Security Issues Associated with Material Flow in Supply Chain of Manufacturing Industry

Shujun Zhang[1], **Kevin Hepashi**[1], **Martin Wynn**[1]

Department of Computing, Business School, the University of Gloucestershire
The Park, Cheltenham, Gloucestershire GL50 2RH, UK
szhang@glos.ac.uk

Abstract: The aim of this paper is to investigate and find out all major security issues and relevant solutions within the material flow in supply chain (SC) in order to help companies to deal, to reduce and to prevent those security issues occurring in their supply chains. In the paper relevant supply chain management (SCM) concepts, security issues and possible solutions are firstly discussed. Then, a number of solution frameworks are proposed through in-depth analysis and evaluation of the security issues in material flow in SC. Finally, a case study in manufacturing industry in UK is presented to demonstrate their security issues and solutions.

Key Words: Supply chain, security, management, material flow, e-supply chain

1 Introduction

Supply Chain Management has become an unavoidable task for suppliers, manufactures, distributors, or other supply chain partners in order to meet the increasing complexity of their customer requirements in a more efficient way. Hence, some companies have made great efforts into directly managing their supply chain themselves, and others have outsourced to professional third party service providers, which leads to more complex and longer supply-chain. Whether a company chooses either to manage their supply chain by their own SCM department or outsource to professional vendors, coordination and collaboration are fundamental to enabling a company to be more responsive and efficient in meeting market or customer requirements. In addition, web-based technology is increasingly being applied to SCM in order to achieve optimum efficiency. However, there are various security issues when raw materials, inventory and finished goods go through a longer and complex supply chain. In material flow, the raw materials, inventory and the finished products can be stolen or faked. In information flow, supply chain information, such as the procurement, billing, order and inventory information could be at great security risk from security attacks due to increased information sharing and information transferring caused by collaborated relationship and usage of web based technology. In addition, financial information, and other financially relate transactions and activities may be in security danger. More seriously, even a small security problem could cause a significant loss for the supply chain as supply chains become more integrated, and thus security attacks can more easily spread to affect other chain partners than was the case hitherto if proper protection is not in place. Thus, an investigation of security issues concerning SCM can give suppliers, OEMs, intermediaries, customers, and even third party service providers more guidance on potential security issues concealed in their business and the possible solutions they can use. So it is important to investigate various security issues and possible solutions to these issues. Due to the limitation of the paper length, this paper will only report our work on the security issues in materials flow of supply-chain in a typical manufacturing company.

2 Discussions of Supply-chain and Its Management

2.1 Supply Chain and Its Management

There are a number of definitions of SC [1-3]. According to Chopra and Meindl [1], the supply chain can be defined as being the dynamic and constant flow of information, product and funds between different stages. Ayers [2] has defined the supply chain as not only involves the physical movement of goods but also the information, money movement and the creation and deployment of intellectual capital. Another point worth to mention is that, from the Shaw's [3] view, the three flows within the supply chain should carry equal weight when the total effectiveness of a supply chain is considered because they form a series of processes all linked together to form a chain and the three flows are in fact intermediates in a continuous process.

Supply chain management can be understood from two different aspects [4]. **SCM as a managerial process:** *"SCM is the process of managing relationships, information, and materials flow across enterprise borders to deliver enhanced customer service and economic value through synchronized management of the flow of physical goods and associated information from sourcing to consumption."* **SCM as a managerial philosophy:** *"The extension of integrated behaviour to incorporate cus-*

978-1-935068-18-1 © 2010 SciRes.

tomers and suppliers through external integration is called supply chain management." However, people often confused the definition of SCM with the definition of logistics management. Bowersox *et al* [5] defined logistics management as being concerned with the movement of inventory and information flows. Nevertheless, Waters [6] added that, although logistics is responsible for the material, inventory flow through a supply chain, it is defined somewhat more narrowly for the movement within a single organisation, while SCM takes a broader view of such movements.

2.2 Discussion of SCM and Internet

To understand how the Internet in particular has influenced SCM, Chopra and Meindl [1] first defined e-business as the execution of business transactions via the internet, and thus any supply chain transactions that involve e-business also include the three flows. Kolluru and Meredith [7] further pointed out that the Internet enables better integration and such integration allows companies to monitor and forecast demand more accurately and allocate assets more productively, while providing a more responsive customer service along the supply chain. However, Chou *et al* [4] further argued that the Internet as an information communication medium does represent some security risks as this information may be the most critical asset for an organization's supply chain partners. Shih and Wen [8] further revealed that doing business via web-enabled supply chain networks can open more doors to some security threats.

