THE POLICY INFORMATION AS A DETERMINANT OF SECURITY IN THE SUPPLY CHAIN

ŻYWIOŁEK Justyna[1]

[1]Technical University of Czestochowa, Czestochowa, Poland, EU

Abstract

The article presents the outcomes of research concerning information security in the supply chain. The research has been based on the scientific observations and the analysis of the state of the enterprise that were performed in three metallurgical plants. The research has entailed the state of information security and information flows in the supply chain.

Keywords: Information security, security in the supply chain, business security system, information flows in the supply chain

1. INTRODUCTION

In the 20th century the flows of loads were exposed to different risk resulting from natural phenomena and human activity. However, the 21st century has brought new perils. Owing to the fact that we became information society, it is the information that is treated as the uppermost resource for a company. Hitherto, the companies have protected data against industrial spying by creating the isolating system. The developing international trade has facilitated supranational cooperation along with having made information and technology security difficult.

2. THE SYSTEM OF INFORMATION PROCESSING

In the companies performing nowadays, a large amount of information is generated. Even the owner or management do not have the complete knowledge of each piece of information arising in a company. At the present time the validity of information is so low and changes so rapidly, that the models of management and systems are created which major aim is to protect data [1, 2]. The development of companies to a large extent causes information paralysis and 90% of decisions are made by 5% of the staff employed in a company [2, 3]. The solution to this situation is to create the policy of information management, delegating decisions to particular employees, building the conduct procedures in difficult or even crisis situations [6, 10] . Unfortunately, transferring the decisiveness to employees is frequently received by the management as a dangerous situation for a company's existing. The **Figure 1** shows the amount of information processed by the company.

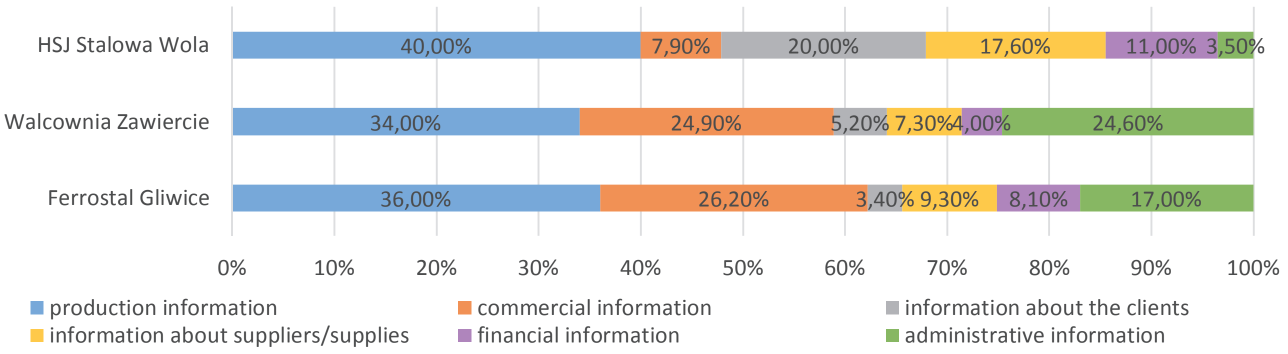


Figure 1 Data gathered in the analyzed companies

The **Figure 1** shows the percentage structure of information in a division into the particular areas of activity taken in the company. It can be noticed that Huta HSJ Stalowa Wola gathers a large amount of information concerning its suppliers and rendered supplies, clients, and the manufacturing process. The remaining two companies gathers administrative and commercial data.

The excess of information can be the reason for losing the control by a company over generating, processing and taking advantage from the data. In this situation the methods for control and information classification should be elaborated [4, 9]. Therefore, the system of secure information processing should be created. The **Figure 2** depicts the scheme of correct and incorrect information management.

