Supply Chain Security Management for Business Continuity Management

Case study: Steel Industry

Virgil POPA

Faculty of Economic Sciences
Valahia University of Târgovişte
Târgovişte, Romania
virgilp51@yahoo.com

***Abstract*—Given the current global crisis and haoticism the newest interests in Supply Chain Management (SCM) are directed to Supply Chain Security Management (SCSM) that can support sustainable development and realizing the benefits of collaborative chain management. This new endeavor is linked to strategic development center, a sustainable business whether they are up-stream or down-stream and that are materialized in Business Continuity Management (BCM). Supply chain security is a supply chain where various measures have been taken to guarantee a certain level of security. Security measures can be taken with regards to physical flows, information flows and money flows (one or all the three flows of supply chains). Supply Chain Security consists in physical and preventive measures and facilities security of cargo for example and non-physical security and preventive measures in information security (cyber security) or security of personnel. World Economic Forum (WEF) and other international institutions and governments discuss issues regulations (for example, President Obama rules) or global standards (ISO 28000). We present best practices from standards that are applied in different organizations in the steel industry in Romania entered a global market full of risks, disasters and acts of terrorism.**

Keywords— Supply Chain Management (SCM); Supply Chain Security Management (SCSM); Business Continuity Management (BCM); vulnerability; emergency plan; reaction plan.

I. INTRODUCTION

Supply Chain Security Management (SCSM) is a relatively new discipline, thus lacking introductory and tutorial papers. The recent concerns on security in global supply chains are driving the introduction of new security initiatives, standards and measures to such an extent that they are becoming an integral part of supply chain management.

Security, its demands and constraints, constitute obstacles (logical and physical barriers) in the flow of supply and distribution. These "barriers" created by a perceived increased need for security, or political reasons, reduce the reaction capacity and the physical and economic performance of the company. Integrating the security dimension into the logistics strategy, organization and operations has become a new challenge for supply chain management. [1]

The recent security concerns have led to the development of multiple initiatives and potential solutions to enhance security in international supply chains without affecting efficiency. Businesses, governments and researchers are tackling the problem from different perspectives and by using several methodologies. However, inherent complexities such as the large quantity and diversity of the actors involved in international supply chain processes, and the need to identify cost-effective security measures, have generated multiple academic research questions in the domain of SCSM.

The first pure SCSM paper was published at MIT [2], a few months after the infamous terrorist attacks in September 2001 and it is one of the manners of research SCSM – Transportation and Logistics field. Other ways of developing involvement SCMSM is that of Lee & Wolfe [3] who saw the entire chain Supply Chain Management and centered philosophy of Total Quality Management applicable in all processes of supply chain management.

Lee and Wolfe (2003) describe three generic requirements or measures from a security perspective for creating a secure freight system: 1. Assuring integrity of conveyance loading, documentation and sealing; 2. Reduce risk of tampering in transit (with comprehensive monitoring of tampering and intrusion); 3. Provide accurate, complete and protected information about shipments to those who need it in a timely manner. Better visibility and control is the focal theme found in most of the measures and requirements to mitigate the security risks. Supply chain security risks can be reduced or eliminated by increasing the visibility of the supply chain, providing transparency with regards to (the status of) physical flows, information flows and money flows [3]. The transparency of a supply chain increases when more, timely and especially quality information becomes available throughout the entire chain.

The third approached is Christopher & Peck [4] in

Chain Risk and Vulnerability concerning for building resilient supply chain who presents the sense-and respond organization and supply chain to respond to unforeseen events in an agile manner. Preventive and detective measures are part of the sensing phase, while detective and corrective measures are part of the responding phase. Furthermore, learning should be incorporated to make security measures effective in the longer term.

II. GLOBAL AND GOVERNMENTAL CONCERNS FOR RISK MANAGEMENT AND SUPPLY CHAIN SECURITY

One of the first concerns centered SCSM was the American government, although at a good time after 9/11 events but concerned about the condition of security of the global business state US citizens.