3 Analysis and Evaluation of Security Issues Associated Material Flow

3.1 Discussions of Security Issues Associated with Materials Flow

The security issues associated with material flow have brought increasing attention from various participants along the supply chain. The key security issues and possible solutions associated with material flows can be summarised as (1) supplier security risks, (2) risks of damaged goods, (3) theft, (4) counterfeiting, (5) food safety and dangerous goods and (6) transportation. Due to the limitation of the paper length, the analysis and evaluation for food safety and dangerous goods will be omitted.

3.2 Supplier security risks and their solutions

Firstly, the security issue associated with suppliers is increasing as the supply chain becomes more complicated today. Suppliers whether or not can deliver required materials on time and in the correct quantity and quality can significantly influence the manufacturing and production process, and influences the flow of materials to the next stage of the supply chain. As Rice [9] has stated, reliability of supplies is a fundamental source of supply chain security. So, supplying is critical start point for a successful flow of materials. It has been found that collaborating, sharing resources, and working toward common goals can help companies not only reduce the problems caused by material flow security, but also address other critical issues such as quality. However, a more preventative approach may be needed in order to better detect any supply risk to material flow and to identify solutions in the first place. Thus, in this paper, a six step approach to assessment and prevention of supplier security risks during the material flow process is suggested as follow, which can be called supply chain risk model (SCRM): The first step is to define and identify the potential supplier security risks; the second step is to filing these risks in the company's database; the third step is to screen to detect those defined security risks; the fourth step is to treat these risks; the fifth step is to continually monitor those security risks. Then, these five step procedure will be guide, support, and monitored under the company's incident handling and contingency planning procedure to become more standardised approach to reduce any supplier relate security risks.

In addition, bar code has been used to secure supply the correct freight in the past. Nowadays, RFID could widely be used to replace the bar code for secure 'supply and loading the correct freight'. As RFID have the advantages of no line of sight required, multiple parallel reads possible and individual items instead of item class identification in practice [10]. Furthermore, operators along the supply chain may still need to set material handling standards, such as better information sharing systems between partners to ensure greater security of 'supply and loading the correct freight'.

3.3 Risks of Damaged Goods and Their Solutions

Generally, for the SCM, risks of damaged goods do exist. For instance, electronic goods in the supply chain often face various hazards, and these hazards not only damage these electronic goods, but also have a strong impact on the profitability of the business. This view can be supported by the research of Magad and Amos's [11] who found that damaged goods represented about 12% of customer service complaints. As a result, improvement in receiving and storage activities can help to minimise damage by utilizing effective handling procedures, equipment and training of employees, various packaging solutions such as use of micro-fluted corrugated cartons and boxes to minimise the shock hazard, compression hazards and vibration hazard causing damage during the transportation and storage process.

3.4 Theft and Its Solution

Theft security issues have always been a major concern with regard to material flow. Principally, cargo theft has become the central concern for material flow security issues within the SCM. This view can be supported by the research finding that 41% of respondents believe cargo security has posed the greatest challenge to supply chain security.

In general, the theft often happens during the transportation or storage process. On the one hand, in order to prevent such theft during the transportation process, investment in technology and in training of staff has been suggested. It is strongly recommend that more attention should be paid to invest in security technology in order to minimise theft during the transportation process. Besides, driver training also needs to be addressed to combat theft security issues during the transportation process. On the other hand, advanced technologies and information systems can also play a major role in combating theft. Many firms have used satellite tracking GPS to provide in-transit visibility and thus enable operators to have a real-time visibility of the flow status of their materials. The development of Radio Frequency Identification Device (RFID) could even support fleet managers to enable them to visualize their latest status of materials and to detect any thefts. However, to only rely on the above two solutions is not sufficiently enough to secure the material flow. Thus it is necessary to integrate above possible solutions with a well-design procedure adopted in practice of supply-chain management.

3.5 Counterfeiting

Counterfeiting becomes another increasing security concern for the flow of materials of the supply chain. However, these security issues may only serious affect certain types of supply chains, such as the electronic goods supply chain and high value goods supply chain. Counterfeiting has become an increasing concern along the pharmaceutical supply chain. In general, it can be noticed that both the computer technology and supply chain structure has contributed to the increase of counterfeit material flow.

Auto-ID technology, such as bar coding and RFID, can be widely used to execute the track and trace function and to give more visibility in order to secure the material flow. However, to successfully prevent counterfeit material flow within some supply chains, various parties in the supply chain may still need to think about the use of packaging technologies and compliance with government regulations.