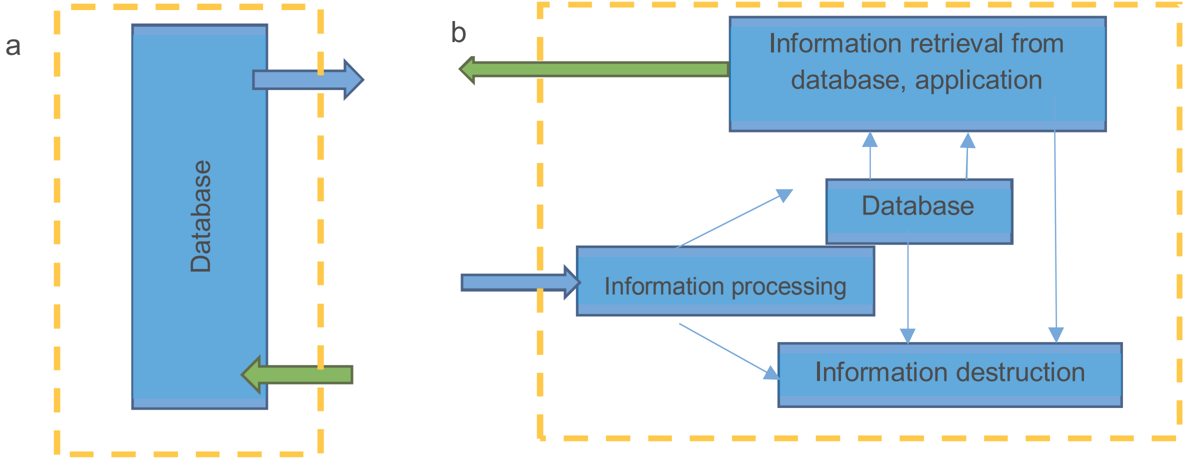


Figure 2 The management of information in a company a) correct, b) incorrect

The proper information management provides a company the opportunity for information processing, verification of its reliability, and if it is acknowledged as useful, it is included in the database. The useless data are destroyed. If information management fails, the flow and deletion of information are entirely uncontrolled, which may lead to information chaos or its lack.

3. INFORMATION SECURITY IN A COMPANY

In each company the selected elements of information security system are in force. More and more entrepreneurs are supervising the movement of people in a company via monitoring or using the antivirus or anti-spyware programs. Nevertheless, the implementation of information security system does not mean keeping to the selected safety rules. It is necessary to use the following rules for creating information security [8,11]:

- determining the requirements of information /data-handling system in a company,
- controlling activities currently taken,
- rating information,
- assessing weak points,
- establishing the budget of activities,
- defining the required security,
- organizing and creating the security.

The application of safety rules requires the collaboration of all employees in a company, pursuing the suitable internal policy, making the abandonment of the binding procedures possible, updating security system [5, 7].

The implementation and functioning of information security policy in a company is the assurance of physical security, as well as data-handling paper and electronic documentation [7], which is illustrated in the **Figure 3**.

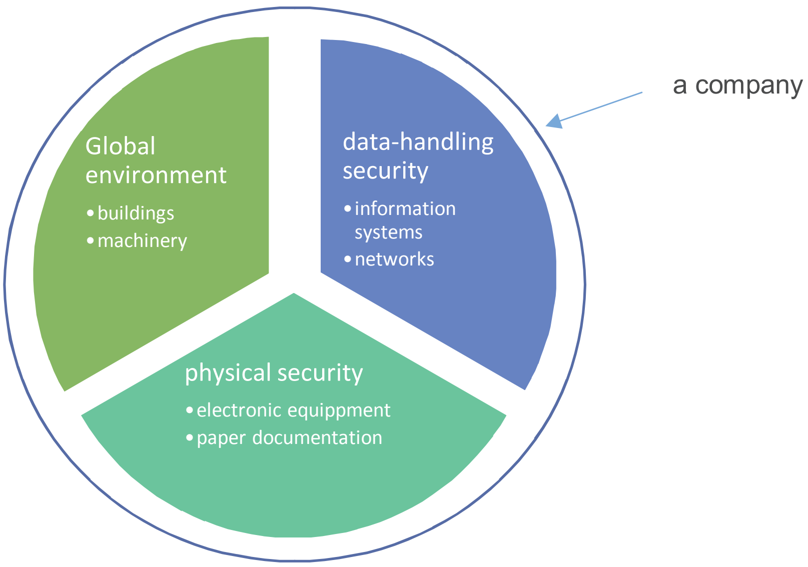


Figure 3 Issues concerning information security in a company

The policy of information security should work in a company in two scopes, the physical and the data-handling ones. The first one comprises global environment, thus the area at which a company functions, the monitored site, entry gate, buildings, civil engineering works within a company and machinery. The second component of security policy is physical security. It concerns inter alia the security of computers, data carriers, paper current and archival documentation, security zones in buildings. Whereas data-handling security is provided inter alia by the security of information systems, security against cyber-attacks, surveillance of internal network and Internet traffic. The system of information security is shown in the **Figure 4**.