Through the National Strategy for Global Supply Chain Security (the Strategy), articulate the United States Government's policy to strengthen the global supply chain in order to protect the welfare and interests of the American people [5]: "Our focus in this Strategy is the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructures by which goods are moved from the point of manufacture until they reach an end consumer, as well as supporting communications infrastructure and systems. The Strategy includes two goals: Goal 1: Promote the Efficient and Secure Movement of Goods; Goal 2: Foster a Resilient Supply Chain. To achieve this we will prioritize efforts to mitigate systemic vulnerabilities and refine plans to reconstitute the flow of commerce after disruptions".

A second important document is the overall impact governmental EU-US agreement of 23 June 2011 concerning the declaration of cooperation in terms Supply-Chain Security [6]. "Our cooperation effort should be applied in multilateral for a as well as in bilateral EU-U.S. relations. A robust response should aim to: 1. Prevent the unlawful transport of dangerous and illicit material throughout the supply chain; 2. Protect critical elements of the supply chain system from attacks and disruptions; …. 5. Build the resiliency of the supply chain".

A comprehensive approach to risk in the supply chain had a World Economic Forum over several events in Davos. In Perspective for Supply Chain Security Management WEF express [7]: "The main external risk factors of the supply chain are: natural disasters, political conflict situations, sudden demand shocks, restrictions on import / export, terrorism". Systemic risks within supply chain and transport networks are characterized by an unexpected trigger event and a network setup that cannot absorb the shock and knock-on effects. The initial event results in a cascading disruption or failure across regions or industries.

However, prediction of specific disruptions is felt to be less important than having the resiliency in place for effective response, no matter what the cause. While highlighting industry robustness in the face of recent shocks, experts identified the vulnerabilities of most concern that limit the resilience of supply chain and transport networks [8].

III. SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN

This Publicly Available Specification specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management [9].

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. Reviews shall include assessing opportunities for improvement and the need for changes to the security management system, including the security policy and security objectives and threats and risks.

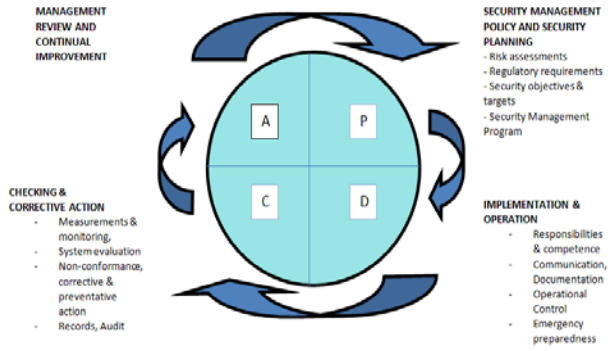

Fig. 1. Elements of the security management system [9].

The elements of security management system (Fig. 1) are organized in the Deming wheel mood which can realize a continuous improvement step by step. Records of the management reviews shall be retained. Input to management reviews shall include: results of audits and evaluations of compliance with legal requirements and with other requirements to; which the organization subscribes; communication(s) from external interested parties, including complaints; the security performance of the organization; the extent to which objectives and targets have been met; status of corrective and preventive actions; follow-up actions from previous management reviews; changing circumstances, including developments in legal and other requirements related to its security aspects, and; recommendations for improvement.

The survivability of organizations within a supply chain depends largely on the resilience of their suppliers and customers. As a result, incorporating resilience, and improving the resilience of an organization within the supply chain, must be focused both within the organization and externally on its suppliers and customers.

ISO 28002 Development of Resilience in the Supply Chain [10]: "Organizations across the globe are rapidly developing risk management and resilience programs to address uncertainty in achieving their objectives. There is a strong demand for standards and best practices, as organizations are seeking assurance that their suppliers and the extended supply chain have planned for, and taken steps to prevent and mitigate the threats and hazards to which they are exposed. To assure resilience in the supply chain, organizations must engage in a comprehensive and systematic process of prevention, protection, preparedness, mitigation, response, continuity and recovery".

IV. BUSINESS CONTINUITY MANAGEMENT

Business continuity plans will ensure that the organization can continue to deliver a minimum level of service in its critical functions in the event of any disruption.

"The strategy requires senior managers to demonstrate that they have considered the need for business continuity planning to cover each functional process within their area of responsibility. The focal point for the production, coordination, validation and review of the council's business continuity activity strategy will be the Corporate Governance and Risk Officer". [11]

Corporate business continuity is closely linked to corporate risk management and this strategy should be read in conjunction with the council's Risk Management Strategy. The basic principles of the Business Continuity Strategy have been accepted by the Corporate Management Team, Governance and Audit Committee. This Strategy applies to all parts of the council as all areas play a key role in maintaining product/service delivery. The requirement to plan applies to activities identified as critical through the council's business continuity methodology and agreed by the Corporate Management Team, Governance and Audit Committee.

