DEVELOPMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM AT THE MEMBERS OF SUPPLY CHAIN

PÁL MICHELBERGER, CSABA LÁBODI *

ABSTRACT: *The paper provides an overview of the role and feasibility of information security in supply chains. After the clarification of basic notions the authors will arrive at establishing requirements postulated for supply chain member companies based on the properties of logistics information systems. The evaluative consideration of major standards connected to the topic of the article may aid the formation of an information security management system that is not necessarily a costly and third-party/advisor audited option, and may open the possibility of fitting it into an integrated logistics system.*

KEY WORDS: *supply chain, SCM, information security, logistics information systems, information security management system*

1. INTRODUCTION

Business transaction and information management between companies is vital for long-term cooperation and strategic partnership. Corporate information systems will thus overstep company boundaries, securing cooperation between strategically linked and allied firms within the supply chain.

Specific company cultures combined with diverse roles fulfilled in the supply chain, continuously shifting corporate business interests and divergent information technologies may cause difficulties for efficient integration; at the same time, information security is of fundamental importance in the creation and maintenance of connections between supply chain members.

* *Prof., Ph.D., Institute of Organisation and Management, Keleti Károly Faculty of Economics, Budapest, Hungary, michelberger.pal@kgk.bmf.hu*
Lecturer, University of Pannonia, Veszprém, Hungary, labodi.csaba@almos.uni-pannon.hu

2. INFORMATION SECURITY

Information is value for the business company, being a basis for decisions and business success. It may be relevant with respect to products, services, technological know-how and available resources as well as business partners – i.e. all the components determining the successful operation of the supply chain. If information is incomplete or missing, inaccurate or dated and if it happens to land in unauthorised hands, major damage may be caused to the company. This means that information must be protected.

Currently this means [7];

- confidentiality (information must be exclusively available to authorised persons),
- integrity (preserving information intact and accurate),
- and availability (authorised users may gain access to the information when necessary).

Information security is a far more complicated domain than IT security. In 1995 John Ward only considered recoverability and backup as the fundamental elements of information security [6]. Today it is not enough to think in terms of firewalls, reliable hardware and well-defined identification systems. A conscious build up of technological background is no longer sufficient. An information security management system will primarily prescribe the management and handling of data storage devices, regardless of the manner in which the information is presented.

Protection functions appropriately if the following are clearly defined: information to be protected, external and internal threats and their risk levels, and finally the necessary instruments and control systems [8].

Information security is especially important for companies that:

- base their operation on information/data, or that are fundamentally determined by information/data in their operation,
- maintain IT links with partners and electronic links determine their external contacts (e.g. logistics organisations),
- are involved in receiving, processing, storing and forwarding data of other (partner, client, etc.) organisations or persons (e.g. banks, insurance firms, data management and storage organisations),
- are involved in the development, setup, launching or implementation of information technology systems (e.g. IT companies),
- conduct research and development activities where the output basically takes the form of information (e.g. research institutes),
- possess, produce and handle confidential personal information (e.g. healthcare institutions).

The aim of information security then is to ensure uninterrupted and undisturbed business handling and reduce damage caused by security events through the regulation of operations. Information security may be reached by introducing safety measures based on the assessment of potential risks. These consist of regulations describing company processes, a corporate structure reflecting these processes and the

regulated use of the appropriate information technology devices (hardware, software and telecommunications devices).

3. THE MANAGEMENT OF SUPPLY CHAINS

The supply chain is a joint system of value added processes and of resources, which involves several companies, starting with the purchase of raw materials and finishing with the delivery of the final product to the consumer. Its various elements comprise suppliers, producers, logistics service organisations, warehouses and other participants of the distribution processes. The operation of the supply chain is primarily determined by the final consumers, which creates common interests for the participants of the chain [2].

According to the definition established by the US Supply Chain Council (SCOR model) a supply chain comprises all activities connected to manufacturing and delivery, from the suppliers' suppliers to the final consumers [14]. The five major processes determining the supply chain are

- planning (supply/demand analysis and the determination of quality, quantity and scheduling factors for products or services);
- sourcing (raw materials, spare parts and cooperational services);
- making (manufacturing of spare parts and assembly);
- delivery (stockpiling, order management, distribution, and serving the final consumers);
- returning (handling faulty or superfluous products and maintenance needs, customer service work).