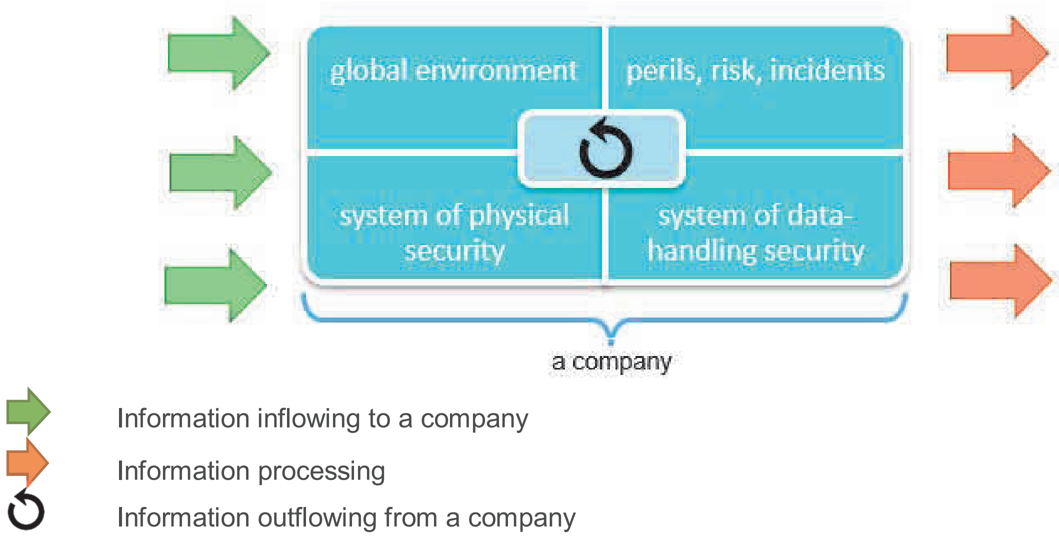

global environment
perils, risk, incidents
system of physical security
system of data-handling security
a company
Information inflowing to a company
Information processing
Information outflowing from a company

Figure 4 The system of information security in a company

The system ensuring information security in the enterprise, but it does not influence the type of information that inflows or when passing the information outside it is received as the same piece of information, without distortions, errors and whether it reaches the addressee. The policy of information security does not provide, however, information security beyond the area that a company functions, which means that cooperating permanently with contractors, entrepreneurs are vulnerable to perils of the same sort as the self-existing company. It would be necessary, then, to create the common system of access to information in order to secure it. However, it is not feasible, because each company acts in its own interest and material profit.

4. SECURITY IN THE SUPPLY CHAIN

The issue of security in the supply chain is a complex issue and it should be considered in various dimensions. Information security is one of them. Information security of the system which is the supply chain may treat each company as one of the subsystems [8]. In order to discuss information security in the supply chain the sites of information flows in the researched chain should be considered (**Figure 5**).

