Częstochowa 06.12.2021r.

Dissertation abstract

D. thesis of Estera Pietras, M.Sc.

titled. "Information Security Management

in companies of the automotive industry".

Observing the growing interest of businesses in protecting their information assets and the dynamically emerging threats of information loss, one can conclude, that the problem of ensuring information security in companies is a topical issue and requires detailed analysis. Management boards of business organizations, aware of the imperfections of their information protection systems, are looking for effective methods of identifying emerging threats, combined with proper risk management. Thus, in the management of the enterprise, one of the very important factors is to prepare for the appearance of a threat and to create opportunities to skillfully reduce its impact on the information resources held.

Due to the occurring problems of inadequate protection during storage, processing and sharing of information, the dissertation attempts to enhance the knowledge of information security and proposes a system to reduce the risk of information loss.

The study adopted the following hypothesis: *"The intense increase in the number of information security threats in enterprises requires the use of adaptable security management systems in which technical and procedural measures are adapted to the requirements determined by current information loss risk analyses."*

The utilitarian aim of the study was to develop guidelines in the field of information security management, which will take into account important, and so far ignored threats, for a selected group of companies, belonging to the automotive sector.

As a result of literature analysis and empirical research, the dissertation's aim was achieved by identifying new threats and concepts of conduct, in the information security management system. The importance of information in companies was highlighted, the way of its protection was shown taking into account the results of risk analysis. The paper identifies subsystems for information flow and security and develops a system design to reduce the risk of information loss.

Surveys were conducted among senior and lower saber management positions and employees in non-management positions. The use of analysis tools (survey, interview, observation, and experiment) allowed us to identify many deficiencies in information security systems. A taxonomy of hazard sources was performed according to the 5M method. The discussed methods enabled the author of this paper to describe the investigated enterprises, establish facts, motivation of employees and their level of awareness towards the stored information and expectations concerning the applied security in the employing unit. In addition, an experiment involving a simulated attack aimed at obtaining potentially protected information showed that organizations lack resilience to real-world events that could result in extortion, destruction, or modification of information.

The risk estimation process created a new catalog of grouped risks that remains open to dynamically emerging new sources of risk. Threats were assessed through a risk analysis process based on confidentiality, integrity, availability, accountability, authenticity, reliability. The adopted analysis methodology led to the determination of the risk of loss of information, or some of its attributes, which turned out to be at a high level. Such a condition cannot be acceptable in any enterprise and requires corrective action to be taken to ensure information security.

Taking into account the construction of information security management systems, the paper develops an information security management system design, reducing the risk of information loss, adapted to the specifics of the analyzed enterprises. The system consists of the following subsystems: project development security, information exchange with the external environment, production and technology used, users and database. Although the research was conducted in nine companies in the automotive industry, the design is versatile enough to be used in other organizations of similar structure and size. The paper mapped the systemic patterns in the form of procedures to facilitate threat identification and faster response to emerging information security incidents.

Conducting research and analyzing the obtained results, the analysis of the risk of information security loss in the studied group of enterprises was performed twice. The first analysis considered the identified risks and existing safeguards and found an unacceptable level of risk. Proposing new safeguards dedicated to the identified threats made it possible to reduce the level of risk of losing information or its attributes to an acceptable level. On the other hand, the implementation of an information security management system should significantly improve management processes in terms of identifying new threats and developing dedicated security measures as quickly as possible.

7. 12. 2021