The application of a sufficiently effective information management system may affect the level of customer requirement satisfaction. As a result of this, we do not see the accumulation of discrete results reached by individual organisations but synergic effects are created in various domains of production due to the allocation of resources. The management of the supply chain means conscious collaboration on behalf of the companies. Its existence is accepted by the participants as a contributing factor to the improvement of their position in competition. The members of the chain are willing to sacrifice their individual, short-term advantages to facilitate the optimal operation of the whole chain. The internal logistics and information systems of the companies are vital for the coordination of inter-company processes [4].

The formation and operation of supply chains may be effected in two possible ways [2]. In the first case a dominant company is capable of directing the activities of the whole chain. The suppliers here are forced to accept the conditions dictated to them from a power position. This is true of information systems, as well. Control of the existence and applicability of an appropriate IT infrastructure is part of the preliminary qualification/assessment of suppliers.

In the other case a real strategic alliance is formed between "equal" partners. The participants are willing to forge relatively long-term cooperation to their mutual advantage but have more difficulty in optimising the operation of the supply chain because individual interests still appear.

4. INFORMATION SHARING IN SUPPLY CHAINS

In supply chains it is essential to provide a few basic company data items to ensure a minimal level of operation (stock levels, sales data and forecasts, customer order status, production and delivery scheduling, capacity data). The other participants of the supply chain must receive clear information and documentation regarding the internal information security requirements of the company.

On a higher level of integration common and integrated information systems are introduced. The members of the supply chain may "freely" access information concerning products, customers and the market situation. In many cases they may get acquainted with partners' internal corporate processes and data previously regarded secret. Empirical surveys show that the number of information technology incidents rises with the multiplication of companies taking part in the supply chain, the advancement of information technology integration and information sharing [5]. In such event the setup of common information security management systems may also be possible.

The effective functioning of supply chains cannot be realised without information technology. It is important for the participating companies to know through what channels (suppliers) with what conditions and costs input arrives, and also what will happen to the output and through what suppliers it will reach the final consumer. Success will come to the supply chain that is faster, more reliable, slimmer and lower-cost than its competitors.

5. SUPPLY CHAIN RISKS

Sources are unanimous concerning supply chain risks. The risk to a supply chain is the event of such potential incident within the supply chain or in its environment (even on its market) which result in danger to customer satisfaction or customer safety. Instead of, and along with, the traditional notion of risk assessment (the size of damage caused by a risk event and the probability of the risk event), the term 'vulnerability' has been introduced.

Risks and the vulnerability of supply chains may be classified into five groups according to their origin [3];

- disturbances in the value-added process (manufacturing, purchasing, storage, delivery, scheduling);
- control (non-existence or failure);
- demand (lack of information, unpredictability, unexpected events);
- supply (unreliability, lack of capacity, vis maior);
- environmental (economic and political events, accidents, natural disasters);

These are complemented by two further risk sources [5].

The internal company organisation (6) is also vulnerable if it does not conform to established processes and does not use information systems well.

Disturbances in cooperation between supply chain members may also occur, in the flow of information as well as that of material. A network composed of several individual companies (7) also leaves space for risk factors (figure 1).

The issue of risk assessment of integrated information systems in supply chains may be approached from the direction of information technology.

Physical protection means creating the appropriate environment and information technology infrastructure to avoid environmental, accidentally or deliberately caused damage.