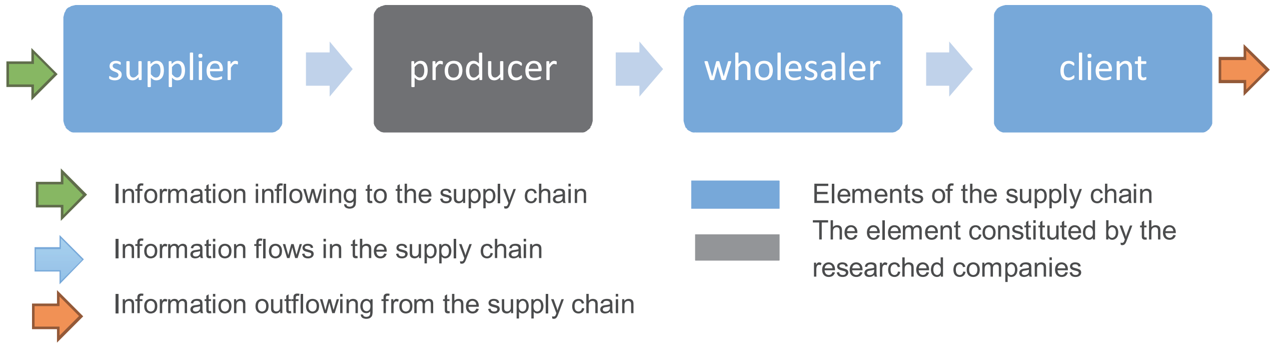
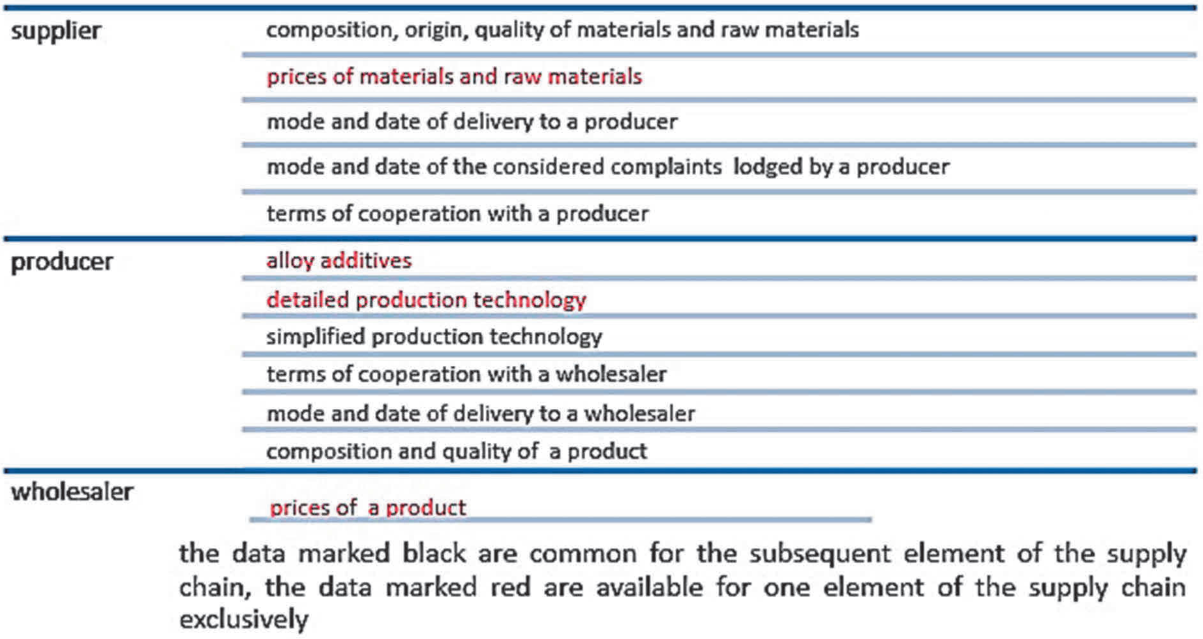

supplier
producer
wholesaler
client
Information inflowing to the supply chain
Information flows in the supply chain
Information outflowing from the supply chain
Elements of the supply chain
The element constituted by the researched companies

Figure 5 The supply chain considering information flows

The manufacturing companies that are researched are the recipients of information from suppliers, and the information processed by them is dealt by wholesalers. The system of security in the supply chain should protect the data that are common for the components of the supply chain that work in close cooperation. (**Figure 6**). Having the common information requires taking steps in order to secure it. The researched companies took actions that have been necessary for protecting common data. The effects of these activities are shown in the **Figure 7**. The elements implemented so far have seen an increase in the indices that are the signs of a positive impact on information security in the supply chain.



supplier	composition, origin, quality of materials and raw materials
	prices of materials and raw materials
	mode and date of delivery to a producer
	mode and date of the considered complaints lodged by a producer
	terms of cooperation with a producer
producer	alloy additives
	detailed production technology
	simplified production technology
	terms of cooperation with a wholesaler
	mode and date of delivery to a wholesaler
	composition and quality of a product
wholesaler	prices of a product

the data marked black are common for the subsequent element of the supply chain, the data marked red are available for one element of the supply chain exclusively

Figure 6 Information which should be protected by security system of the supply chain