Business continuity management (BCM) can be defined, according to Morris [12], as: "A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities".

A. Good Practices and International Standards. BSI – Standard 100-4 Business Continuity Management

Business Continuity Management [13] "is a discipline that prepares an organization for the unexpected. It is a management process that provides the framework for building resilience to business and service interruption risks, responding in a timely and effective manner to ensure continuity of critical business activities, and ensuring the long term viability of the organization following a disruptive event". The purpose of business continuity management is to ensure that critical business processes are interrupted only temporarily, even in critical situations, and the organization will exist after the appearance of serious damage. Ruptures of business processes can have different causes, namely, effects. To illustrate the events described in the Business Continuity Management framework we provide a brief explanation of the terms: "emergency", "crisis" as they were understood and used in businesses.

"Emergency" is an event in which an organization's processes and resources do not work properly. These processes and resource availability cannot be restored in the time established by the framework.

"Crisis" is understood as a situation deviated from the normal state, which can occur at any time, regardless of protective measures implemented in the company or government organization in question and cannot be solved by normal operational and organizational structures. Emergency situations that may affect the continuity of business processes can develop and turn into crises.

B. ISO 22313– Societal Security – Business Continuity Management Systems

This International Standard for business continuity provides guidance based on best international practice for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented management system that enables organizations to prepare for, respond to and recover from disruption [14].

It is not the intent of this International Standard to imply uniformity in the structure of a BCMS but for an organization to design a BCMS that is appropriate to its needs and that meets the requirements of its interested parties. Business continuity management system (BCMS) is that part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

V. CASE STUDY: S.C. OȚELINOX S.A.

Oţelinox was established on June 01 1974, following an international auction won by Japanese companies NISSHIN STEEL CO Ltd.

For manufacturing of cold rolled stainless steel strips and sheets and DAIDO STEEL Co for manufacturing of hot rolled small profiles and wire rod. Now the company is privately held and its main shareholder (94.25%) Samsung Deutschland GmbH.

The company has implemented several best management practices including: integrated Standards (9001, 14001, 18001), 5S, Six Sigma, Kaizen. It is currently implementing Lean Manufacturing and prepares strategic base for operations excellence EFQM award. The company has developed a risk management system which is still based on

ISO 31000, but it is a good start in terms of internal good practices, taking into consideration all the risk sources for ISO 28000 and 28002.

The company was argued before the classic approach - identifying organizational risk, based on ISO 31000 and quality management instrumental in FMECA, and especially for domestic incidents. The literature and practice management deepens and environmental risks suppliers (up-stream) and customers (down-stream) and business environment.

In our paper-based on the organization studies determines us to go towards what ISO 28002 is based - event risk in organization and processes upstream and downstream with the processes in the value chain of the organization's component supply chain management (Source - Make - Delivery). Incident management through a plan of urgent and truer reactive plan is proposed in the appendixes, for example an action plan (Table I), reaction plan (Table II). Making a resilient chain / safe driving can generate a system of goals and Key Performance Indicators to be monitored and managers in dashboards. The organization had enough major incidents which resulted in a managerial proactive (disappearance almost instant a Chinese client who take about 25% of the products one of the lines fabrication, what caused organization that took over much of this sheet steel to realize an investment extreme high, in a ward of precision in achieving flatness sheet form mini sizes thickness and width, a different incident). Not even parallels what says ISO 28000 - theft was up -stream from a supplier from Italy.
Following the approach of the Balanced Scorecard strategic management can be seen that there is some performing explained by KPI (Table III) of this approach started by identifying internal risks (mostly) and external ones. By preparing a response plan can also determine business continuity management.

VI. CONCLUSIONS

Even though the organization has already developed tools such as: Reaction Plan and Plan for Response to emergency situations, as an improvement opportunity it is recommended drafting an integrated Plan on business continuity starting with the Balanced Scorecard and ISO 22313 for the response to major risks plans which offer a systemic vision. Suggestions: 1. the establishment of a department or office in an existing department, to handle security risk management; 2. based on the Pareto principle (also known as 20/80 principle) to develop discussions with main suppliers and customers (Integrated in the Supply Chain) to achieve a system of security management throughout the chain of organizations that are coordinated from Germany's Korean subsidiary Samsung [15,16].

