INFORMATION SECURITY IN LOGISTICS COOPERATION

Tomasz Małkus
31-510 Cracow ul. Rakowicka 27, Cracow University of Economics, malkust@uek.krakow.pl
Sławomir Wawak
31-510 Cracow, ul. Rakowicka 27, Cracow University of Economics, wawaks@uek.krakow.pl

Keywords: information security, supply chain, logistics outsourcing, ISO 27001 standard, contract
Abstract: Cooperation of suppliers of raw materials, semi-finished products, finished products, wholesalers, retailers in the form of the supply chain, as well as outsourcing of specialized logistics service require ensuring adequate support of information. It concerns the use of appropriate computer tools. The security of information in such conditions of collaboration becomes the important problem for parties of contract. The objective of the paper is to characterize main issues relating to security of information in logistics cooperation.

1. Introduction

Rapid changes in the business environment, including the changing expectations of customers caused the increasing importance of logistics activities to achieve competitive advantage. The ability of quick supply of goods to clients became the important factor of success on markets. Such circumstances resulted with both, the integration of logistics activities between companies producing and supplying goods to clients, as well as the growth of interest in logistics outsourcing. At the same time, toegether with objective to increase the rate of delivery of goods to customers, the supply chain concept is treated as a way to reduce the cost of storage and movement of goods.

Organizing cooperation both between suppliers of raw materials, semi-finished products, finished products, wholesalers, retailers in the form of the supply chain, as well as outsourcing of specialized logistics service it is important to ensure adequate support of information. It requires to use appropriate computer tools. The security of information in such conditions of collaboration becomes the important problem for parties of contract.

The objective of the paper is to characterize main issues relating to security of information in logistics cooperation. Presentation of nature of such cooperation, importance of information security, as well as guidelines, how to ensure information security in logistics collaboration are included in the paper. Mentioned guidelines are based on well known ISO 27001 standard.

2. Characteristics of logistics cooperation

The supply chain concept was created as an alternative to the traditional perception of the relationship between suppliers and clients, which was characacterised by antagonisms, using their own bargaining power, and consequent transfer of obligation to incurr the increased costs to a partner [6]. The development of supply chain can be also treated as a consequence of the need for cooperation in pursuing partners' objectives in an environment, where the frequency and scale of change has significantly increased. This approach to cooperation decisions about design and development of individual companies should take into account the relationship with other units on the market. Although the regulations of law impose on each company to draw up a proper documentation of its effects of performance, however, these results are usually dependent on both, the solutions within the enterprise, as well as the achievements of other cooperating parties.

In the supply chain cooperation, concerning production and delivery of products to clients, the relationship between achievements of individual enterprises play a special role. This approach is related to the necessity to adapt methods of delivery, as well as subsequent after-sales service to the individual needs of each buyer. The fulfillment of these expectations is difficult, because suppliers want to provide fast inventory turnover and at the same time to ensure low operating costs.

Considering the requirements of information systems, supporting the supply chain it should be noted, that the achievement of sufficient flexibility to changing clients expectations depends mostly on close cooperation of suppliers and flow of relevant information between these units. Fast and undistorted customer service, in accordance to their expectations is also difficult without the exchange of information between final buyers and distributors, which allows on one hand quick ordering, affecting the production and supply planning, as well as information on changes of preferences, and on the other hand informing notifying clients on the status of their orders. It should be emphasized, that suppliers seek to maintain more complete control of their own business, but planning and coordinating the flow of raw materials, semi-finished products, finished products, waste, recyclable materials, relevant information and financial resources should be carried out in the whole chain.

The role of information in activities of supply chain is reflected between principles of supply chain management, formulated by APICS (American Production and

Inventory Control Society, now organization named as: The Educational Society for Resource Management). Such principles are described in detail in the work of W. Walker [4]:

- velocity – concerns tasks performed from receipt of order to the point of obtaining financial resources for goods supplied to customers, which is associated primarily with the provision of adequate infrastructure,
- variability – associated with reduction of variability, which results with reduction of the need for network inventory, also logistics and quality costs,
- vocalize – concerns ensuring the flow of information between cooperating units, appropriate in the form, place and time – in particular on the demand for finished products, reported by customers, also ensuring an adequate level of inventories of raw materials, semi-finished in each partner's firm, as well as determination of the required terms of deliveries and ensuring cash flow needed for inventories of individual units,
- visualize – associated with the awareness and understanding of expected results of cooperation – related mainly to agreement (contract) of partners, concerning expected results across the chain and the use of appropriate performance indicators,
- value – emphasizing the need to recognize and take into account the expectations of all stakeholders in supply chain operations.

