’s capacity to reduce the probability that this risk will occur. For instance, the same security measure will reduce the probability that an undesirable event will occur within companies facing high risks and others facing low risks to the same extent. However, the riskier companies will perceive higher benefits because the potential savings from preventing undesirable events are higher than for the low risk companies.
• There might be relevant differences in the items that were considered to calculate the cost of implementation and maintenance by each company.
• The relationship between costs and benefits might depend on the situation of the company. For instance, a company where several security standards were implemented prior to starting the certification process will incur reduced costs in comparison to that which starts from zero level.
• The size of quantifiable benefits can depend on many variables. For instance, on the implemented security measures, on the maintenance activities or on the execution of any additional efforts. Better understanding of the connections between such variables could provide important insights to analyse the relationship between costs and benefits for security investments.

**Relationship between number of security measures and obtained benefits**

As discussed in the previous section, there are multiple barriers to quantifying and explaining the potential benefits derived from the investments in security programs. Not being able to quantify the benefits creates obstacles to justify the investments. Not understanding the connections between cost, security measures and benefits makes it difficult to create cost-effective security programs. In this section, this problem is assessed by exploring whether any relationship exists between the number, type and cost of the implemented security measures and the number and type of obtained benefits.

In simple terms a security program consists of a list of security measures. Given that, in principle, each security measure reduces the probability of occurrence of a certain identified risk, it could be argued that the more security measures are implemented, the more benefits will be obtained. Results presented in previous sections indicate that BASC member companies have followed this same logic while trying to implement as many measures as possible.

To test this hypothesis, the number of implemented measures was graphed (Figure 6) against the number of obtained benefits for each company. However, the graph shows that it is not possible to establish any significant positive or negative association between these two variables. For instance, there are several companies which implemented the same number of measures and while one obtained the maximum number of benefits (16), the other obtained zero benefits.

**Figure 6. Relationship between number of security measures and number of obtained benefits**
In order to avoid the potential bias given by the fact that not all benefits and not all measures are applicable for all companies, the following two percentages were graphed one against the other: the number of implemented measures out of the total applicable for each company, and the number of obtained benefits out of those that were expected by each company. Figure 7 shows that, in this case, neither is it possible to say that there is a positive relationship between the number of security measures and the number of obtained benefits.

Figure 7. Relationship between implemented applicable security measures and obtained benefits

The same graphic was done adding several control variables such as company’s main activity (Logistic service provider or manufacturer), size (large or SME), main reason to implement the program (security or image), commercial relationships with US and/or EU, and number of measures implemented from each category (facility, cargo, human resources, information and business partners management). Once again, it was not possible to establish any pattern or significant association for any of the analysed groups of companies.

Given that it was not possible to establish any robust connection between the global efforts made in security (represented as number of implemented measures) and the global effectiveness of these efforts (represented as the number of obtained benefits), the next step was to analyse independently the potential connection between effort (represented as cost of implementation) and effectiveness for each security measure.

Classification of measures in terms of cost and effectiveness

Respondents were asked to qualify each measure in terms of their implementation cost and efficiency in improving security. Two five-point Likert scales were used by respondents to qualify each security measure in terms of these two properties. Table 3 presents the different values and the corresponding meaning.

Table 3. Qualitative scales to qualify security measures in terms of cost and effectiveness

<table>
<thead>
<tr>
<th>Implementation cost</th>
<th>Effectiveness to improve security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = 0 – 2,000 USD</td>
<td>1 = Very low effectiveness</td>
</tr>
<tr>
<td>2 = 2,001 – 10,000 USD</td>
<td>2 = Low effectiveness</td>
</tr>
<tr>
<td>3 = 10,001 USD – 50,000 USD</td>
<td>3 = Medium effectiveness</td>
</tr>
<tr>
<td>4 = 50,001 USD – 100,000 USD</td>
<td>4 = High effectiveness</td>
</tr>
<tr>
<td>5 = &gt; 100,000 USD</td>
<td>5 = Very high effectiveness</td>
</tr>
</tbody>
</table>
Once each measure was evaluated separately in terms of cost and effectiveness, analyses were carried out to establish which type of relationship exists between the cost of implementation and the effectiveness of security measures. Providing answers to this question could provide essential insights to designing cost effective security programs. For instance, if effectiveness is positively related to the cost of the measure, companies with higher investments in security will be more likely to achieve higher security enhancements. On the other hand, should such relationships not exist, the creation of a cost effective supply chain security program would only require implementing low cost and effective security measures.

Most of the answers indicated that all the 25 measures are low cost and high effective. Figure 8 shows the percentage of answers for each possible combination between cost and effectiveness for all the 25 measures. It can be observed that 61.7% (= 9.1% + 13.6% + 14.7% + 24.3%) of the answers point out that all the measures cost between 0 and 10,000 USD and are highly or very highly effective.