Furthermore, 3D (three-dimensional) code technology can be a good solution for counterfeiting risks. The 3D code is much more difficult to be identified and copied than 2D bar code and even RFID. The 3D code is based on designed secret geometrical information, and this information is saved and stored in a firm’s database as a verifying key against counterfeiting. However, the application of the 3D code is still in its early stages, but we believe that the uses of this powerful technology for combating counterfeiting will increase rapidly in the not-too-distant future due to its effectiveness.

Table 1 security issues and solutions within material flow

Key Security Issues	**Solutions**
Supplier Security Risks	• Collaborate Relationship • New SCRM Model • Bar code, RFID • Better Information Sharing Systems
Risks of Damaged Goods	• Proper designed handling procedure • Packaging technologies
Theft	• Invest in physical assets and driver Training • Invest in advanced technologies for security control (GPS, RFID) • Operate 6 steps for theft prevention
Counterfeiting	• Packaging technology • Auto-ID technology • Government regulations and others • 3D codes
Food Safety and Dangerous Goods	Food Safety • Technologies: bar code, RFID, and packaging technologies; freshness indicators; thermochromic ink and laminates Dangerous Goods • Technologies, Management, Staff Training

Nevertheless, overall the solution we would suggest against counterfeiting is an amalgamation of packaging technologies, auto-id technologies, government regulation and more advanced 3D code. In summary, Table 1 listed various security issues and proposed solutions.

4 Case Study: Findings and Discussion

4.1 Introduction to Case Study – ASP Aero UK

In this section, a case study is presented. The objective is to investigate how real industrialists manage the security issues associated with their SCM, and also to test the usage and validity of the solutions discussed in Sections 3. The study of ASP Aero UK (ASPAUK) was mainly based on interviews with its IT Manager, through a set of interview questions. It mainly manufactures bearings for aerospace industrial applications, racing equipment and provides engineering solutions for the racing industry. It belongs to the ASP Group, which is a leading global supplier of rolling bearings and lubrication systems. In the UK, the ASPAUK operation has already formed a SCM of its own, and at the same time, it has integrated with other subgroups of the ASP. So ASPAUK is a typical manufacturing company for investigating secure issues of the supply chain.

4.2 Supplier Security Risks

ASPAUK has determined that the quality of supplier has become extremely important for the successful flow of material through the whole supply chain. From our study, it was found that they placed the quality of their suppliers' material at the top of the supplier management agenda. ASP shared some of their production planning information systems with their major suppliers, such as a shared MRP (manufacturing requirements planning) system to make sure that suppliers had sufficient time to prepare for delivery. It is worthy to point out that it is fundamentally required to minimise errors in the aerospace industry. So supply chain entities collaborate with each other to reduce any supplier-related risks. For quality of supply issues, ASPAUK has following solutions:

- All the material supplied has to be checked in the laboratory before the order is made up.
- Everything made from these materials must have a serial number, and thus every single item made from that material can be listed and identified, and reported to the supplier immediately in order to prevent any further quality problems.
- More important is that all suppliers have to be approved by ASPAUK's customers by conducting various supplier risk assessments. However, the use of the "customers' approval" as a solution to combat supplier security risks in practice should not be sufficient to guarantee the continuous quality of supply, as it can only be a good method of reducing the total occurrence of bad quality of supply by selecting only qualified suppliers. Thus, we would like to recommend SCRM model for ASPAUK to adopt as a formal and continuous process to prevent any potential supplier security risks occurring in the future.

It was also identified that in order to combat the supplier security issue, ASPAUK did apply the "collaborate relationship", and "information-sharing with suppliers" as discussed in Section 3. In other words, the solutions proposed earlier do have validity in a real industrial environment.

Another finding is that ASPAUK only produces when customers place orders, without keeping too much stock. Potentially, such a strategy could result in ASPAUK suppliers being under pressure when ASPAUK places a big order, as their suppliers may also want to minimise their cost in relation to the inventory. In the long term, this conflict could potentially damage their relationship with their suppliers if their orders are not managed properly, and could become a big supplier security issue for ASPAUK. Yet, this issue not having been brought out in the interview, we would like to suggest that ASPAUK probably needs to review their forecasted demand information and sales information with their suppliers more closely, and not just rely on the MRP.

4.3 Risks of Damaged Goods and Counterfeiting Risks

The risk of damaged goods and counterfeiting risk are two other potential risks recognised by ASPAUK. The incoming materials, such as bars and rings, cannot be easily damaged, but if damage does occur, it can only be noticed in the production process (IT manager of ASPAUK). ASPAUK currently uses simple packaging technology, such as plastic sheets, to wrap their materials. However, this solution seems to be too reactive to solve the "risk of damaged goods". It is recommended that the use of more packaging technology at least for finished products.