Usually logistics cooperation in the supply chain includes suppliers of raw materials, semi-finished products, finished goods manufacturers, wholesalers and retailers. There is also important role of service providers, involved in the loading, movement, unloading and storage of goods. Cooperation with such companies may be associated with a focus on reducing the costs of contracted services. Taking into account the important role of logistics in achieving competitive advantage the cooperation with providers of logistics service can also be treated as part of the strategy of the client. In the case of wide range of outsourced service, core business of the client may be significantly influenced by the activities of providers.

Basic models of activities of specialized logistic units, which were formed on the basis of the different orientation of the principals, concerning required range of logistics services is presented in one of the studies the IBM Institute for Business Value [1]:

- providers of simple service, such as transport or storage, sometimes taking into account also customs clearance, settlement between the client and the service provider shall be implemented on the basis of transactions,
- units referred to as 3PL (third party logistics) - offering logistics services for client in such areas as procurement, distribution and movement of goods in the manufacturing process, taking into account the packaging, marking goods, warranty and post-warranty, performance of these tasks is similar as in previous case under a contract with the client, specifying mutual expectations, obligations and rights of the parties, the settlement take place on the basis of a fixed rate for an agreed range and quantity of services.
- units named as the LLP (Lead Logistics Provider) – managing logistics activities of several or even all partners cooperating in the supply chain, from suppliers of raw materials, semi-finished products, producers of final products up to deliveries to buyers of finished products, such units operate like the previous primarily on the basis of contract with individual principals, settlement takes place on the basis of a fixed rate for probably range of services, but also participate in the sharing of risks associated with joint ventures, such individuals often rely on the help of other service providers, providing individual types of services, e.g. transport, or shipping,
- units acting as an integrator in the supply chain, often regulate flows (to eliminate "bottlenecks") between cooperating companies in manufacturing and supplying purchasers of products, also referred to as the LLM (Lead Logistics Manager) – in this case a partnership between the client and the service provider is shaped by the terms of the contract between parties, but to a greater extent related to the implementation of joint projects, in which there is both risk-sharing between the client and provider, but also the sharing of benefits after the completion of the project, the benefits of this project are considered as the basic form of compensation for the involvement of the service provider,
- units known as 4PL (fourth party logistics) - a term coined by Andersen Consulting to determine the companies referred to previously as 3PL, that developed offers to a wide range of logistics services, far beyond the transport and storage, such units generally shall cooperate with others, specialized service providers, entrusting them to perform different types of tasks within a comprehensive service harvested principal, 4PL may also have expertise in the field of supply chain management.

Taking into account presented distinction of types of logistics service providers it should be noted, that among them are both, units implementing simple tasks for individual companies in the supply chain, as well as providers of comprehensive logistics service to all participants of the chain. Problem of information security applies to each of cases considered. The differences concern the range of data and information used in cooperation. From the point of view of comprehensive service of all supply chain partners units described as LLP play most important role. It should be noted that their

activities in the supply chain, as well as coordination of subcontractors requires the use of complex information systems that enable the rapid flow of a wide range of data and information.

3. Support of information in logistics cooperation

Logistics cooperation is associated with the use of different computer tools, depending on the scope of information required. The example of description of software offered by SAP, named mySAP SCM can be used to present wide range of types of information used in most complex supply chain cooperation. Names of main components of the software reflect the range of data and information collected, created, used and transferred:

- supply chain planning,
- supply chain execution,
- supply chain collaboration,
- supply chain cooperation.

Data and information useful in mentioned areas, grouped in main functions available are presented in Table 1.