**Figure 8. Number of answers per possible combinations of cost and effectiveness**

The analysis of joint cost and effectiveness answers doesn’t provide much information about the differences in cost and effectiveness for the 25 security measures. However, by studying the cost and the effectiveness separately, it was possible to establish how cost-effective each security measure is in relation to the others. In order to do this, each security measure was ranked in terms of cost (from the one which was considered more expensive to the one which was considered cheaper by the higher percentage of companies) and effectiveness (following the same logic as for cost). Then these two ranks were combined in Figure 9, where the measures are classified into two levels of cost (low and high) and two levels of effectiveness (low and high).
No linear positive relationship between cost and effectiveness was found. On the other hand, four main groups of security measures which account for inverse and identical combinations of cost and effectiveness levels were identified. For instance, there are six of the 25 security measures which present a LOW implementation cost and HIGH effectiveness in relation to the others (for details, see measures in group II). In contrast to this group, five of the 25 measures present the opposite combination: HIGH implementation cost and LOW effectiveness (for details, see measures in group III).
Types of measures comprising each cost-effectiveness group

A closer analysis of the type of measures that comprise each of the identified cost-effectiveness groups shows that there are certain types of measures which dominate for some groups or are completely absent. For instance, the HIGH cost and HIGH effectiveness group is comprised only of facility management and information management measures. The LOW cost and HIGH effectiveness, as well as the LOW cost and LOW effectiveness group are comprised of measures from all categories, except from facility management. Finally, the HIGH cost and LOW effectiveness group is comprised mainly of measures related with cargo management, and some related with business networks and management systems and facility management. Figure 10 presents the percentage of different types of measures that comprise each cost-effectiveness group.

Figure 10. Types of measures comprising each cost-effectiveness group

It is interesting to see that those groups where the cost is high have higher concentrations of measures from the same type, contrary to the low cost, which tend to have measures from almost all the categories. These results suggest that measures related to facility management are more likely to be costly to implement and less effective than the others.

In addition, understanding why certain measures are less effective or more expensive than others, and understanding if it is possible to transform them into better performing security measures, could provide important insights for the design of future cost effective supply chain security programs. Figure 11 illustrates the potential strategies to enhance a set of measures which comprise a security program.
Up to this point, some insights have been presented regarding the relationship between the effort (cost) and effectiveness of the investments in security. However, the successful implementation of a supply chain security program should not only aim to identify the lowest cost and most effective security measures, it should also give priority to those measures that can contribute to creating the benefits that are of highest importance for the company. In order to achieve this goal, it would be desirable to identify any existing strong connections, that is, statistically significant associations, between certain benefits and security measures.
Sample connections between security measures and benefits

It should be noted that the necessary statistical analysis used in this study is not included in this paper. However, Table 4 presents some potential connections that were reported by respondents when asked about the most important benefits obtained by their companies and the corresponding measures that were implemented to achieve them.

Table 4. Samples of connections between benefits and measures identified by some respondents

<table>
<thead>
<tr>
<th>Measures implemented</th>
<th>Obtained benefits</th>
<th>Type of benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logistics process control, information management on-time and collaboration with authorities</td>
<td>Anti-smuggling and anti-theft</td>
<td>Direct security</td>
</tr>
<tr>
<td>Supply chain traceability, identification and control of process responsibilities (knowing who does what, at what moment)</td>
<td>Anti-loss and damage</td>
<td></td>
</tr>
<tr>
<td>Document revision and training employees to detect and report anomalies</td>
<td>Decrease containers theft</td>
<td></td>
</tr>
<tr>
<td>Document protection and process supervision</td>
<td>Better process control, processes bottlenecks and mistakes reduction</td>
<td>Supply chain efficiency</td>
</tr>
<tr>
<td>Use of security seals, supervision of deviations in vehicles travel times, access control with bar code system</td>
<td>More control over operations, personnel, documents and cargo</td>
<td></td>
</tr>
<tr>
<td>Access control (working with closed doors), registration of visitors, adequate information management, monitoring of vehicles 24 hours, use of security seals</td>
<td>Improve internal organisation, decrease in disruptions and hence, insurance premiums</td>
<td></td>
</tr>
<tr>
<td>Creation of strategic alliances, risk evaluation of clients and suppliers, adequate employee selection process, establishment of security best practices agreements with clients</td>
<td>Increase of 24% of the business, increasing the turnover by around 2 million US dollars</td>
<td>Company image</td>
</tr>
<tr>
<td>Inspection of containers and vehicles while in storage (this company has used this extra security activity to sell their clients a corporate image which promotes very high security standards)</td>
<td>Client recognition of improved security level; differentiation from competitors</td>
<td></td>
</tr>
</tbody>
</table>

These results suggest that supply chain efficiency related benefits are the result of certain security measures which contribute to security and at the same time, create operationally desirable conditions that are essential for improving efficiency. For instance, some respondents explained that certain security measures reduced the time and variability of certain logistics operations and improved cargo visibility and control, which together contributed to the reduction of the vulnerability of the supply chain. Others reported an improvement in logistics processes and level of service, which contributed to the improvement of supply chain performance. In spite of these examples, which connect certain measures and benefits, there were several respondents who argued that the obtained benefits were the result of all the implemented measures and they were not able to establish any relevant connections between single measures and single benefits.
Conclusions
This paper presents the first broad survey study carried out within a voluntary supply chain security management program. The BASC program appears to be a successful sample of a business alliance, which was initiated with a specific security goal of reducing narcotics smuggling from a high risk geographic area to the rest of the world, and later expanded to become a general supply chain security management program. The paper shows empirical data about the costs, efforts required and effectiveness of this sample security management program.