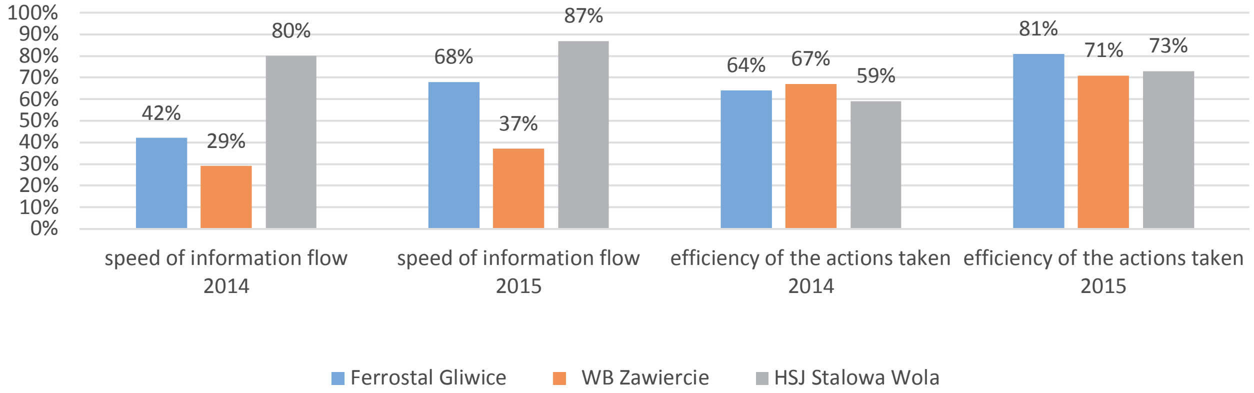


Figure 7 Indicators of the effects of implementing the system of information security in the supply chain

5. CONCLUSION

The article presents the outcomes of research concerning information security in the supply chain. The research has been made at the beginning of 2016. The analysis has entailed three elements of the supply chain which are suppliers, producers and wholesalers. Their system of information processing has been analyzed, which has enabled to create the model system of information management and indicate the errors that the entrepreneurs have made so far. Subsequently, there has been made the distribution of the processed data into the separate and common ones, which has enabled to determine which information should be under collective security. Implementing these solutions has allowed for making calculations whether the security had brought the expected results. It can be univocally acknowledged that creating the system of information security has contributed to the speed of information flows to the final recipient. It has also increased the efficiency of the conducted activities within information management.

REFERENCES

[1] KIFNER T., Polityka bezpieczeństwa i ochrony informacji, Wyd. Helion, Gliwice, 1999.

[2] POLACZEK T., Audyt i bezpieczeństwo informacji w praktyce, Helion, Gliwice, 2006.

[3] BLAIK P., Logistyka w systemie zarządzania przedsiębiorstwem, PWE, Warszawa, 2013.

[4] ŁUCZAK J., TYBURSKI M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań, 2010.

[5] ŁUNARSKI J., Systemy zarządzania bezpieczeństwem w przedsiębiorstwie, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów, 2009.

[6] CYGAN T., Podręcznik administratora bezpieczeństwa informacji, Presscom, Wrocław, 2011.

[7] ŻYWIOŁEK J., STANIEWSKA E., Zagrożenia zarządzania bezpieczeństwem informacji w przedsiębiorstwie, Logistyka VOL 6, 2012

[8] ŻYWIOŁEK J., Wpływ obniżania jakości informacji na przepływ informacji w przedsiębiorstwie, Logistyka VOL 6, 2012

[9] ULEWICZ R., JELONEK D., MAZUR M. Implementation of logic flow in planning and production control, management and production engineering review , Volume: 7 , Issue: 1, Pages: 89-94 , MAR 2016 DOI: 10.1515/mper-2016-0010

[10] NOWICKA-SKOWRON, M., ULEWICZ R., quality management in logistics processes in metal branch, Metal 2015: 24th international conference on metallurgy and materials, tanger Ltd, brno 2015, pages: 1707-1712

[11] BORKOWSKI S., ULEWICZ R., SELEJDAK J., KONSTANCIAK M., KLIMECKA-TATAR, D., The use of 3x3 matrix to evaluation of ribbed wire manufacturing technology, 21ST INTERNATIONAL CONFERENCE ON METALLURGY AND MATERIALS (METAL 2012), TANGER Ltd, 2012, Pages: 1722-1728.