One good thing in ASPAUK is that it widely uses a "designed handling procedure" and other standard operation procedures (SOP). So it can be noticed that the proposed "designed handling procedure" and "packaging technology" in Section 3, have validity in the real supply-chain environment.

4.4 Risks of Counterfeiting

Counterfeiting has been regarded as another general security issue in the aerospace industry. The solutions from ASPAUK include applying packaging technologies, application of the barcode and complying with government regulations. They include:

- *Overt Technologies and Covert Technology*
  The ASP group uses a special dye in the ink and the packing boxes sent to their customers. This ink can be scanned using ultraviolet light to tell whether or not the boxes are real ASP boxes. Also, each box has a seal to prevent tampering and products being counterfeited.
- *Auto-ID Technology*
  A 2D code provided by their supplier, Rolls Royce, to protect against counterfeiting.
- *Government Regulations*
  Follow strict government regulations and guidelines in exporting to certain countries, to reduce the risk of counterfeiting.

Obviously, these three solutions show consistency with the proposed solutions in Section 3. In other words, the proposed solutions have their use and validity in a real industrial environment. Nevertheless, although a 2D code is in use, there may sometimes be errors and it is prone to damage and easy to copy. This could be another security issue for ASPAUK to consider at the moment. So it is suggested to use 3D codes. In addition, the use of RFID technology to combat the counterfeiting can also be suggested.

5. Conclusion and Discussions

The main security issues and solution frameworks of material flow of a typical supply chain have been analysed, evaluated and particularly examined in the case study of a manufacturing company in UK.

It was found that most of the principal security issues lie in the material flow of SCM. This is mainly due to increasing use of standard IT security management by supply chain participants to reduce information flow security risks, and this is especially true for large companies. However, whether it concerns large or small companies, the major security issues related to material flows has been found to be: 'Supplier Security Risks', 'Risks of Damaged Goods', 'Counterfeiting Risks', and 'Theft', although the seriousness of each security risk and the solutions used can be different for different companies due to the material involved, the product nature, and the industry that the company is in.

Nevertheless, regarding solutions for those security issues mentioned above. the development of 'collaborate relationships', 'better information sharing systems', the 'New SCRM model', 'Vendor Management' and 'Suppliers being approved by customers' is often being used by manufactures to reduce the 'Supplier Security Risks'. Regarding solutions for 'Counterfeiting', manufactures often use 'patent protection', 'keep the core material ingredients',' packaging technologies', auto-ID technology of 2D code', and 'government regulations' to solve counterfeiting problem. Whereas, 'RFID technology' and '3D code' are also being suggested for use in the future with regard to this security issues. Regarding solutions for 'Risks of Damaged Goods', manufactures often use 'proper handling procedure' and 'packaging technologies'. Finally, regarding solutions for 'Theft', manufactures often use 'stock check', 'change of factory procedures for internal theft' and using 'Third Party Logistic Service Providers'. However, apart from those common solutions, the fundamental requirement to secure the material flow has been found to make sure that the supply chain is visible or traceable.

Reference

[1] S Chopra and M Meindl. Supply Chain Management: strategy, planning, and operations, 2nd edition. Upper Saddle River, N.J, 2004.

[2] J B Ayers, J.B. Handbook of Supply Chain Management. , St Lucie Press, Alexandria, VA, 2001.

[3] M J Shaw. E-business Management: Integration of Web Technologies with Business Models. Boston Kluwer Academic Publisher, 2003.

[4] D C Chou, X Tan and D C Yen. "Web technology and supply chain management", Information management & computer security, 2004, Vol.12 No.4, pp.338-349.

[5] D J Bowersox, D J Closs and M B Cooper. Supply chain logistics management, 2nd international edition. London: McGraw-Hill, 2007.

[6] D Waters. Logistics: an introduction to supply chain management. Basingstoke: Palgrave Macmillan, 2003.

[7] R Kolluru. and P H Meredith. Security and trust management in supply chains, Information Management & Computer Security, 2001, Vol.9 No.5, pg.233-245.

[8] S C Shih and H J Wen. E-enterprise security management life cycle, Information management and computer security, 2005, Vol.13 No.2, pp.121-134.

[9] B J Rice and F Caniato. Building a secure and resilient supply network, Supply Chain Management Review, 2003, Vol.7 No.5, pg.22.

[10] H Jung, F Chen and B Jeong. Trends in supply chain design and management: technologies and methodologies. London: Springer, 2007.

[11] E L Magad and J M Amos. Total materials management: achieving maximum profits through materials /logistics operations, 2nd edition. London: Chapman & Hall, 1995.