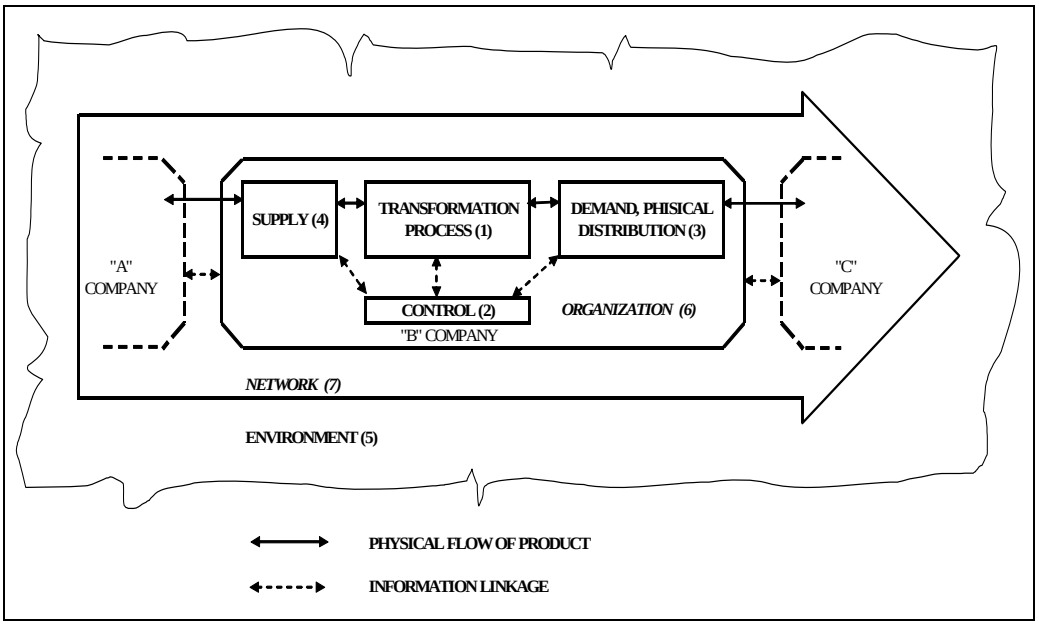

Figure 1. Supply chain risk sources [5]

Logical or "operational" protection includes linked networks, basic applied software (operational systems and database managers), applications (e.g. ERP and EAM systems), and stored data. Work processes are regulated (e.g. diary keeping rules, virus protection activities); user authorisations and competences are defined.

The result of the regulating process is usually a Business Continuity Plan and a Disaster Recovery Plan. The former ensures the availability of business process backup IT resources at given times and functional levels as well as the minimization of damage caused by unexpected events. The latter contains substitute solutions for the case of major damage and events resulting in the breakdown of information technology service. The aim is to facilitate the minimization of negative effects and the fast restoration of original circumstances at acceptable costs.

6. RECOMMENDED STANDARDS

The authors have tried to compile the set of documents sufficient for the launching of an information security management system for a company trying to enter a supply chain. All standard packages are process-focussed and apply the PDCA (plan-do-check-act) model (figure 2).

6.1. ISO/IEC 2700x

An information security system and standard package of British development, which provides a guide to information protection activities [15]. Security requirements and related measures are determined by companies according to business aims and objectives and corporate strategy. Information security receives a central position (integrity, confidentiality and availability), not linked to any type of information technology.

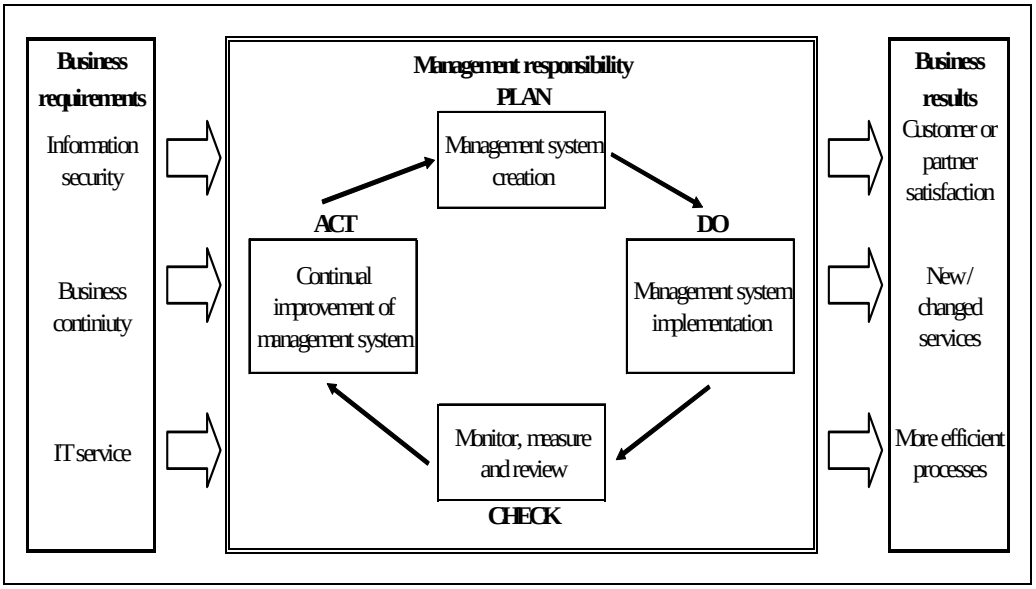

Figure 2. PDCA model for information security processes

The standard [7] divides the operation of the company and the related requirements into 11 security areas and within these, to 39 objectives and 133 protective measures. The built-up and documented information security management system may be approved by an independent accreditation organisation [8]. There are a few supplementary parts to the standard package (these appear as separate individual standards): e.g. prescriptions concerning information security management - ISO/IEC 27005 [9]. Development is continuous. New standards are planned to be introduced (e.g. introduction guide - ISO/IEC 27003; inter-sector communication regulations based on information security - ISO/IEC 27010; information security for telecommunications - ISO/IEC 27011).