Table 1. Types of information used in supply chain cooperation

Types of actions	Description
Supply chain planning	- supply chain design function enables centralized overview of the entire supply chain, contains key performance indicators, as well as weak links and places of potential improvement, at also supports strategic planning, by enabling tests of various scenarios, concerning the influence of changes in market conditions and customer demand on the results of activities of cooperating parties, - demand planning takes into account historical demand data, causal factors, marketing demand, results of market intelligence, sales objectives, it enables cooperating parties also working on single forecast, - function of supply planning concerns materials management, production, distribution, as well as transportation requirements, also constraints of activity.
Supply chain execution	- materials management function contains inventory and procurement order information, it supports plan-driven procurement, inventory management and invoicing, with a feedback loop between demand and supply to increase responsiveness, - collaborative manufacturing refers to sharing of information, supporting coordination of production and to increase visibility and responsiveness, there is a continuous information flow across engineering, planning and execution for optimization of production schedules across all cooperating parties, - collaborative fulfillment includes global available-to-promise (ATP) feature, that locates finished products, components and machine capacities (in a matter of seconds), it also manages flow of products through sales channels, matching supply to market demand, it results with managing with transportation and warehousing.
Supply chain collaboration	- inventory collaboration hub uses Internet to gain visibility to suppliers and manage the replenishment process, it enables to gain data and information about the status of parts at all plants and to receive alerts concerning too low levels of inventories, as well as to respond quickly, - collaborative replenishment planning (useful especially in the area of consumer goods flow and in retail industry) enables exception-based collaborative planning, forecasting and replenishment process, that allows adding retail partners without a proportional increase in staff, - vendor managed inventory (VMI) enables vendor managed replenishment, without the need of cyclic ordering by client, concerns continuous updating inventory data at the destination point - enterprise portal enables personalized access to a range of information, applications and

	services supported by the system, it uses role-based technology to deliver information to users, according to their individual responsibilities in supply chain network, also the ability to use Web-based tools to integrate third-party systems in the firm's supply chain network should be emphasized, - mobile supply chain management can be treated as supplementary function, it enables planning, execution and monitoring of activities using mobile and remote devices, availability of data and information also should be personalized.
Supply chain coordination	- supply chain event management concerns monitoring of events (supply chain actions) as: issue of pallet, departure of truck, it is especially useful for product traceability, - supply chain performance management enables to define, select and monitor key performance indicators, measuring results of activities and generating alerts in cases of differences, between results and plan

Source: own study, based on: [3].

As presented in Table 1, main users of such information system are suppliers of raw-materials, semi-finished products, final products, wholesalers and retailers. Functions of system allow also the involvement of logistics service providers in the network.

The problem of information security can be analyzed with the transaction cost theory [5], agency theory and incomplete contract theory [2]. According to transaction costs theory, bounded rationality (associated with asymmetry in access to information), opportunism of parties to transaction and the specificity of the assets used in transaction were recognized by O. Williamson as main sources of transaction costs [5]. Using agency theory assumptions it should also be noted that agents typically act for their own benefit and they represent the opportunistic attitude [2], [5]. Considering information security, the use of information needed for the transaction by one party for its own purpose, as well as limiting access of other party to information may be examples of opportunistic behaviour. Limiting access to data and information, as well as the use of data and information for individual purpose of one party are also important factors of incompleteness of contract.

Taking into account the problem of reducing the risks associated with limited access to data and information important for cooperation, as well as improper use of data and information, it is worth paying attention to the role of regulations in the contract, concerning informational support of cooperation (creation of information, use, transfer, access etc.). ISO 27001 guidelines may be useful, as the inspiration in the formulation of regulations concerning the principles of cooperation.

4. ISO 27001 as proposal of basic rules for enhancing information security in logistics cooperation[1]

Development of the information technology accelerates growth of globalization, however, this relationship is two-directional. Global economy affects the ways of thinking about information management. Awareness of this fact among the companies executives grows, but still is insufficient. The major roles in top management decisions are played by economic effects, whereas information security problems are often overlooked.

Correct calculation of the cost should, however, take into account the risk of security problems. The awareness and appreciation for information security of personnel can be significantly less in some countries. Moreover, there should be considered other threats, e.g.: political risk, industrial espionage, intellectual property theft, as well as disaster recovery issues. The cost cutting results also in reduction of audits number in overseas departments. Lack of control can lead to loosening of security procedures, and increase of security incidents.