The study concluded that benefits of such a program are not likely to depend on the number of security measures, and that security effectiveness is not linearly nor positively related to the cost of security measures. However, it was possible to identify security measures which appear to be highly effective and low cost in comparison with the other measures, and vice versa. Estimating the quantified cost of implementing the BASC program was done to some degree, but quantifying the benefits turned out to be a more difficult task, clearly subject to future studies.

The documented experience of BASC member companies provides an important reference document for the future development of supply chain security standards for global, end-to-end supply chains. The lessons learned with the BASC program should be carefully analysed by the ongoing regional and global standardisation initiatives, including the European Union’s Authorised Economic Operator (EU AEO), the World Customs Organization’s Framework of Standards to Secure and Facilitate Global Trade (the SAFE Framework of Standards), and the International Standards Organization’s Supply chain security management system (ISO28000).

In order to have successful future supply chain security management standards, it must be ensured that the participating companies get tangible benefits for their efforts, with one of the main benefits being preferential treatment at border crossing points, both in normal conditions and in high alert and post-disaster situations. How to do this remains a key topic for future supply chain security research as well as governmental policy development work.

Acknowledgements
FNS (Fond National Suisse de la Recherche) as the main sponsor of this study.
BASC: Ms Mayra Hernández de Cavelier, President, World BASC Organization. Mr Diego Castillo, BASC Chapter Pichincha, Mr Stephen R Tiernay, BASC Dominican Republic, Jose Luis Hernández Valentino, BASC Chapter Carabobo, and John Reinberg, BASC Chapter Ecuador; and all BASC member respondents to the study.
EPFL: Professor Michel Bierlaire.
HEC University of Lausanne: Professor Erkko Autio.
HEC University of Lausanne – IUMI: Professor Jean-Claude Usunier, Mr Vincent Vandersluys.
HEC University of Lausanne and CBRA: Mr Vladlen Tsikolenko.

References
Bodner, Nathan 2003, ‘The weakest supply chain link (five categories of food manufacturing supply chain risks)’, *Food Logistics*, no. 42.


Official program documents


New Zealand Customs Service 2003, Secure exports partnership: important information for applicants, December.


TAPA 2000-2005, Freight suppliers’ minimum requirements, January.


World Customs Organization 2005, Framework of Standards to secure and facilitate global trade (SAFE Framework), June.

Endnotes


The study preparation and results were presented on slides at:

The study results were presented on slides at PICARD 2007, 2nd Conference on WCO Research Network, Hintsa presented study results, Brussels, Belgium, March 2007.

For a copy of the full version of this study, please contact either the Editor-in-Chief at editor@worldcustomsjournal.org, or basc-study@cross-border.org.

2 See Gutiérrez, Wieser & Hintsa 2006 for the detailed questions.

3 See Gutiérrez, Wieser & Hintsa 2006 for more details.

4 See Gutiérrez, Wieser & Hintsa 2006 for more details.
Ximena Gutiérrez

Ms Gutiérrez has a Master of Science in Industrial Engineering from Universidad de Los Andes, Colombia (2000). After working for a few years in the Logistics Service Providers industry, she moved to Switzerland to obtain an Executive Masters in Management of Logistical Systems from Ecole Polytechnique Fédérale de Lausanne (EPFL) (2003). In 2004, Ms Gutiérrez joined the College of Management of Technology at EPFL as a Research Assistant, where she is conducting studies in the fields of Logistics, Supply Chain Security and Cross-border Operations Management, mainly in studies coordinated and led by the Cross-border Research Association.

Juha Hintsa

Juha Hintsa is a Senior Researcher in global supply chain security management, with an MSc (Eng.) in Industrial Management and Artificial Intelligence. He is one of the founding partners of the Global Customs Research Network, and the founder of the Cross-border Research Association (CBRA) in Lausanne, where he undertakes research into various aspects of supply chain security management in close collaboration with several multinational corporations.

Philippe Wieser

Dr Philippe Wieser obtained his Diploma of Engineering in Mechanics at EPFL in 1977 and his PhD in 1981. After a few years working in an engineering consulting company, he joined EPFL as a Lecturer. His fields of research and teaching deal with logistics and information systems, and integrated logistics. Since May 2000, Dr Wieser has been the Executive Director of IML: International Institute for the Management of Logistics (EPFL-Lausanne and ENPC-Paris). Dr Wieser teaches in EPFL-Lausanne (Master and Executive Master MSL) and ENPC-Paris (Executive Master). He is author and co-author of more than sixty publications.

Ari-Pekka Hameri

Dr Ari-Pekka Hameri is Professor of Operations Management at University of Lausanne, Switzerland. He has been involved with numerous EC-funded and other international research projects dealing with lead time reduction and supply chain management. He has published over fifty articles about industrial IT, and production, project and supply chain management in international management and science journals.