6.2. ISO/IEC 20000-1, -2

The standard was created on the basis of and in harmony with the British-developed ITIL (Information Technology Infrastructure Library), dealing with the operation issues of information systems [1], [16]. The first part of the document [10] is

a set of formal requirements concerning acceptable information technology services, while the second part [11] is a guide to service management and auditing according to the first part. Service management activities are connected to the currently popular PDCA model, which is applied in several standards.

In addition to the management system, the issues of planning and implementation of information technology systems and the planning and creation of new services, there are five basic areas of complete service management;

- Service delivery (service level, service reporting, capacity, service continuity, availability, budgeting and accounting for IT services)
- Management processes (configuration and change management)
- Release (documents, operational description distribution management, release management)
- Solution processes (incident and problem management)
- Relationship (customer service, business relationship and supplier)

6.3. BS 25999-1, -2

The British standard package [12], [13] concerning business continuity also facilitates the creation of a corporate process management system. It is applicable to all types of organisations. The assessment of potential threats and risk factors is the result of a complex impact analysis (Business Impact Analysis, BIA). The key products of the company and the steps of their manufacturing as well as service support processes, the maximum acceptable period of business breakdown and dependence on external business partners are examined.

Based on the impact analysis the company creates a Business Continuity Plan which helps avoid problems even in case of unexpected events (natural disaster, shortage of raw materials, utility failure, labour force shortage, breakdown of technological equipment, IT problems, customer complaints etc.). The firm retains its good reputation and is able to carry on value-added processes and maintain connections with business partners.

The company's critical material and information processes all have substitute options that facilitate operation under extraordinary circumstances and the return to the original conditions. According to the PDCA cycle, documentation, regular managerial checking, testing and continuous development of the management system is very important.

7. THE MANAGEMENT OF INFORMATION SECURITY FOR PARTICIPANTS OF THE SUPPLY CHAIN

The management of information security for participants of the supply chain. Today the choice of strategic business partners depends on communication possibilities resting on a stable, reliable IT basis no less than on the price and quality of the product to be purchased or the existence of verifiable references. Systematically analysing the aims and objectives of the ISO/IEC 27001 standard and the practical guide needed for the audit, risks must be managed in several areas.

The aim of the setup of an information security management system is the creation of information security and operation according to partners' expectations and applicable domestic and international regulations; the preservation of the integrity and the confidentiality of data and information and the providing of their availability. Incidental business damage should be minimised and business continuity ensured.

7.1. Information security screening

The first step in constructing the system after managerial decision and the setup of the task organisation is the information security screening and assessment.

In general it may be said that in the preliminary phase of the creation of management systems the issues tackled in various forms are the assessment of protection requirements, threat analysis, risk analysis and risk management.

Information security screening may concern environmental infrastructure, data carriers, hardware, software, documents, communication and the human factor in 'an information technology configuration'.

An important part of the information security chapter of the evaluation is a detailed and individualised "stock-taking" of hardware, software and communication systems and relations. This facilitates a concrete definition and analysis of threat/danger, and the creation of the appropriate management system.

7.2. Risk assessment and evaluation

In the course of disclosure weak points and dangerous factors are revealed in the examined areas. They are evaluated, analysed and ranked. Possible damage and risks associated with these threats are also grouped. Necessary measures to avoid or reduce them to an acceptable level are also assigned.

In accordance with this, the steps of risk assessment and analysis are the following:

- disclosure of protection demands, definition of information assets, disclosure and scheduling of primary importance data for the organisation,
- threat analysis; the collection of threatening factors,
- risk analysis; the examination of the effects of threats,
- risk management and definition of protective measures; risk protection or minimization on the basis of risk analysis by defining possible options.