REFERENCES

[1] J. Hintsa, Ph. Wieser, X. Gutierrez, A.-P. Hameri "Supply Chain Security Management: An Overview", HEC University of Lausanne, Ecole Polythecnique Fédéral de Lausanne Cross-border Research Association (CBRA), Lausanne, Switzerland.

[2] Y. Sheffi, "Building a Resilient Supply Chain", Harvard Business Review Supply Chain Strategy, Volume 1, Nr. 8, Octombrie 2005.

[3] H. Lee, M.Wolfe, "Supply Chain Security Without Tears", Supply Chain Management Review, Vol. January/February 2003.

[4] M. Christopher, H. Lee, "Mitigating supply chain risk through improved confidence", International Journal of Physical Distribution and Logistics Management, 2004, Vol. 34, No 5.

[5] The White House – National strategy for global supply chain security, Washington, January 2012.

[6] EU-US_Joint_Statement_Protocol, "Joint statement on supply-chain security", http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/eu_us_joint_statement_protocol_en.pdf

[7] World Economic Forum, New Models for Addressing Supply Chain and Transport Risk, 2012.

[8] World Economic Forum, Resilience and Dynamism: How countries survive and thrive, January 2013

[9] ISO 28000 – Supply Chain Security Management Systems, 2007. [10] ISO 28002:2011, *Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use*.

[11] Western Australian Government, Business continuity management guidelines – second edition, 2009, Risk Cover.

[12] N. Morris, "Business continuity management strategy policy," Zurich, Management Services Limited, February 2011.

[13] BSI –Standard 100-4 Business Continuity Management, Federal Office for Information Security, Bonn, Germany, in www.bsi.bund.de.drundschutz.

[14] ISO 22313– Societal Security – Business Continuity Management Systems, 2012.

[15] D. Vissarion, and V. Popa, « «Supply Chain Risks Management (SCRM). Case study: Steel Industry – OTELINOX", Supply Chain Management Journal, Volume 5, Issue 1, 2014, Valahia University Press https://drive.google.com/file/d/0B4dxx8_8gi7lbFoxaFhjMDZ5Zkk/view

[16] V. Popa, "Supply Chain Risk Management. Creating The Resilient Supply Chain", Supply Chain Management Journal, Volume 4, Issue 1, 2013, Valahia University Press https://drive.google.com/file/d/0B4dxx8_8gi7lLUhsbTF4RnFXNkE/view