Information Security Management System (ISMS) is meant to be the answer to such problems. It was first published in 2005 and updated in 2013. Its scope comprises the development of security policy at the strategic level, the evaluation of risks, the determination and implementation of security controls aimed at eliminating threats, and also the monitoring of the system with the aid of internal audits and a management review. It has been reflected in the structure of ISO 27001:2013 standard that comprises of eleven chapters. The first four chapters contain an introduction, a description of the scope of the standard, normative references, and also terms and definitions. Key chapters focus on the organisational context and stakeholders, information security leadership and high-level support for policy, planning an information security management system, supporting it, making it operational, reviewing its performance and corrective action. Such a structure corresponds to other standards established by the ISO that

[1] The chapter presents results of own study based on: [7], [8], [9], [10] and [11].

relate to management systems. Current standard was significantly changed in comparision to previous version. Its structure and clarity of requirements is much higher than in ISO 27001:2005.

The key part of ISO 27001:2013 is Annex A that contains a list of security controls concerning among others: information security policy, system organization, security of staff, assets management, access control, cryptography, physical and environmental security, security of systems operation, communication, development of systems, relations with suppliers, incidents management, business continuity, compliance with the law. The security groups are strictly related to the contents of the ISO 27002:2013 standard, where detailed guidelines concerning the implementation and monitoring of security controls may be found. It should be noted that in many cases the ISO 27002:2013 standard deals with an information technology system, however, in the case of implementing the information security management system, it should be interpreted more broadly, as an information system.

Apart from ISO 27002, implementation of information security management system requires knowledge related to other standards of this family: implementation guidance (ISO 27003), principles of measurement (ISO 27004), risk management methodology (ISO 27005, which refers to ISO 31000).

While developing standards for management systems, the International Organisation for Standardisation complies with the principles of their compatibility and complementarity. Apart from ISO 27001, the most popular standards in this field also include systems of quality management, environment and occupational safety. The compatibility is seen in the application of similar management methods and tools, e.g. principles of supervision over documents and records, the development of organisational policies, carrying out management system reviews, internal audits, identification of non-conformities, corrective actions. This approach makes ISO 27001 standard easier to implement in organizations, which already have certified ISO 9001 system.

Organization's interfaces are particularly vulnerable to information security problems. It is no different in case of cooperation with suppliers. The standard mentions in appendix A six main controls related to information security management in context of relationships with suppliers: - A.11.1.6. Delivery and loading areas, - A.15.1.1. Information security policy for supplier relationships, - A.15.1.2. Addressing security within supplier agreements (contracts), - A.15.1.3. Information and communication technology supply chain, - A.15.2.1. Monitoring and review of supplier services, - A.15.2.2. Managing changes to supplier services.

The main provision of ISO 27001 concerning suppliers is information security policy for supplier relationships (A.15.1.1). This is new requirement, which was added in amendment of 2013. It is expected, that requirements of information security should be agreed between organization and supplier, and also documented. It should reduce risks related to supplier's access to organization assets. This is legal protection, which should be reinforced by additional organizational, technical and IT protection. The organization should identify groups of suppliers, evaluate their access to information, determine and implement restrictions of access which will improve security and at the same time won't worsen conditions of cooperation. Suppliers can influence the business continuity, therefore organization should discern its fault tolerance. In case of close cooperation, it may be desirable to plan staff awareness training not only for own personnel, but also for supplier's employees.

In case of suppliers who are able to access, process, store, transmit information or provide ICT infrastructure, organization should establish contracts to ensure that duties of both parties are known and well understood (A.15.1.2). The common misunderstanding about ISO 27001 controls is their limitation to ICT problems, while most of them relate to whole organization. This control is good example. In fact most of suppliers have access to organization's information, which should be protected (tenders, specifications, technical documentation). Contracts should regulate issues of methods of protection used by both parties, rules of acceptable use of information, intellectual property, dealing with incidents and others.

ISO 27001:2013 introduces new requirement, concerning communication in supply chain management (A.15.1.3). Sensitive information in supply chain can be transferred not only to direct supplier (of goods or service), but also to subcontractors. It is important to implement information security policy, that will embrace not only individual organization and its suppliers, but all participants in the supply chain.

Supplier service should be monitored and reviewed on regular basis (A.15.2.1). Monitoring should include service level, accordance with the requirements of the contract, review of supplier reports, incidents management and audits if appropriate. Monitoring is important part of maintaining supplier relationship. Organization can identify early signals of problems and help solve supplier problems before they induce problems within the organization cooperating with such supplier. To improve communication, both parties should appoint personnel responsible for relationship management and problem solving.