7.3. Documentation

The next step in the creation of an information security management system is the preparation of the documentation. In the course of this we must take into consideration the size and structure of the organisation, the complexity of its processes and their interactions, external and internal regulations pertaining to its functioning as well as specifications and traditions of the trade. Beside general aims, the formulation of a documentation and regulation system calls for the completion of concrete tasks in the light of the operation and protection objectives of the organisation.

7.4. Introduction

In addition to along general considerations there are further areas to be regulated in the course of creating the management system:

- document management,
- human policy activities,
- security classification of information management devices, physical and environmental protection,
- planning and developing activities, the development of the system of information management,
- the order of supplier contract signing and supplier assessment,
- ”standard” work processes,
- supervision of an integrated management system,
- control and examination of work processes,
- management of security disturbances and operational errors,
- corrective and preventive activities.

7.5. Auditing as a possibility

There is a possibility to have the information security management system audited by an independent organisation. This ensures a stronger guarantee for the appropriateness of the system and may influence the company image in a positive way. Auditing the management system comprises factors of client demand satisfaction and the examination of guarantees offered by the system. The areas listed below encompass the prescriptions considered in creating the system, together with their appropriate regulation and documentation;

- security policy,
- risk analysis and management,
- business continuity plan,
- disaster recovery plan,
- declaration of applicability,
- data protection, virus protection,
- registering and investigating incidents,
- security regulations connected to jobs and persons, applicable laws and regulations, other (external) regulations, the existence of professional recommendations, familiarity and compliance with them,
- existence of administrative – environmental (defence and security) – information technology regulations, and their simultaneous implementation in practice.

8. CONCLUSIONS

An information technology management system created according to the above discussed international standards and recommendations may help companies fit into

supply chains. Informational technology and process developments are easier to complete since there exists a set of regulations complementing and fulfilling a system of demands.

Joint application of seemingly hardly related standards and recommendations is justified by the fact that the optimal running of integrated supply chain information systems is not only a question of information technology. When and how who may get access to necessary information, or when they may launch or step into an intra-company or inter-company business transaction is of vital importance for supply chain-organised companies. Risk management is not separable in material and information processes and information technology.

REFERENCES:

[1]. Bon, J.V.; Verheijen, T. - IT Service Management Forum: *Frameworks for IT Management,* Van Haren Publishing, 2006

[2]. Chikán, A.; Gelei A. - *Az ellátási láncok és menedzsmentjük,* Harvard Business Manager (Hungarian Edition), 2005. January, pp.35-44

[3]. Christoper, M.; Peck, H. - *Building the resilient supply chain,* International Journal of Logistics Management, vol.15, no.2, 2004, pp.1-13

[4]. Mentzer, J.T.; Dewitt, W.; Keebler, J.S.; Min, S.; Nix, N.W.; Smith, C.D.; Zacharia, Z.G. - *Defining Supply Chain Management,* Journal of business Logistics, vol.22, no.2, January 2001, pp.1-25

[5]. Smith, G.E.; Watson, K.J.; Baker, W.H.; Pokorsk, J.A. - *A critical balance: collaboration and security in the IT-enabled supply chain,* International journal of production research, vol.45, no.11, June 2007, pp.2595-2613

[6]. Ward, J. - *Principles of information systems management,* Routledge, London, 1995

[7]. *** - ISO/IEC 27001:2005, Information technology, Security techniques - Information security management systems - Requirements

[8]. *** - ISO/IEC 27002:2005, Information technology, Security techniques - Code of practice for information security management

[9]. *** - ISO/IEC 27005:2008, Information technology, Security techniques - Information security risk management

[10]. *** - ISO/IEC 20000-1:2005, Information technology, - Service management, Part 1: specification

[11]. *** - ISO/IEC 20000-2:2005, Information technology, Service management, Part 2: Code of practice

[12]. *** - BS 25999-1:2006, Business Continuity Management, Code of Practice, www.bs25999.com

[13]. *** - BS 25999-2:2006, Business Continuity Management, Specification, www.bs25999.com

[14]. *** - Supply Chain Council: Supply-Chain Operations Reference-model (SCOR), Overview. Version 9.0, 2008, www.supply-chain.org

[15]. *** - ISO27k Toolkit, Version 3.2, 2008, Prepared by the international community of ISO27k implementers at www.ISO27001security.com

[16]. *** - An Introductory Overview of ITIL V3. IT Service Management Forum, 2007, www.itsmfi.org