Emergency Plan (Examples) **Appendix 1**

No	Identified emergency situations	Preventive actions	Responsible Preventive actions	Emergency actions	Responsible Emergency actions
1	Extreme weather phenomena: a. Thunderstorms, heavy rain, tornadoes b. Floods caused by extreme weather production (Events may cause damage to building roofs, rainwater pipes, clogged sewers, flooding of technological lines, basements of buildings or hydraulic cellars, electrical	- Personnel training in order to know the color codes for weather alerts and warnings and to take preventive measures ; - Preventive inspection of the condition of rainwater pipes and collection pipes; - Check the condition of sewers and clean them - Establish the areas / locations where the water infiltration may occur due to various cases, determine the	SU responsible/ Chiefs of workplaces Chief of Administrative Team/ Chiefs of workplaces Chief of Energy team and utilities Chiefs of plants / Chiefs of work places	-Announce the chief of plant and the duty officer; -Announce the management of the company; - Personnel from the affected line in collaboration with the maintenance staff (under the command of the chief of the workplace) initiate measures to limit the consequences and to remove the event, according to the "Action plans in case of emergency' ;	Chiefs of the workplaces *(foremen / team chiefs)* Duty officer / Chief of plant Chief of workplace
2	Extreme weather phenomena: a. Thunderstorms, heavy rain, tornadoes b. Floods caused by extreme weather production (Events may cause damage to building roofs, rainwater pipes, clogged sewers, flooding of technological lines,	- Personnel training in order to know the color codes for weather alerts and warnings and to take preventive measures ; - Preventive inspection of the condition of rainwater pipes and collection pipes; - Check the condition of sewers and clean them - Establish the areas / locations where the water infiltration may occur due to various cases, determine the	SU responsible/ Chiefs of workplaces Chief of Administrative Team/ Chiefs of workplaces Chief of Energy team and utilities Chiefs of plants / Chiefs of work places Chiefs of work places	-Announce the chief of plant and the duty officer; -Announce the management of the company; - Personnel from the affected line in collaboration with the maintenance staff (under the command of the chief of the workplace) initiate measures to limit the consequences and to remove the event, according to the "Action plans in case of emergency' ;	Chiefs of the workplaces (foremen / team chiefs) Duty officer / Chief of plant Chief of workplace
3	Exceptional situations: a. War b. Embargo c. Revolution (Probability of such events is very low.)	- Maintenance of the alarm sirens, of the ALD shelter in functioning state - Ensuring safety lighting (in plants and buildings); - Maintenance of telephone lines; - Set working instructions in case of war; - Train the personnel regarding the usage of warning signals ; -Establishing the evacuation assembly points and conducting evacuation exercises with the employees.	Chief of maintenance Chief of Maintenance Chief of Administrative General Director ES Responsible/ Chiefs of workplaces	- Turn on the electric sirens (after receiving the notification and turn on agreement from local authorities); -Taking the decision to evacuate the personnel on site; - Telephone announcement about the evacuation of the employees at the site (following the decision of the General Director).	Duty officer / Chief of Administrative General Director HR Director/Chief s of workplaces

Reaction Plan (Examples) **Appendix 2**

Potential situations that may result to nonconformities	Emergency actions taken	Responsible
1. Raw material defects: Failure to comply with the quality requirements of raw materials identified in various stages of processing in the production flow with repercussions concerning fulfilling in time the orders.	- it is blocked the nonconformity coil that presents defects from raw material; - in case of blocking of at least 3 raw material coils in over 24 hours that comes from the same supplier and shows the same type of defect is prepared and sent an RNAC to the supplier; - in the next 24 hours the stocks of raw materials from the supplier involved is analyzed by QC&CS and Processes Programming &Control teams and in consequential the coils that may have the same problem are blocked and isolated; - are requested information from supplier about quality of raw material in stock; - if the answer of the supplier imposes this, is requested the emergency replacement of raw materials affected.	QC inspector QC engineer responsible for complaints of raw material QC engineer & Processes Programming &Control QC engineer responsible for complaints of raw

2. Failure to satisfy capability conditions, variations in product characteristics **3.** nalyzed distribution characteristics does not meet customer requirements / standard values	- roducts that do not meet customer requirements, or are not within the OTELINOX standard value are blocked; - he nonconforming product are 100% inspected and it is decided the way it can be handled according to the "Nonconformities control" procedure, code …; - here are established corrective actions for all non-compliant products in order to eliminate the causes that generated nonconformities; - ll records of non-compliant products are kept within QC&CS team; - or all non-compliant products management staff of the department from where are generated is informed.	material Operator QC inspector Plant chief QC engineer

Comparative analysis of Key Performance Indicators for 2013-2015 **Appendix 3**

From Balanced Scorecard of OTELINOX Company

Name of process	**No.**	**Performance Indicator**	**Indicator value 2013 year**	**Indicator value 2014 year**	**Indicator value 2015 year**	**Target 2016**
Client support	**1**	Orders for analysis: up to 4 days for at least 98% of total commands	99.20%	99.40%	99.60%	Minimum 99.95%
	2	For analysis applications offer: up to 13 working hours for minimum 95% of applications offer	91.72%	93.30%	93.70%	Minimum 95%
	3	The first response to receiving a complaint: working for up to 6 hours 99,5% of complaints	96.18%	99.24%	99.50%	Minimum 99,5%
	4	The final response to receipt of all necessary details investigate by a maximum of 36 hours for 99,5% of complaints	96.40%	99.31%	99.50%	Minimum 99,5%
Delivery	**1**	Delivery date fixed	x	99.03%	98.71%	98%
Raw material supply **……** **……** **…...** **……** **……** **……**	**1**	Ensuring raw material for the second rolling mill of the first and the third rolling mill.	94%	132%	115.60%	100%