All changes to supplier service should be managed to assure compliance with current information security policies, procedures and controls (A.15.2.2). According to requirements of ISO 27001 new contracts, as well as all changes should be examined in the process of risk assessment.

According to A.11.1.6, organization should supervise delivery and loading areas or other points, where unauthorized persons may try to enter. This includes

identification an authorization of personnel having access to loading areas, reorganization of loading areas and procedures to allow suppliers to operate without need of special authorization, verification of supplies for hazardous materials and violations during transport before further transfer, recording supplied materials, physical separation from outgoing deliveries. Those requirements may entail reconstruction of delivery zones. Suppliers should be informed in advance about procedures of delivery.

Apart from above mentioned controls, cooperating companies should share some common policy of information security incident management, aspects of business continuity management and intellectual property rights.

ISO 27001:2013 focuses on the planning of cooperation processes which includes: identification of risks, determination and implementation of legal, organizational and technical protection means. Information security management system shouldn't be restricted to logistic cooperation, as it will work properly only when all controls will be implemented. Thanks to the system approach and compatibility with other management systems standards, it allows the company to enhance information security in whole organization.

5. Conclusions

The problem of information security is particularly important in changing environment, where individual suppliers of goods (raw materials, semi-finished products, wholesalers, retailers) cooperate with companies, competing in various supply chains. Under these conditions also logistics service providers collaborate with customers, competing with each other. Taking into account the possibility of opportunism in such conditions it should be emphasized, that there is the ability to reduce the risk of incorrect management of information by relevant provisions in the contract. Considering the use of ISO 27001 as a guide to creation of information security system and assuming a positive attitude of parties to cooperation (based mostly on mutual trust and understanding), the following examples of solutions can be also applied:

- submission and explanation of every doubt concerning regulations on informational support of cooperation,
- application of regulations influencing motivation of parties and discouraging opportunistic behavior (mutual benefits resulting from improvements of long-term cooperation, further joint investments, the ability to extend the range of cooperation etc.),
- specification of required compatible, reliable computer tools,
- the ability to renegotiate the terms of contract if (specified) changes influencing information management occur,
- requirement of agreement of any change in terms of cooperation, introduced by each party,
- description of procedures for informing about the changes of those responsible for cooperation in each cooperating company,
- preparation of plans for extraordinary situations (concerns activities of parties taken for adjustment to new terms).

It is important to add, that presented guidelines may be applied to any contract between companies in the supply chain. Among main conditions, affecting the flexibility of contracts and enabling adaptation to changing conditions in the environment of cooperation the possibility of renegotiations and consideration of plans for unexpected situations play most important role.

References

[1] BUTNER K., MOORE D., *Building value in logistics outsourcing*, IBM Institute for Business Value, Available: http://www-07.ibm.com, [10 Jan. 2015], 2006.
[2] HART O., *Firms, Contracts and Financial Structure*, Clarendon Press, Oxford 1995.
[3] JACOBS F.R., BERRY W.L., WHYBARK D.C., VOLLMANN T.E., *Manufacturing, Planning and Control for Supply Chain Management*, Mc Graw Hill Companies Inc, 2011.
[4] WALKER W. T., *Supply Chain Architecture: A Blueprint fir Networking the Flow of Material, Information and Cash*, CRC Press LLC, Boca Raton, London, New York, Washington, D.C., 2005.
[5] WILLIAMSON O., *The Economic Institutions of Capitalism*, The Free Press, A Division of Macmillan Inc., New York, Collier Macmillan Publishers, London, 1985.
[6] WITKOWSKI J., *Precursors of logistics and supply chain management*, Gospodarka Materiałowa i Logistyka, No. 9, pp. 2-5, 2003. (Original in Polish)
[7] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*, ISO, Geneva, 2013.
[8] ISO/IEC 27002, *Information technology - Security Techniques - Code of practice for information security controls*, ISO, Geneva, 2013
[9] ISO/IEC 27003, *Information technology - Security techniques - Information security management system implementation guidance*, ISO, Geneva, 2010.
[10] ISO/IEC 27004, *Information technology - Security techniques - Information security management - Measurement*, ISO, Geneva, 2009.
[11] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*, ISO, Geneva, 2011.

Review process
Single-blind peer reviewed process by two reviewers.